Compléments et errata à

Algèbre et géométrie

81 thèmes pour l'Agrégation de mathématiques

Ellipses 2017

Jean Fresnel & Michel Matignon

(mai 2024)

page de l'ouvrage		page du document ci-après
5	complément : déterminant et indicateur d'Euler	3
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-*	6
66	complément : prolongement d'une colonne en une matrice inversible .	7
80	paragraphe I.8. , actualité des résultats sur $\mathbb{R}$, ...	71
107	complément : description des produits scalaires	11
121	complément: les sous-groupes de $\frac{\mathbb{Q}}{\mathbb{Z}}$	19
128	complément : le théorème est encore valable si on suppose seulement que G est un groupe fini (non nécessairement abélien).	26
128	ligne -2 avant 2.2) enlever ")"	26
130	complément : sur le nombre minimum de générateurs d'un groupe de type fini	26
131	complément : quand tout groupe d'ordre n est abélien (resp. cyclique)	34
133	ligne 2 du théorème 1.4, remplacer "les orbites de S sous cette" par "les orbites de S sous l'action de Σ"	45

136	ligne -2 avant la définition 2.5, lire "homomorphisme" au lieu de "homorphisme"	45
144	ligne -1, lire" proposition 5.3" au lieu de "proposition 1"	45
145	complément : famille de transpositions génératrice de $\mathfrak{S}_n$ et connexité du graphe associé	45
235	complément à IV.7.1. discriminant	47
235	complément à IV.7.1. quelques calculs de discriminant	51
247	paragraphe IV.8.1., 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 $G = \mathbb{U}_d$.	54
249	complément à IV.8.2. : sommes de Newton relatives aux racines du polynôme cyclotomique	54
278	complément : quand le groupe des inversibles d'un anneau est fini	56
299	complément : triangles rectangles isocèles et quadrilatère	62
299	complément : sur trois cercles passant par un même point (théorème de Johnson 1916)	65
302	paragraphe V.2.1	67
306	paragraphe V.2.2.	68

page 5, déterminant et indicateur d'Euler

Définition 1 Soient $a, b \in \mathbb{Z}$, alors $\text{pgcd}(a,b)$ désigne le générateur positif ou nul de l'idéal $a\mathbb{Z} + b\mathbb{Z}$.

Définition 2 Soit $n \geq 1$, un entier, alors *l'indicateur* d'Euler de n, noté $\varphi(n)$ est le cardinal du groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ des inversibles de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$. En particulier $\varphi(1) = 1$.
Facilement, on a

$$\varphi(n) = \text{card}\{k \mid 1 \leq k \leq n \text{ et } 1 = \text{pgcd}(k,n)\}.$$

Il suit du théorème des restes chinois que si m, n sont des entiers avec $m \geq 1, n \geq 1$ et $1 = \text{pgcd}(m,n)$, alors

(1) $$\varphi(mn) = \varphi(m)\,\varphi(n).$$

En particulier si $p \geq 1$ est un nombre premier, si $\alpha \geq 1$, on a

(2) $$\varphi(p^\alpha) = p^{\alpha-1}(p-1).$$

Proposition 1 Soit $n \geq 1$, *un entier, alors on a*

(3) $$n = \sum_{d \mid n} \varphi(d)$$

où $\varphi(d)$ est l'indicateur d'Euler de d.

Démonstration
Soit p un nombre premier, $\alpha \geq 0$, alors la proposition est satisfaite pour $n = p^\alpha$. En effet l'ensemble des diviseurs positifs de p^α est $\{p^k \mid 0 \leq k \leq \alpha\}$. Comme $\varphi(p^k) = (p-1)\,p^{k-1}$ si $k \geq 1$ et $\varphi(p^0) = 1$, on a bien

(4) $$p^\alpha = \sum_{k=0}^{\alpha} \varphi(p^k),$$

i.e. la proposition est vraie pour $n = p^\alpha$.
Il reste à faire une récurrence sur le nombre de premiers distincts qui divisent n.
Ainsi on peut écrire $n = m\,p^\alpha$ où p est premier, $\alpha \geq 1$ et $p \nmid m$.
Si $\mathcal{D}$ est l'ensemble des diviseurs positifs de m, et si $\mathcal{D}'$ est l'ensemble des diviseurs positifs de $m\,p^\alpha$, alors on a

$$\mathcal{D}' = \mathcal{D} \cup p\,\mathcal{D} \cup \ldots \cup p^\alpha \mathcal{D}.$$

Il suit donc que

$$\sum_{d \mid n} \varphi(d) = \sum_{\delta \in \mathcal{D}} \left(\sum_{k=0}^{\alpha} \varphi(\delta p^k) \right) .$$

Facilement, il suit de (1) que $\varphi(\delta p^k) = \varphi(\delta)\, \varphi(p^k)$, ainsi

$$\sum_{d \mid n} \varphi(d) = \left(\sum_{\delta \in \mathcal{D}} \varphi(\delta) \right) (1 + (p-1) + p - 1)\, p + \ldots + (p - 1 p^{\alpha - 1}) ,$$

i..e.

$$\sum_{d \mid n} \varphi(d) = \left(\sum_{\delta \in \mathcal{D}} \varphi(\delta) \right) p^{\alpha} .$$

Or par hypothèse de récurrence, on a $\sum_{\delta \in \mathcal{D}} \varphi(\delta)) = m$.

Ce qui montre la proposition.

Remarque 1 (une autre démonstration élémentaire)

Soient $n \geq 1$, un entier, $F_n := \{ \frac{a}{n} \in \mathbb{Q} \mid 1 \leq a \leq n \}$.

Soient $1 \leq d \leq n$ avec $d \mid n$ et $F'_d := \{ \frac{b}{d} \in \mathbb{Q} \mid 1 \leq b \leq d$ et $1 = \text{pgcd}\,(b, d) \}$.

Facilement $\text{card}\, F_n = n$ et $\text{card}\, F'_d = \varphi(d)$.

Supposons avoir montré que

(1) $$F_n = \bigcup_{d \mid n} F'_d \text{ (réunion disjointe)} ,$$

alors il suit que $\text{card}\, F_n = \sum_{d \mid n} \text{card}\, F'_d$, i.e.

(2) $$n = \sum_{d \mid n} \varphi(d) ,$$

ce qui est la proposition 1.

Il nous reste donc à montrer (1).

(3) Montrons que si $d \mid n$, alors $F'_d \subset F_n$.

En effet si $z \in F'_d$, on a $z = \frac{b}{d}$, $1 \leq b \leq d$. Comme $d \mid n$, il existe c avec $n = c\, d$ et donc $z = \frac{c\, b}{c\, d} = \frac{c\, b}{n}$ et facilement $1 \leq c\, d \leq n$.

Ce qui montre (3) et donc $\bigcup_{d \mid n} F'_d \subset F_n$.

(4) Montrons que $F_n \subset \bigcup_{d \mid n} F'_d$.

Si donc $z = \frac{a}{n} \subset F_n$, soit $c = \text{pgcd}(a, n)$, on a donc $a = c\, b$, $n = c\, d$ et $1 = \text{pgcd}(b, d)$. Il suit que $z = \frac{b}{d}$ et que $z \in F'_d$.

(5) Il reste à montrer que $F'_d \cap F'_{d'} \neq \phi$ implique $d = d'$.
On a donc $z \in F'_d \cap F'_{d'}$, ce qui veut dire que $z = \frac{a}{d} = \frac{a'}{d'}$
avec $d \mid n,\ d' \mid n$, $1 \leq a \leq d$, $1 \leq a' \leq d'$) , $1 = \text{pgcd}(a, d)$ et $1 = \text{pgcd}(a', d')$ et aussi

(6) $$a\,d' = a'\,d$$

Comme $1 = \text{pgcd}(a, d)$ il suit du lemme de Gauss que $a \mid a'$ et par une méthode analogue $a' \mid a$; ainsi $a = a'$ et alors $d = d'$.

Remarque 2 (sur les racines de l'unité)
Soient $n \geq 1$, $\mathbb{U}_n := \{ z \in \mathbb{C} \mid z^n = 1 \}$, $d \mid n$, $\mathbb{U}'_d = \{ z \in \mathbb{U}_n \mid o(z) = d \}$.
Facilement, l'application $\frac{a}{n} \longmapsto e^{i\,2\pi\frac{a}{n}}$ est une bijection de F_n sur $\mathbb{U}_n$; de même , l'application $\frac{b}{d} \longmapsto e^{i\,2\pi\frac{b}{d}}$ est une bijection de F'_d sur $\mathbb{U}'_d$.
Il suit alors de la remarque 1 que

$$\mathbb{U}_n = \biguplus_{d \mid n} \mathbb{U}'_d \ .$$

Proposition 2 *Soient* $n \geq 1$, $D_n := [\text{pgcd}(i-j, n)]_{1 \leq i, j \leq n} \in M_n(\mathbb{Z})$, *il suit en particulier de la définition 1 que* $\text{pgcd}(i-j, n) = \text{pgcd}(j-i, n)$. *Soit*

$$P(T) := \text{pgcd}(0, n) + \text{pgcd}(1, n)\,T + \ldots + \text{pgcd}(n-1, n)\,T^{n-1}.$$

Alors $\det D_n = P(\omega^0)\,P(\omega^1)\,\ldots\,P(\omega^{n-1})$ *où* $\omega := e^{i\frac{2\pi}{n}} \in \mathbb{C}$. *Par ailleurs on a* $P(\omega^k) = \sum_{d \mid n} \varphi(d)\,(1 + \omega^{k\,d} + \omega^{2\,k\,d} + \ldots + \omega^{(\frac{n}{d}-1)\,k\,d}) > 0$, *ce qui montre que* $\det D_n > 0$.

Démonstration
Compte tenu du fait que $\text{pgcd}(k, n) = \text{pgcd}(n-k, n)$, il suit que la matrice D_n est circulante avec pour première colonne

$$^t(\text{pgcd}(0, n), \text{pgcd}(1, n), \ldots, \text{pgcd}(n-1, n)) \ ,$$

on sait alors que

$$\det D_n = P(\omega^0)\,P(\omega^1)\,\ldots\,P(\omega^{n-1}) \ \text{ où } \ \omega := e^{i\frac{2\pi}{n}} \ ,$$

c'est I.2.3. p. 3.

Par ailleurs, il suit facilement de la proposition 1 que

$$\text{pgcd}(k,n)=\sum_{d\mid \text{pgcd}(k,n)}\varphi(d)$$

où φ est l'indicateur d'Euler, que

$$P(T)=\sum_{d\mid n}\varphi(d)(1+T^{kd}+T^{2kd}+...+T^{(\frac{n}{d}-1)kd}) .$$

Ainsi $P(\omega^k)=\sum_{d\mid n}\varphi(d)(1+\omega^{kd}+\omega^{2kd}+...+\omega^{(\frac{n}{d}-1)kd})$.

Si $\omega^{kd}\neq 1$, on a $1+\omega^{kd}+\omega^{2kd}+...+\omega^{(\frac{n}{d}-1)kd}=0$,

si $\omega^{kd}=1$, on a $1+\omega^{kd}+\omega^{2kd}+...+\omega^{(\frac{n}{d}-1)kd}=\frac{n}{d}$,

Tout cela montre clairement que $P(\omega^k)>0$ et donc que $\det D_n>0$.

Proposition 3 *Soient $n\geq 1$ un entier, φ l'indicateur d'Euler, alors on a*

$$\sum_{k=1}^{n}\text{pgcd}(k,n)=\sum_{d\mid n}d\,\varphi(\tfrac{n}{d}) .$$

Démonstration

Soit $d\geq 1$ avec $d\mid n$, il suffit de calculer

$$\text{card}\{k\mid 1\leq k\leq n \text{ avec } \text{pgcd}(k,n)=d\}$$

puisque

$$\sum_{k=1}^{n}\text{pgcd}(k,n)=\sum_{d\mid n}d\,\text{card}\{k\mid 1\leq k\leq n \text{ avec } \text{pgcd}(k,n)=d\} .$$

Or $f\in\{k\mid 1\leq k\leq n \text{ avec } \text{pgcd}(k,n)=d\}$ si et seulement si $d\mid f$, $d\mid n$ et $1=\text{pgcd}(\frac{f}{d},\frac{n}{d})$. Cela veut dire que $f=dg$ avec $1\leq g\leq\frac{n}{d}$ et $1=\text{pgcd}(g,\frac{n}{d})$.

Cela montre bien que

$$\text{card}\{k\mid 1\leq k\leq n \text{ avec } \text{pgcd}(k,n)=d\}=\varphi(\tfrac{n}{d}) .$$

[F.M.1] Fresnel J. & Matignon M. Algèbre et Géométrie Hermann 2011

[F.M.2] Fresnel J. & Matignon M. Algèbre et Géométrie Ellipses 2017

page 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-

page 66, prolongement d'une colonne unimodulaire en une matrice inversible

Soient A un anneau commutatif, $M \in G\ell_n(A)$, i.e. il existe $N \in M_n(A)$ avec $MN = I_n$. Il suit de cela que $\det M \in A^\times$, i.e. $\det M$ est un inversible de A . Si $x := {}^t(x_1, x_2, \ldots, x_n)$ est la première colonne de M , le calcul du déterminant de M en utilisant le développement selon la première colonne montre qu'il existe $u_1, u_2, \ldots, u_n \in A$ avec $x_1 u_1 + x_2 u_2 + \ldots + x_n u_n = \det M \in A^\times$, ce qui veut dire que $A = x_1 A + x_2 A + \ldots + x_n A$.
Une colonne $x := {}^t(x_1, x_2, \ldots, x_n)$ de A^n telle que $A = x_1 A + x_2 A + \ldots + x_n A$ est appelée *unimodulaire*.

La question est donc de savoir si réciproquement, une colonne unimodulaire peut être la première colonne d'une matrice inversible.
Plus généralement, on dira que l'anneau A satisfait le prolongement de la colonne unimodulaire si toute colonne unimodulaire à coefficients dans A peut être la première colonne d'une matrice inversible à coefficients dans A.

La réponse est toujours positive si $n = 2$, en effet si $u x_1 + v x_2 = 1$, alors $\det \begin{bmatrix} x_1 & -v \\ x_2 & u \end{bmatrix} = 1$.
La réponse est aussi toujours positive si A est un anneau principal (proposition ci-après).
Sans changer une virgule, la démonstration s'adapte au cas d'un anneau de Bézout, i.e. d'un anneau intègre dans lequel tout idéal de type fini est principal.
La réponse est toujours positive si $A = K[X_1, X_2, \ldots, X_n]$ lorsque K est un corps commutatif, c'est un résultat de Quillen et Suslin, 1976 ([**La**] p. 848).
Un théorème de Suslin ([**Lam**] p. 111) dit le suivant.
Soient A un anneau commutatif, $a_1, a_2, \ldots, a_n \in A$ avec $A = a_1 A + a_2 A + \ldots + a_n A$. Soient $r_1, r_2, \ldots, r_n$ des entiers avec $r_i \geq 1$ pour $1 \leq i \leq n$ avec $n!$ divise $r_1 r_2 \ldots r_n$, alors ${}^t(a_1^{r_1}\ a_2^{r_2} \ldots a_n^{r_n})$ est la première colonne d'une matrice inversible de $M_n(A)$.

Proposition *Soient* A *un anneau principal,* $n \geq 2$, $x := {}^t(x_1, x_2, \ldots, x_n)$ *avec* $x_k \in A$ *pour* $1 \leq k \leq n$ et $A = x_1 A + x_2 A + \ldots + x_n A$. *Alors il existe* $M \in S\ell_n(A)$ *tel que* x *soit la première colonne de* M *; ce qui veut aussi dire que* $x = M\varepsilon_1$ *où* $\varepsilon_1 := {}^t(1, 0, \ldots, 0)$ *; ce qui veut aussi dire qu'il existe* $N \in S\ell_n(A)$ *tel que* $Nx = \varepsilon_1$.

Démonstration
La démonstration sera par récurrence sur n .

1) Le cas $n = 2$ (on remarquera que dans ce cas, on n'utilise pas le fait que A est principal).
De la relation $A = x_1 A + x_2 A$, il suit qu'il existe $u, v \in A$ avec $u x_1 + v x_2 = 1$.
Soit $N := \begin{bmatrix} x_1 & -v \\ x_2 & u \end{bmatrix}$, on a $\det N = 1$; il suit donc que la proposition est satisfaite.

2) On suppose que $n \geq 3$ et que la proposition est satisfaite pour $n-1$.
Comme A est principal, il existe $d \in A$ avec $dA = x_2 A + x_3 A + \ldots + x_n A$, il suit alors de la relation $A = x_1 A + x_2 A + \ldots + x_n A$ que $A = x_1 A + dA$.
Comme $x_i \in dA$, il existe $y_i \in A$ avec $x_i = d y_i$ pour $i \geq 2$. On a donc $A = y_2 A + y_3 A + \ldots + y_n A$, il suit de l'hypothèse de récurrence qu'il existe $P \in S\ell_{n-1}(A)$ avec $Py = e_1$ où $y := {}^t(y_2, y_3, \ldots, y_n)$ et $e_1 := {}^t(1, 0, \ldots, 0)$ et $(1, 0, \ldots, 0) \in A^{n-1}$. Il suit de cela que

$$Pz = d e_1 \text{ , si } z := {}^t(x_2, x_3, \ldots, x_n) .$$

Soit B la matrice qui est le tableau diagonal (I_1, P) , alors on a

$$B\,{}^t(x_1, x_2, \ldots, x_n) = {}^t(x_1, d, 0, \ldots, 0) \text{ avec } \det(B) = 1 .$$

De la relation $A = x_1 A + dA$, il suit qu'il existe $\alpha, \beta \in A$ avec $\alpha x_1 + \beta d = 1$.
Soit $T := \begin{bmatrix} \alpha & \beta \\ -d & x_1 \end{bmatrix}$, on a $\det T = 1$ et $T \begin{bmatrix} x_1 \\ d \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Soit la matrice C qui est le tableau diagonal (T, I_{n-2}) , on a donc

$$CB\,{}^t(x_1, x_2, \ldots, x_n) = \varepsilon_1 \text{ avec } \det(CB) = 1 ;$$

ce qui montre la proposition.

Description du procédé algorithmique
Comme A est principal, il existe $d_{n-1} \in A$ avec $d_{n-1} A = x_{n-1} A + x_n A$. On a donc $x_{n-1} = d_{n-1} y_{n-1}$, $x_n = d_{n-1} y_n$; il existe donc $\alpha, \beta \in A$ avec

$\alpha y_n+\beta y_{n-1}=1$. Soit $T:=\begin{bmatrix} \beta & \alpha \\ -y_n & y_{n-1}\end{bmatrix}$, on a $\det T=1$ et $T\begin{bmatrix} y_{n-1} \\ y_n\end{bmatrix}=\begin{bmatrix} 1 \\ 0\end{bmatrix}$ et donc $T\begin{bmatrix} x_{n-1} \\ x_n\end{bmatrix}=\begin{bmatrix} d_{n-1} \\ 0\end{bmatrix}$. Si donc N_{n-1} est la matrice qui est le tableau diagonal (I_{n-2},T) , on a

$$N_{n-1}\,{}^t(x_1,x_2,\dots,x_n)={}^t(x_1,x_2,\dots,x_{n-2},d_{n-1},0)\ .$$

Comme A est principal, il existe $d_{n-2}\in A$ avec $d_{n-2}A=x_{n-2}A+d_{n-1}A$, i.e. $d_{n-2}A=x_{n-2}A+x_{n-1}A+x_nA$. Alors en utilisant la méthode précédente, il existe $R\in S\ell_2(A)$ tel que

$$R\begin{bmatrix} x_{n-2} \\ d_{n-1}\end{bmatrix}=\begin{bmatrix} d_{n-2} \\ 0\end{bmatrix}.$$

Si donc N_{n-2} est la matrice qui est le tableau diagonal (I_{n-3},R,I_1) , on a $\det(N_{n-2})=1$ et

$$N_{n-2}N_{n-1}\,{}^t(x_1,x_2,\dots,x_n)={}^t(x_1,x_2,\dots,x_{n-3},d_{n-2},0,0)\ .$$

On continue le processus en choisissant $d_k\in A$ tel que $d_kA=x_kA+x_{k+1}A+\dots+x_nA$ pour $k\geq 2$ et $d_1=1$. Il suit alors que

$$N_1N_2\dots N_{n-2}N_{n-1}\,{}^t(x_1,x_2,\dots,x_n)={}^t(1,0,\dots,0,0)\ .$$

Cela montre d'abord que $(N_1N_2\dots N_{n-2}N_{n-1})$ est un élément de $G\ell_n(A)$ et ainsi $M:=(N_1N_2\dots N_{n-2}N_{n-1})^{-1}$ est un élément de $G\ell_n(A)$ avec $M\,{}^t(1,0,\dots,0,0)={}^t(x_1,x_2,\dots,x_n)$; ce qui veut dire que M est un élément de $G\ell_n(A)$ dont la première colonne est ${}^t(x_1,x_2,\dots,x_n)$.

Remarque Sans changer une virgule, la démonstration ci-dessus s'adapte au cas d'un anneau de **Bézout**, i.e. d'un anneau intègre dans lequel tout idéal de type fini est principal.

Bibliographie

[Bk1] Bourbaki N. *Algèbre commutative ch. 7. Hermann (1965)*

[Bk2] Bourbaki N. *Algèbre ch. 1, 2, 3 Hermann (1970)*

[Fr1] Fresnel Jean *Anneaux Hermann* 2001

[Fr2] Fresnel Jean *Algèbre des matrices Hermann* 2011

[Lam] T. Y. *Serre's problem on projective modules Springer Monographs in Mathematics (Berlin, Heidelberg) 2006*

[Lang] Lang Serge *Algebra Addison-Wesley publisching company* 1993 ou *Graduate Texts in Mathematics Springer-Verlag* 2002

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

page 107, description des produits scalaires sur $\mathbb{R}^n$

1. Les produits scalaires de $\mathbb{R}^n$

Définition Une forme bilinéaire symétrique $f : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ est appelée *produit scalaire* sur $\mathbb{R}^n$ si pour tout $X \in \mathbb{R}^n - \{0\}$, on a $f(X,X) > 0$; on dit aussi que f est une une forme bilinéaire symétrique *définie positive* ([Fr.B.C.D.] p. 64)

Théorème spectral (corollaire 8.14. p. 118 (Fr B,C,D)).
Soient $n \geq 1$, $S \in M_n(\mathbb{R})$, *alors les propriétés suivantes sont équivalentes.*
i) *On a* ${}^tS = S$ (i.e. S est symétrique) ,

ii) il existe $U \in O_n(\mathbb{R})$, $d_1, d_2, \ldots, d_n \in \mathbb{R}$, D *une matrice diagonale de diagonale* $(d_1, d_2, \ldots, d_n)$ *tels que*

$$S = {}^tUDU$$

(i.e. *une matrice symétrique est orthogonalement diagonalisable*).

Proposition 1 (version matricielle des formes bilinéaires symétriques)
Soit $f : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ *une forme bilinéaire symétrique, alors il existe une matrice symétrique* $S \in M_n(\mathbb{R})$ *telle que pour tout* $(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n$, $f(X, Y) = {}^tXSY$.

Démonstration
Si $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ est la base canonique $\mathbb{R}^n$, il suffira de considérer

$$S := [\, f(\varepsilon_i, \varepsilon_j) \,]_{\substack{1 \le i \le n \\ 1 \le j \le n}} .$$

Proposition 2 *Soient* f *un produit scalaire sur* $\mathbb{R}^n \times \mathbb{R}^n$ *. Alors il existe* $U \in O_n(\mathbb{R})$, $d_1, d_2, \ldots, d_n$ *avec* $d_i \in \mathbb{R}$ *et* $d_1 \ge d_2 \ge \ldots \ge d_n > 0$, D *une matrice diagonale, de diagonale* $(d_1, d_2, \ldots, d_n)$ *tels que pour tout* $(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n$
on a

(1) $$f(X, Y) = {}^tX\,{}^tUDUY .$$

Démonstration
C'est une conséquence du théorème spectral et de la proposition 1.

2. Un système de représentants des produits scalaires.

Soient $\mathcal{D}_+$ l'ensemble des matrices diagonales D de $M_n(\mathbb{R})$, de diagonale $(d_1, d_2, \ldots, d_n)$ avec $d_1 \ge d_2 \ge \ldots \ge d_n > 0$, $\mathcal{S}c$ l'ensemble des produits scalaires sur $\mathbb{R}^n \times \mathbb{R}^n$, $\varphi : \mathcal{D}_+ \times O_n(\mathbb{R}) \to \mathcal{S}c$ l'application définie par $\varphi(D, U) := f_{D,U}$ où $f_{D,U}$ est le produit scalaire défini pour tout $(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n$ par $f_{D,U}(X, Y) = {}^tX\,{}^tUDUY$.

Il suit donc de la proposition 2 que φ est une application surjective. Facilement, cette application n'est pas injective. L'objectif de la suite est de trouver une partie $\mathcal{T}$ de $\mathcal{D}_+ \times O_n(\mathbb{R})$ de façon que la restriction ψ de φ à

$\mathcal{T}$ soit une bijection de $\mathcal{T}$ sur $\mathcal{Sc}$; c'est donc ce qu'on pourrait appeler une paramétrisation de $\mathcal{Sc}$.

Proposition 3 *Soient* $U,V\in O_n(\mathbb{R})$, $d_i\in\mathbb{R}$, $d_1\geq d_2\geq\ldots\geq d_n>0$, D *une matrice diagonale, de diagonale* $(d_1,d_2,\ldots,d_n)$ (resp. $\delta_i\in\mathbb{R}$, $\delta_1\geq\delta_2\geq\ldots\geq\delta_n>0$, Δ *une matrice diagonale, de diagonale* $(\delta_1,\delta_2,\ldots,\delta_n)$) .
On suppose que pour tout $(X,Y)\in\mathbb{R}^n\times\mathbb{R}^n$ *on a*
(2) $$f(X,Y)={}^tX\,{}^tU\,D\,U\,Y={}^tX\,{}^tV\,\Delta\,V\,Y\ .$$
Alors $D=\Delta$. *Il suit donc, selon les notations ci-dessus que* $f_{D,U}=f_{\Delta,V}$ *implique* $D=\Delta$.

Démonstration
Facilement (2) dit que
(3) $$ {}^tU\,D\,U={}^tV\,\Delta\,V\ .$$
Comme $U,V\in G\ell_n(\mathbb{R})$ et que ${}^tUU=I_n$, ${}^tVV=I_n$ en considérant le polynôme caractéristique de ${}^tU\,D\,U$ et de ${}^tV\,\Delta\,V$, on a
$$(X-d_1)(X-d_2)\ldots(X-d_n)=(X-\delta_1)(X-\delta_2)\ldots(X-\delta_n)\ .$$
Alors l'unicité de la factorisation et le fait que $d_1\geq d_2\geq\ldots\geq d_n$, $\delta_1\geq\delta_2\geq\ldots\geq\delta_n$, impliquent que $d_i=\delta_i$ pour $1\leq i\leq n$.
Ainsi pour (1) la suite $d_1\geq d_2,\geq\ldots\geq d_n$ est unique.
Il reste donc à examiner l'égalité
${}^t(UV^{-1})\,D\,(UV^{-1})=D$, i.e.
(4) $${}^tW\,D\,W=D\ ,\text{ avec } W\in O_n(\mathbb{R})$$

Proposition 4 *Soit* $P(X)=(X-d_1)^{\alpha_1}(X-d_2)^{\alpha_2}\ldots(X-d_r)^{\alpha_r}$, *avec* $d_i\in\mathbb{R}, d_1>d_2>\ldots>d_r>0$, $\alpha_1+\alpha_2+\ldots+\alpha_r=n$ *et* $\alpha_i\geq 1$. *Soit* D_P *la matrice diagonale constituée du tableau diagonal* $(d_1I_{\alpha_1},d_2I_{\alpha_2},\ldots,d_rI_{\alpha_r})$. *Soit* H_P *le sous-groupe de* $O_n(\mathbb{R})$ *constitué des éléments qui sont des tableaux diagonaux de la forme* $(A_1,A_2,\ldots,A_r)$ *avec* $A_i\in O_{\alpha_i}(\mathbb{R})$ *pour* $1\leq i\leq r$. *Soit* $W\in O_n(\mathbb{R})$.
Alors les propriétés suivantes sont équivalentes.
i) On a ${}^tW\,D_P\,W=D_P$,
ii) on a $W\in H_P$.

Soient maintenant $U, V \in O_n(\mathbb{R})$. *Il suit donc de ce qui précède que les propriétés suivantes sont équivalentes.*
i) On a ${}^tU D_P U = {}^tV D_P V$,
ii) les éléments U *et* V *sont dans la même classe à droite de* $O_n(\mathbb{R})$ modulo H_P .

Démonstration
1) Montrons *ii)* implique *i)* .
Soit W le tableau diagonal de la forme $(A_1, A_2, \ldots, A_r)$ avec $A_i \in O_{\alpha_i}(\mathbb{R})$.
On a donc ${}^tA_i d_i I_{\alpha_i} A_i = d_i I_{\alpha_i}$. Il suit de cela que ${}^tW D_P W = D_P$.
Ce qui est *i)* .

2) Montrons *i)* implique *ii)* .
On a donc ${}^tW D_P W = D_P$, i.e. $D_P W = W D_P$ puisque ${}^tW W = I_n$.
On décompose W par blocs en $W = [W_{i,j}]_{\substack{1 \le i \le r \\ 1 \le j \le r}}$, $W_{i,j} \in M_{\alpha_i, \alpha_j}(\mathbb{R})$. Alors compte tenu de $d_i \neq d_j$ si $i \neq j$ et de la relation $D_P W = W D_P$, on a $W_{i,j} = 0$ si $i \neq j$, ainsi W est le tableau diagonal par blocs $(W_{1,1}, W_{2,2} \ldots W_{r,r})$ et comme $W \in O_n(\mathbb{R})$, on a $W_{i,i} \in O_{\alpha_i}(\mathbb{R})$.
Il suit donc que $W \in H_P$.

Proposition 5 *Soit* $P(X) = (X - d_1)^{\alpha_1}(X - d_2)^{\alpha_2} \ldots (X - d_r)^{\alpha_r}$, *avec* $d_i \in \mathbb{R}, d_1 > d_2 > \ldots > d_r > 0$, $\alpha_1 + \alpha_2 + \ldots + \alpha_r = n$ *et* $\alpha_i \geq 1$. *Soit* D_P *la matrice diagonale constituée du tableau diagonal* $(d_1 I_{\alpha_1}, d_2 I_{\alpha_2}, \ldots, d_r I_{\alpha_r})$. *Soit* H_P *le sous-groupe de* $O_n(\mathbb{R})$ *constitué des éléments qui sont des tableaux diagonaux de la forme* $(A_1, A_2, \ldots, A_r)$ *avec* $A_i \in O_{\alpha_i}(\mathbb{R})$ *pour* $1 \leq i \leq r$. *Soit* $\mathcal{T}_P$ *un système de représentants des classes à droite de* $O_n(\mathbb{R})$ modulo H_P .
Soit $\mathcal{Sc}_P$ *l'ensemble des produits scalaires* $f_{P,U}$ *avec* $U \in O_n(\mathbb{R})$ *et définis pour tout* $(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n$ *par* $f_{D,U}(X, Y) = {}^tX\, {}^tU D_P U Y$.
Alors l'application $\varphi_P : \mathcal{T}_P \to \mathcal{Sc}_P$ *définie par* $\varphi_P(U) := f_{D_P, U}$ *est bijective.*
Soit $\mathcal{Q} := \{ (P, U) \in (\mathcal{P}_+, O_n(\mathbb{R})) \mid U \in \mathcal{T}_P \}$. *Soit toujours* $\varphi : (\mathcal{P}_+ \times O_n(\mathbb{R})) \to \mathcal{Sc}$ *défini par* $\varphi(P, U) = f_{P,U}$.
Il suit de ce qui précède que la restriction ψ *de* φ *à* $\mathcal{Q}$ *est une bijection de* $\mathcal{Q}$ *sur* $\mathcal{Sc}$.

Démonstration
C'est une conséquence des propositions 2, 3, 4, 5.

3. Un système de représentants des produits scalaires. dans le cas $n=2$.

C'est donc l'égalité
(5) $\quad {}^tW\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} W=\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$ où $W:=UV^{-1}\in O_2(\mathbb{R})$.
3.1) Le cas $d_1=d_2$ est trivial puisque
$f(X,Y)={}^tX\,{}^tU\begin{bmatrix} d_1 & 0 \\ 0 & d_1 \end{bmatrix}UY$, comme ${}^tUU=I_2$, on a $f(X,Y)=d_1\,{}^tXY$.
3.2) On suppose maintenant que $d_1\neq d_2$.
On sait que $W=\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}\in SO_2(\mathbb{R})$ ou
$W=\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}\in O_2(\mathbb{R})-SO_2(\mathbb{R})$ avec $\theta\in[0,2\pi[$.
Ainsi (5) peut s'écrire
$\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}=\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$ ou
$\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}=\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$.
Comme $d_1\neq d_2$, il suit que W est élément du sous-groupe H de $O_2(\mathbb{R})$ défini par
$H:=\{I_2,-I_2,\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\}$ et donc
${}^tU\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}U={}^tV\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}V$ si et seulement si $U=WV$ avec $W\in H$.
Ce qui se traduit par
${}^tU\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}U={}^tV\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$ si et seulement si U et V sont dans la même classe à droite de $O_2(\mathbb{R})$ modulo H .
Il est alors facile de montrer que
$\{\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}\mid\theta\in[0,\pi[\}$ est un système de représentants des classes à droite de $O_2(\mathbb{R})$ modulo H .
Soient $\theta\in[0,\pi[$, $\mathcal{T}:=\{(d_1,d_2)\in\mathbb{R}^2\mid d_1>d_2>0\}$, $f_{\theta;d_1,d_2}$ le produit

scalaire défini sur $\mathbb{R}^2 \times \mathbb{R}^2$ par
$f_{\theta;d_1,d_2}(X,Y) = {}^tX \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} Y$.
Soit $\mathcal{Sc}$ l'ensemble des produits scalaires sur $\mathbb{R}^2 \times \mathbb{R}^2$ qui ne sont pas multiples du produit scalaire canonique, i.e. $(X,Y) \mapsto d\,{}^tXY$ avec $d>0$.
Alors l'application $\varphi : [\,0\,,\,\pi\,[\times \mathcal{T} \to \mathcal{Sc}$ définie par
$\varphi(\theta\,;(d_1,d_2)\,] := f_{\theta;d_1,d_2}$ est une bijection .

Remarque. Le paragraphe 2 peut, en prenant quelques précautions s'adapter facilement pour rechercher un système de représentants des formes quadratiques non dégénérées sur $\mathbb{R}^n \times \mathbb{R}^n$.

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

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.
On notera $\mathbb{Z}$ (resp. $\mathbb{Q}$) le groupe additif $(\mathbb{Z},+)$ (resp. $(\mathbb{Q},+)$)

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 $G=\underset{m\geq 1}{\cup} G_m$,*
iii) le groupe G est isomorphe à un sous-groupe de $\frac{\mathbb{Q}}{\mathbb{Z}}$.

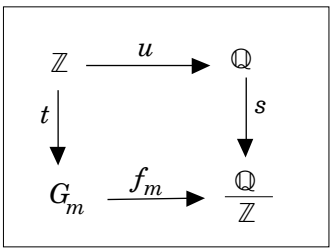
Démonstration
1) Montrons *ii)* implique *i)*.
Comme $G=\underset{m\geq 1}{\cup} G_m$, il suit que tout élément de G est d'ordre fini.
Soit K un sous-groupe fini de G. Comme $G=\underset{m\geq 1}{\cup} G_m$ et que la réunion est croissante, il existe m avec $K\subset G_m$, sachant que G_m est cyclique, 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
$$o(u x + v y) = \mathrm{ppcm}(o(x), o(y)) = \mathrm{ppcm}(d_1, d).$$
Or $\mathrm{ppcm}(o(x), o(y)) \mid m!$, ainsi $u x + v y \in G_m$. Par définition de y, on a $\mathrm{ppcm}(d_1, d) \leq d$, 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 $u(z):=\frac{z}{d_m}$, $t:\mathbb{Z}\to G_m$ est 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 $1 = \operatorname{pgcd}(q_1 , q_2 , \ldots , q_r)$, 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

$\frac{a}{N}=a_1\frac{q_1}{N}+a_2\frac{q_2}{N}+\ ...+a_r\frac{q_r}{N}$, 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 $s(\frac{a}{N})\in K_{p_1}+K_{p_2}+...+K_{p_r}$. 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 $0=x_1+x_2+...+x_r$ avec $p_i^{\beta_i}x_i=0$. Comme $1=\text{pgcd}(p_1^{\beta_1},p_2^{\beta_2}p_3^{\beta_3}...p_r^{\beta_r})$, par Bézout, il existe $u,v\in\mathbb{Z}$ avec $1=u\,p_1^{\beta_1}+v\,p_2^{\beta_2}p_3^{\beta_3}...p_r^{\beta_r}$; il suit de cela que $0=(1-u\,p_1^{\beta_1})\,x_1+\ v\,p_2^{\beta_2}p_3^{\beta_3}...p_r^{\beta_r}\,(x_2+x_3+...+x_r)$, i.e. $0=x_1$. On montre de même que $0=x_i$ pour $2\le i\le r$. 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 $m\in\mathbb{N}$, $m\ge 1$, $G_m:=\{x\in K\mid x^{m!}=1\}$ où $m!:=1.2.....m$. Alors on a*

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

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 $p\ge 2$ 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 $p\ge 2$ 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-groupes 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* $o(t)=n$, $o(s)=2$, $sts^{-1}=t^{-1}$.

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 $1 = \text{pgcd}(\alpha, u)$ et $pz = \alpha x$.
Supposons $1 = \text{pgcd}(\alpha, up)$. Il existe donc $\gamma \in \mathbb{Z}$ tel que $\alpha\gamma \equiv 1 \text{ modulo } (up\mathbb{Z})$; ainsi $1 = \text{pgcd}(\gamma, up)$ et donc $o(\gamma z) = up$; de plus $p(\gamma z) = x$. Ainsi $y := \gamma z$ convient.
Supposons $1 \neq \text{pgcd}(\alpha, up)$, sachant que $1 = \text{pgcd}(\alpha, u)$ cela veut dire que $p \mid \alpha$ et donc $p \nmid u$. Il suit de cela que sachant que $1 = \text{pgcd}(\alpha, u)$, cela veut dire que $1 = \text{pgcd}(\alpha + u, up)$.
Il existe donc $\gamma \in \mathbb{Z}$ tel que $(\alpha + u)\gamma \equiv 1 \text{ modulo } (up\mathbb{Z})$; ainsi $1 = \text{pgcd}(\gamma, up)$; 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 $c = p_1 p_2 \ldots p_r$ 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 , $C_0, C_1, \ldots, C_r$ 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 $o(y_{i+1}) = p_{i+1} (p_1 p_2 \ldots p_i a)$ 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*
$o(u x + v y) = \text{ppcm}(o(x), o(y))$.

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 128, ligne -2 avant 2.2) enlever ")"

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 $\mathfrak{S}_n$ et $\mathfrak{A}_n$)
1. *Le groupe* $\mathfrak{S}_n$ *est engendré par* $(1, 2, \ldots, n)$ *et* $(n-1, n)$ *; ainsi le nombre minimal de générateurs de* $\mathfrak{S}_n$ *est* 2 *pour* $n \geq 3$ *. Le groupe* $\mathfrak{S}_n$ *est aussi engendré par* $(2, \ldots, n)$ *et* $(1, 2)$ *. Ainsi* $r(\mathfrak{S}_n) = 2$ *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 $H\cap\mathbb{Z}x_1=\mathbb{Z}ax_1$. Il reste à montrer que
$H=\mathbb{Z}ax_1+\mathbb{Z}h_1+\mathbb{Z}h_2+\ldots+\mathbb{Z}x_k$. L'inclusion
$\mathbb{Z}ax_1+\mathbb{Z}h_1+\mathbb{Z}h_2+\ldots+\mathbb{Z}h_k\subset H$ 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

$$h-(\lambda_1h_1+\lambda_2h_2+\ldots+\lambda_kh_k)\in H\cap(\ker\rho)=H\cap\mathbb{Z}x_1=\mathbb{Z}ax_1\ ,$$

ce qui veut dire que $h-(\lambda_1h_1+\lambda_2h_2+\ldots+\lambda_kh_k)=\mu\ (ax_1)$. Cela montre $H\subset\mathbb{Z}ax_1+\mathbb{Z}h_1+\mathbb{Z}h_2+\ldots+\mathbb{Z}x_k$.
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 $x\longmapsto hx$; 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 $o(G)=16$, $o(a)=4$, $o(b)=o(c)=2$, $ab=ba$, $bc=cb$ et $cac^{-1}=ab$.*
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 $c\,a\,c^{-1} = a\,b$ 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, $n := r(G)$, $(x_1, x_2, \ldots, x_n)$ 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) $\quad (x_1)^{\alpha_1} (x_2)^{\alpha_2} \dots (x_n)^{\alpha_n} = (x_1)^{\beta_1} (x_2)^{\beta_2} \dots (x_n)^{\beta_n}$.
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 $\operatorname{pgcd}(\alpha_k - \beta_k, o(x_k)) = 1$, 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 $h \mapsto a\,h\,a^{-1}$. 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) $\quad a\,e_1 = e_1\,a$, $a\,e_2 = e_2\,a$, $a\,e_3 = e_2\,e_3\,a$.

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 $aca^{-1} = bc$.
Or $aca^{-1} = bc$ 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 $aca^{-1} = bc$ 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 131, complément, **quand tout groupe d'ordre n est commutatif** (resp. **cyclique**)

Introduction

Si $n \geq 1$ est un entier, notre question est de savoir si tout groupe d'ordre n est abélien.
Le résultat de cette question est un article de Dickson de 1905 ([D]) qui repose partiellement sur des résultats de Miller et Morena [M.-M.] qui déterminent les groupes non abéliens dans lesquels tout sous-groupe strict est abélien.
Si $n \geq 1$ est un entier, on peut aussi chercher à savoir si tout groupe d'ordre n est cyclique. Ce cas a été traité par Szele en 1947 ([S]), curieusement ce dernier ne semble pas faire allusion au théorème de Dickson.
Conrad ([C]) a aussi traité le cas des groupes cycliques.

Nous reprenons ici le résultat de Dickson (théorème 1) et celui de Szele (théorème 2) en utilisant essentiellement les ingrédients de Conrad, i.e. la structure des groupes abéliens finis, la structure des produits semi-directs de groupes et la technique de groupe opérant sur un ensemble.

Définition 1 (la propriété (*)) Soit $n \in \mathbb{N}$, avec $n \geq 2$, on dit que n satisfait *la propriété* $(*)$ *si* $n = p_1^{e_1} p_2^{e_2} \ldots p_s^{e_s}$ *avec* $p_i > 0$, *premiers,* $p_i \neq p_j$ *si* $i \neq j$, $1 \leq e_i \leq 2$ *et si pour* $s \geq 2$, *pour tout* $i \neq j$, *on a* $p_j \nmid (p_i^{e_i} - 1)$.

Remarque 1 Soient $n \geq 2$ un entier qui satisfait la propriété $(*)$, $m \geq 2$ avec $m \mid n$. Alors m satisfait la propriété $(*)$.

Théorème 1 ([D]) *Soit* $n \in \mathbb{N}$, $n \geq 2$. *Alors les propriétés suivantes sont équivalentes.*
i) L'entier n *satisfait la propriété* $(*)$,
ii) tout groupe G *avec* $o(G) = n$ *est abélien.*

Démonstration
A. *Montrons que* non *i) implique* non *ii).*
On suppose que $n = p_1^{e_1} p_2^{e_2} \ldots p_s^{e_s}$ *avec* $p_i > 0$, *premiers,* $p_i \neq p_j$ *si* $i \neq j$.

A.1) Supposons qu'il existe i avec $e_i \geq 3$, par exemple $e_1 \geq 3$ et posons $p = p_1$. Soient $\mathbb{F}_p$ le corps à p éléments, K le sous-groupe de $G\ell_3(\mathbb{F}_p)$ défini par

$$K := \left\{ \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \in G\ell_3(\mathbb{F}_p) \mid x, y, z \in \mathbb{F}_p \right\},$$

alors K est un groupe d'ordre p^3 et facilement $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ et $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$ ne commutent pas . Ainsi K est un groupe non abélien d'ordre p^3.
Si donc $e_1 = 3$, le groupe

$$G := K \times (\frac{\mathbb{Z}}{p_2^{e_2}\mathbb{Z}}, +) \times \ldots \times (\frac{\mathbb{Z}}{p_s^{e_s}\mathbb{Z}}, +)$$

est donc non abélien d'ordre $n = p_1^3 p_2^{e_2} \ldots p_s^{e_s}$.

Si $e_1 > 3$, le groupe

$$G = K \times (\frac{\mathbb{Z}}{p_1^{e_1-3}\mathbb{Z}}, +) \times (\frac{\mathbb{Z}}{p_2^{e_2}\mathbb{Z}}, +) \times \ldots \times (\frac{\mathbb{Z}}{p_s^{e_s}\mathbb{Z}}, +)$$

est non abélien d'ordre $n = p_1^{e_1} p_2^{e_2} \ldots p_s^{e_s}$.

A.2) On suppose maintenant que $1 \le e_i \le 2$ pour $1 \le i \le s$ et par exemple que $p_2 \mid p_1^{e_1} - 1$.
Il suit alors du lemme 1 et du corollaire du lemme 2 (ci-après) appliqué à $q = p_1$, $r = e_1$, $m = p_2$ et $k = 1$ si $e_2 = 1$, $k = 2$ si $e_2 = 2$ qu'il existe un groupe K d'ordre $p_1^{e_1} p_2^{e_2}$ non abélien. Il suit alors que

$$G = K \times (\frac{\mathbb{Z}}{p_1^{e_3}\mathbb{Z}}, +) \times (\frac{\mathbb{Z}}{p_4^{e_4}\mathbb{Z}}, +) \times \ldots \times (\frac{\mathbb{Z}}{p_s^{e_s}\mathbb{Z}}, +)$$

est un groupe d'ordre $n = p_1^{e_1} p_2^{e_2} \ldots p_s^{e_s}$ qui est non abélien.

Il suit que A. est satisfait.

B. *On suppose que i) est satisfait, montrons que ii) est satisfait.*

Supposons le contraire, i.e. qu'il existe un groupe qui satisfait *i)* et qui n'est pas abélien.
Compte tenu de la remarque 1, on peut supposer qu'il existe un groupe G avec la propriété suivante que l'on note (**).

(**) *Il existe un groupe G non abélien avec $n = o(G)$, n qui satisfait i) et tout groupe H avec $o(H) = m$, $m \mid n$, $m \neq n$ est abélien.*

B.1) *Soit toujours G un groupe qui satisfait* (**) . On dit qu'un sous-groupe U de G est *maximal*, si $U \neq G$ et si H est un sous-groupe avec $U \subset H \subset G$, on a $H = U$ ou $H = G$.
Comme G est un groupe qui satisfait (**) , on a $n \ge 2$ et si e est l'élément neutre de G , alors tout élément $x \neq e$ est contenu dans un sous-groupe maximal ; en particulier un sous-groupe maximal est différent de $\{e\}$.

Soient U et V des sous-groupes maximaux de G . Montrons que $U = V$ ou $U \cap V = \{e\}$, ce qui veut aussi dire que $(U - \{e\}) = (V - \{e\})$ ou

$(U-\{e\})\cap(V-\{e\})=\emptyset$.

Supposons $U\cap V\neq\{e\}$, alors il existe $x\in U\cap V$ et $x\neq e$. Soit $C_G(x):=\{y\in G\mid yx=xy\}$, alors $C_G(x)$ est un sous-groupe de G . Comme par (**), U est commutatif, on a $U\subset C_G(x)$ et comme U est maximal, on a $C_G(x)=U$ ou $C_G(x)=G$.
Si $C_G(x)=G$, cela implique que $x\in Z(G)$, le centre de G . Si on avait $Z(G)=G$, cela contredit le fait que G n'est pas abélien. Soient donc $y\in G-Z(G)$ et $H:=\{zy^k\mid z\in Z(G)$ et $k\in\mathbb{Z}\}$. Facilement H est un sous-groupe de G avec $U\subset Z(G)\subset H\subset G$; comme U est maximal et $Z(G)\neq H$, on a $H=G$. Facilement H est commutatif, ce qui contredit (**).
Par une méthode identique, on a $C_G(x)=V$. Et ainsi $U=V$.

B.2) *Soit toujours G un groupe qui satisfait* (**), *soit U un sous-groupe maximal de G, $u:=o(U)$. Montrons que*

$$\mathrm{card}\Big(\bigcup_{g\in G}(gUg^{-1})\Big)=1+n-\frac{n}{u}\ .$$

Soit $\mathcal{M}$ l'ensemble des sous-groupes maximaux de G . Alors G opère sur $\mathcal{M}$ par $(g,U)\to gUg^{-1}$; en effet si U est maximal, il suit que gUg^{-1} est aussi maximal. Si donc $U\in\mathcal{M}$, le stabilisateur de U est

$$\mathrm{Stab}(U):=\{g\in G\mid gUg^{-1}=U\}\ .$$

On montrera en B.3) que $U=\mathrm{Stab}(U)$; c'est la partie la plus délicate de la démonstration.
On suppose donc que $\mathrm{Stab}(U)=U$.
Il suit alors que $\mathrm{card}(\text{orbite de } U)=\frac{n}{u}=:s$. Il existe donc $g_1,g_2,\ldots,g_s\in G$ tels que

$$\text{orbite de } U=\{g_1Ug_1^{-1},g_2Ug_2^{-1},\ldots,g_sUg_s^{-1}\}\ .$$

Comme $g_iUg_i^{-1}\neq g_jUg_j^{-1}$ pour $i\neq j$, il suit de B.1) que

$$g_iUg_i^{-1}\cap g_jUg_j^{-1}=\{e\}\ \text{ pour }\ i\neq j\ .$$

Ce qui se traduit par

$$g_i(U-\{e\})g_i^{-1}\cap g_j(U-\{e\})g_j^{-1}=\emptyset\ \text{ pour }\ i\neq j\ .$$

Soit donc

$$\mathcal{A}:=g_1(U-\{e\})g_1^{-1}\cup g_2(U-\{e\})g_2^{-1}\cup\ldots\cup g_s(U-\{e\})g_s^{-1},$$

il suit de ce qui précède que $\mathcal{A}$ est la réunion disjointe,

$$\mathcal{A} := g_1 (U - \{e\}) g_1^{-1} \cup g_2 (U - \{e\}) g_2^{-1} \cup \ldots \cup g_s (U - \{e\}) g_s^{-1},$$

et donc

$$\text{card } \mathcal{A} = s(u-1) = n - \frac{n}{u}.$$

Sachant que $\mathcal{A} \subset G - \{e\}$ et que $n - \frac{n}{u} < n - 1$, cela montre que le nombre d'orbites de $\mathcal{M}$ sous l'action de G est au moins 2. Ainsi, il existe un sous-groupe maximal V tel que $(V - \{e\}) \cap \mathcal{A} = \emptyset$; sinon, cela voudrait dire qu'il existe i avec $1 \le i \le s$ tel que $g_i (U - \{e\}) g_i^{-1} \cap (V - \{e\}) \neq \emptyset$.
Il suivrait alors que $g_i (U - \{e\}) g_i^{-1} = V$ et donc $\text{orbite}(U) = \text{orbite}(V)$.
Ainsi pour tout $gUg^{-1} \in \text{orbite}(U)$ et $g'Ug'^{-1} \in \text{orbite}(V)$, on a

$$g(U - \{e\}) g^{-1} \cap g'(V - \{e\}) g'^{-1} = \emptyset.$$

On a

$$\text{orbite de } V = \{ h_1 V h_1^{-1}, h_2 V h_2^{-1}, \ldots, h_t V h_t^{-1} \}.$$

avec $t = \frac{n}{v}$ et $v = o(V)$.
Soit

$$\mathcal{B} := h_1 (V - \{e\}) h_1^{-1} \cup (h_2 (V - \{e\}) h_2^{-1} \cup \ldots \cup h_t (V - \{e\}) h_t^{-1},$$

il suit de ce qui précède que $\mathcal{B}$ est la réunion disjointe,

$$\mathcal{B} := h_1 (V - \{e\}) h_1^{-1} \cup h_2 (V - \{e\}) h_2^{-1} \cup \ldots \cup h_t (V - \{e\}) h_t^{-1},$$

et aussi que $\mathcal{A} \cap \mathcal{B} = \emptyset$, ce qui montre que

$$\text{card } \mathcal{B} = n - \frac{n}{v},$$

et

$$\text{card}(\mathcal{A} \cup \mathcal{B}) = (n - \frac{n}{u}) + (n - \frac{n}{v}).$$

Sachant que

$$\mathcal{A} \cup \mathcal{B} \subset G - \{e\},$$

il suit que

$$(n - \frac{n}{u}) + (n - \frac{n}{v}) \le n - 1,$$

ce qui donne une contradiction puisque $u \ge 2$, $v \ge 2$.

B.3) *Soit U un sous-groupe maximal de G satisfaisant* (**). *Il s'agit de montrer que* $U = \{y \in G \mid yUy^{-1} = U\}$.

Supposons le contraire, comme U est maximal et que
$U \subset \{y \in G \mid yUy^{-1} = U\}$, cela veut dire que

$G=\{y\in G \mid yUy^{-1}=U\}$, i.e. que U est distingué dans G .

B.3.1) *Montrons que* $\frac{G}{U}$ *est un groupe cyclique d'ordre* p *, avec* p *premier.*
On a $o(\frac{G}{U})\neq 1$, si donc $\rho: G\to\frac{G}{U}$ est la surjection canonique, il existe $y\in G$ tel que $o(\rho(y))=p$ avec p premier. Montrons que

$$G=\{hy^k \mid h\in U \text{ et } k\in\mathbb{Z}\} .$$

Sachant que U est distingué dans G , on a en particulier $yUy^{-1}=U$ et aussi $y^kUy^{-k}=U$ pour tout $k\in\mathbb{Z}$. Il suit facilement de cela que $\{hy^k \mid h\in U \text{ et } k\in\mathbb{Z}\}$ est un sous-groupe de G avec

$$U\subset\{hy^k \mid h\in U \text{ et } k\in\mathbb{Z}\} \text{ et } U\neq\{hy^k \mid h\in U \text{ et } k\in\mathbb{Z}\} .$$

Sachant que U est maximal, on a donc $G=\{hy^k \mid h\in U \text{ et } k\in\mathbb{Z}\}$. Il suit de cela que $\frac{G}{U}$ est le groupe cyclique d'ordre p engendré par $\rho(y)$.

B.3.2) *Sur l'ordre de* G *et l'ordre de* U *.*
Par (*) si $n:=o(G)$, on a $n=p_1^{e_1}p_2^{e_2}\dots p_s^{e_s}$ *avec* $p_i>0$ *, premiers,* $p_i\neq p_j$ *si* $i\neq j$, $1\leq e_i\leq 2$ *et si* $s\geq 2$ *, pour tout* $i\neq j$ *, on a* $p_j\nmid(p_i^{e_i}-1)$.
Si $m:=o(U)$, il suit de B.3.1) que $n=mp$. Ainsi $m=(q_1q_2\dots q_r)^2(r_1r_2\dots r_t)$ où $\{q_1,q_2,\dots,q_r,r_1,r_2,\dots,r_t\}$ est un ensemble de $r+t$ premiers (distincts).
Comme $n=(q_1q_2\dots q_r)^2(r_1r_2\dots r_t)p$, il suit de (*) que $p\notin\{q_1,q_2,\dots,q_r\}$.
On a donc deux possibilités
(1) $p\notin\{r_1,r_2,\dots,r_t\}$, ainsi $n=(q_1q_2\dots q_r)^2(r_1r_2\dots r_tp)$,
(2) $p\in\{r_1,r_2,\dots,r_t\}$, ainsi $n=(q_1q_2\dots q_rp)^2(r_2\dots r_t)$, si $p=r_1$.

B.3.3) *Un automorphisme de* U *.*

Soit τ l'automorphisme de U défini pour tout $z\in U$ par $\tau(z):=yzy^{-1}$, où y est défini en B.3.1). On a donc $\tau^p=\mathrm{Id}_U$ puisque $y^p\in U$ et que U est commutatif par (**).

L'objectif consistera à montrer que $\tau=\mathrm{Id}_U$.

B.3.4) *On a* $U\simeq\mathbb{Z}\omega_1$ i.e. U *est cyclique ou* $U\simeq\mathbb{Z}\omega_1\oplus\mathbb{Z}\omega_2$ *avec* $o(\omega_1)\mid o(\omega_2)$ *et* $1<o(\omega_1)$.

Puisque $o(U)<o(G)$, on sait par (**) que U est commutatif. Ainsi $U\simeq \mathbb{Z}\,\omega_1\oplus\mathbb{Z}\,\omega_2\oplus\ldots\oplus\mathbb{Z}\,\omega_k$ avec $o(\omega_1)\mid o(\omega_2)\mid\ldots\mid o(\omega_k)$, $1<o(\omega_1)$ et la suite $(o(\omega_1),o(\omega_2),\ldots,o(\omega_k))$ est unique ([F. M. 2.] théorème 1 p. 123). Il existe donc un premier π avec $\pi\mid o(\omega_1)$, il suit que $\pi^k\mid o(U)$, il suit donc de (**) que $1\le k\le 2$.

B.3.5) *On suppose que* $U\simeq\mathbb{Z}\,\omega_1$ i.e. U *est cyclique.*
Soit $m=o(U)$, il suit donc de B.3.2) que $m=(q_1q_2\ldots q_r)^2(r_1r_2\ldots r_t)$ où $\{q_1,q_2,\ldots,q_r,r_1,r_2,\ldots,r_t\}$ est un ensemble de $r+t$ premiers (distincts). On sait que $\mathrm{Aut}(U)\simeq(\frac{\mathbb{Z}}{m\mathbb{Z}})^\times$.
Il suit du théorème des restes chinois que

$$U\simeq(\prod_{i=1}^{r}(\frac{\mathbb{Z}}{q_i^2\mathbb{Z}},+))\times(\prod_{i=1}^{t}(\frac{\mathbb{Z}}{r_i\mathbb{Z}},+)),$$

et donc

$$\mathrm{Aut}(U)\simeq(\prod_{i=1}^{r}(\frac{\mathbb{Z}}{q_i^2\mathbb{Z}})^\times)\times(\prod_{i=1}^{t}(\frac{\mathbb{Z}}{r_i\mathbb{Z}})^\times).$$

Or $o((\frac{\mathbb{Z}}{q_i^2\mathbb{Z}})^\times)=q_i(q_i-1)$ et $o((\frac{\mathbb{Z}}{r_i\mathbb{Z}})^\times)=r_i-1$. Il reste à montrer que $p\nmid q_i(q_i-1)$ et $p\nmid r_i-1$. Cela résulte du fait que $n=mp$, de (1) et (2) et que n satisfait (*).
Ainsi donc l'automorphisme τ défini en B.3.3) est l'identité sur U ; il suit alors de B.3.1) que G est commutatif, ce qui est une contradiction.

B.3.6) *On suppose que* $U\simeq\mathbb{Z}\,\omega_1\oplus\mathbb{Z}\,\omega_2$ avec $a=o(\omega_1)$, $a\,b=o(\omega_2)$.

Comme $n=o(G)$ avec $n=o(U)p$ d'après B.3.1) , ainsi $n=a^2bp$. Sachant que n satisfait (*) on a $p\nmid a$, $1=\mathrm{pgcd}(a,b)$. On a donc

$$U\simeq((\frac{\mathbb{Z}}{a\mathbb{Z}},+)\times(\frac{\mathbb{Z}}{a\mathbb{Z}},+))\times(\frac{\mathbb{Z}}{b\mathbb{Z}},+),$$

sachant que $1=\mathrm{pgcd}(a,b)$, on a

$$\mathrm{Aut}(U)\simeq\mathrm{Aut}((\frac{\mathbb{Z}}{a\mathbb{Z}},+)\times(\frac{\mathbb{Z}}{a\mathbb{Z}},+))\times\mathrm{Aut}(\frac{\mathbb{Z}}{b\mathbb{Z}},+).$$

Enfin, on peut écrire $b=c^2d$, encore avec $1=\mathrm{pgcd}(c,d)$ compte tenu de (*) pour n . Il suit alors que

$$\mathrm{Aut}(U)\simeq\mathrm{Aut}((\frac{\mathbb{Z}}{a\mathbb{Z}},+)\times(\frac{\mathbb{Z}}{a\mathbb{Z}},+))\times\mathrm{Aut}((\frac{\mathbb{Z}}{c^2\mathbb{Z}},+))\times\mathrm{Aut}((\frac{\mathbb{Z}}{d\mathbb{Z}},+)).$$

On peut aussi écrire $a=a_1a_2...a_r$, $c=c_1c_2...c_s$, $d=d_1d_2...d_t$ où $\{a_1,a_2,...,a_r,c_1,c_2,...,c_s,d_1,d_2,...,d_t\}$ est un ensemble de $r+s+t$ premiers (distincts). Ainsi

$\mathrm{Aut}((\frac{\mathbb{Z}}{a\mathbb{Z}},+)\times(\frac{\mathbb{Z}}{a\mathbb{Z}},+))\simeq\prod_{i=1}^{r} G\ell_2(\frac{\mathbb{Z}}{a_i\mathbb{Z}})$, $\mathrm{Aut}((\frac{\mathbb{Z}}{c^2\mathbb{Z}}))\simeq\prod_{i=1}^{s}(\frac{\mathbb{Z}}{c_i^2\mathbb{Z}})^{\times}$,

$\mathrm{Aut}((\frac{\mathbb{Z}}{d\mathbb{Z}}))\simeq\prod_{i=1}^{t}(\frac{\mathbb{Z}}{d_i\mathbb{Z}})^{\times}$.

Ensuite, on a $o(G\ell_2(\frac{\mathbb{Z}}{a_i\mathbb{Z}}))=(a_i^2-1)(a_i^2-a_i)$,

$o((\frac{\mathbb{Z}}{c_i^2\mathbb{Z}})^{\times})=c_i(c_i-1)$, $o((\frac{\mathbb{Z}}{d_i\mathbb{Z}})^{\times})=d_i-1$.

Sachant que $n=(a_1a_2...a_r)^2(c_1c_2...c_s)^2(d_1d_2...d_t).p$ satisfait (*), on a $p\nmid a_i$, $p\nmid c_i$ et en plus $p\nmid(a_i-1)$, $p\nmid(c_i-1)$, $p\nmid(d_i-1)$, il suit que $p\nmid o(\mathrm{Aut}(U))$. Ainsi l'automorphisme τ défini en B.3.3) est l'identité sur U ; il suit alors de B.3.1) que G est commutatif, ce qui est une contradiction.

Définition 2 (la propriété (***)) Soit $n\in\mathbb{N}$, avec $n\geq 2$, on dit que n satisfait *la propriété* $(***)$ *si* $n=p_1p_2...p_s$ *avec* $p_i>0$ *, premiers,* $p_i\neq p_j$ *, si* $i\neq j$*, et si* $s\geq 2$ *, pour tout* $i\neq j$ *, on a* $p_j\nmid(p_i-1)$.
Cette propriété (***) est équivalente à $1=\mathrm{pgcd}(n,\varphi(n))$ où $\varphi(n)$ est l'indicateur d'Euler de n .

Remarque 2 Soient $n\geq 2$ un entier qui satisfait la propriété $(***)$, alors n satisfait la propriété $(*)$.

Remarque 3 Soient $n\geq 2$ un entier qui satisfait la propriété $(***)$, $m\geq 2$ avec $m\mid n$. Alors m satisfait la propriété $(***)$.

Théorème 2 ([S] , [C]) *Soit* $n\in\mathbb{N}$ *, avec* $n\geq 2$ *. Alors les propriétés suivantes sont équivalentes.*
i) L'entier n *satisfait la propriété* (***) ,
ii) tout groupe G *avec* $o(G)=n$ *est cyclique.*

Démonstration

A) *Momtrons que i) implique ii).*

Comme (***) implique (*) , il suit du théorème 1 que G est abélien on a donc $G \simeq \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \oplus ... \oplus \mathbb{Z}\omega_k$ avec $o(\omega_1) \mid o(\omega_2) \mid ... \mid o(\omega_k)$, $1 < o(\omega_1)$ et la suite $(o(\omega_1), o(\omega_2), ..., o(\omega_k))$ est unique ([F. M. 2.] théorème 1 p. 123). Si donc p est un premier avec $p \mid o(\omega_1)$, on a $p^k \mid n$. Il suit alors de (***) que $k = 1$ et donc que G est cyclique.

B) *Montrons que* non *i) implique* non *ii).*

Non (***) veut dire que $n = p_1^{e_1} p_2^{e_2} ... p_s^{e_s}$ avec $p_i > 0$, premiers, $p_i \neq p_j$ si $i \neq j$ et qu'il existe ℓ , avec $e_\ell \geq 2$, ou que si $n = p_1 p_2 ... p_s$ avec $p_i > 0$, premiers, $p_i \neq p_j$ si $i \neq j$, il existe $i \neq j$, avec $p_j \mid (p_i - 1)$.

B.1) *Si par exemple* $e_1 \geq 2$.

Soit

$$G = (\frac{\mathbb{Z}}{p_1\mathbb{Z}}, +)^{e_1} \times (\frac{\mathbb{Z}}{p_2\mathbb{Z}}, +)^{e_2} \times ... \times (\frac{\mathbb{Z}}{p_s\mathbb{Z}}, +)^{e_s} ,$$

on a donc $o(G) = n = p_1^{e_1} p_2^{e_2} ... p_s^{e_s}$ et pour tout $x \in G$ on a $o(x) \mid p_1 p_2 ... p_s < n$, ce qui contredit le fait que G est cyclique.

B.2) *On suppose que* $n = p_1 p_2 ... p_s$ et que $p_1 \mid p_2 - 1$.

On sait que $\mathrm{Aut}((\frac{\mathbb{Z}}{p_2\mathbb{Z}}, +)) \simeq (\frac{\mathbb{Z}}{p_2\mathbb{Z}})^\times \simeq (\frac{\mathbb{Z}}{(p_2 - 1)\mathbb{Z}}, +)$.

Comme $p_1 \mid p_2 - 1$, il existe un homomorphisme $\tau : (\frac{\mathbb{Z}}{p_1\mathbb{Z}}, +) \to \mathrm{Aut}((\frac{\mathbb{Z}}{p_2\mathbb{Z}}, +))$ qui est injectif. Ainsi $\tau((\frac{\mathbb{Z}}{p_1\mathbb{Z}}, +)) \neq \{\mathrm{Id}\}$ où Id est l'automorphisme de $(\frac{\mathbb{Z}}{p_2\mathbb{Z}}, +)$ qui est l'identité, il suit alors du lemme 2, ci-après que $K := (\frac{\mathbb{Z}}{p_2\mathbb{Z}}, +) \times_\tau (\frac{\mathbb{Z}}{p_1\mathbb{Z}}, +)$ est un groupe qui n'est pas abélien et que $o(K) = p_1 p_2$. Ainsi

$$G := K \times (\frac{\mathbb{Z}}{p_3\mathbb{Z}}, +) \times ... \times (\frac{\mathbb{Z}}{p_s\mathbb{Z}}, +)$$

est un groupe d'ordre $n=p_1p_2...p_s$ qui n'est pas abélien, donc qui n'est pas cyclique.

Définition 3 (produit semi-direct) ([Fr.] définition 1.5.1 , p. 24, [F. M. 1.] ex. 54 p. 139) Soient F et G deux groupes, $\mathrm{Aut}(F)$ le groupe des automorphismes de F , $\tau:G\to\mathrm{Aut}(F)$ un homorphisme de groupes. On appelle *produit semi-direct de G par F relativement à τ* l'ensemble $F\times G$ muni de la loi de composition défini par

$$((f,g),(f',g'))\mapsto(f\,\tau(g)(f'),gg').$$

Ce produit semi-direct se note $F\times_\tau G$.

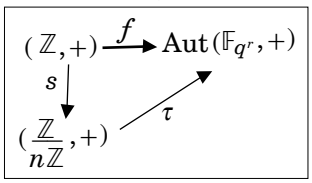
Lemme 1 *Soient F et G deux groupes, $\mathrm{Aut}(F)$ le groupe des automorphismes du groupe F , $\tau:G\to\mathrm{Aut}(F)$ un homomorphisme de groupes.*
Alors les propriétés suivantes sont équivalentes.
i) Le produit semi-direct $F\times_\tau G$ est un groupe abélien,
ii) le groupe F est abélien, le groupe G est abélien et $\tau(G)=\{\mathrm{Id}_F\}$.

Démonstration
i) implique ii) Comme $F\times_\tau G$ est abélien, F qui est isomorphe à un sous-groupe de $F\times_\tau G$ est abélien et G qui est isomorphe à un quotient de $F\times_\tau G$ est abélien.
Enfin, on a la relation $f\,\tau(g)(f')=f'\tau(g')(f)$; si donc $f=e$, l'élément neutre de F , on déduit que $\tau(g)(f')=f'$ ainsi $\tau(G)=\{\mathrm{Id}_F\}$.
ii) implique i) est immédiat.

Lemme 2 *Soient q un nombre premier, $r\geq1$, $\mathbb{F}_{q^r}$ le corps à q^r éléments, enfin m un entier avec $m\geq2$ et $m\mid q^r-1$. Soient les groupes additifs ,*
$(\frac{\mathbb{Z}}{m\mathbb{Z}},+)$ et $(\mathbb{F}_{q^r},+)$. Alors il existe un homomorphisme
$\tau:(\frac{\mathbb{Z}}{m\mathbb{Z}},+)\to\mathrm{Aut}((\mathbb{F}_{q^r},+))$ avec $\tau((\frac{\mathbb{Z}}{m\mathbb{Z}},+))\neq\{\mathrm{Id}\}$.

Démonstration
On a donc $a\in\mathbb{N}$ avec $m\,a=q^r-1$. Soient ξ un générateur du groupe multiplicatif $(\mathbb{F}_{q^r})^\times$, $z\in\mathbb{Z}$ et $f(z):(\mathbb{F}_{q^r},+)\to(\mathbb{F}_{q^r},+)$, défini pour tout

$x \in \mathbb{F}_{q^r}$ par $f(z)(x) := \xi^{az} x$. Alors $f(z)$ est un automorphisme du groupe $(\mathbb{F}_{q^r}, +)$ .Par ailleurs, l'application $f : (\mathbb{Z}, +) \to \mathrm{Aut}((\mathbb{F}_{q^r}, +))$ est un homomorphisme du groupe $(\mathbb{Z}, +)$ dans le groupe $\mathrm{Aut}((\mathbb{F}_{q^r}, +))$.



Soit $s : \mathbb{Z} \to \frac{\mathbb{Z}}{m\mathbb{Z}}$ la surjection canonique, facilement on a $\ker f = \ker s = m\mathbb{Z}$. Il suit de cela qu'il existe un homomorphisme injectif $\tau : (\frac{\mathbb{Z}}{m\mathbb{Z}}, +) \to \mathrm{Aut}((\mathbb{F}_{q^r}, +))$ tel que $f = \tau s$. En particulier $\tau((\frac{\mathbb{Z}}{m\mathbb{Z}}, +)) \neq \{\mathrm{Id}\}$ où Id est l'automorphisme identité de $(\mathbb{F}_{q^r}, +)$.

Corollaire *Soient q un nombre premier, $r \geq 1$, $\mathbb{F}_{q^r}$ le corps à q^r éléments, enfin m un entier avec $m \geq 2$, $m \mid q^r - 1$ et $k \geq 1$ un entier. Soient les groupes additifs , $(\frac{\mathbb{Z}}{km\mathbb{Z}}, +)$ et $(\mathbb{F}_{q^r}, +)$. Alors il existe un homomorphisme $\theta : (\frac{\mathbb{Z}}{km\mathbb{Z}}, +) \to \mathrm{Aut}(\mathbb{F}_{q^r}, +)$ avec $\theta((\frac{\mathbb{Z}}{km\mathbb{Z}}, +)) \neq \{\mathrm{Id}\}$. Ainsi le produit semi-direct $(\mathbb{F}_{q^r}, +) \times_\theta (\frac{\mathbb{Z}}{km\mathbb{Z}}, +)$ relativement à θ est un groupe d'ordre $km q^r$ qui n'est pas abélien.*

Démonstration

Il suit du lemme 2 qu'il existe un homomorphisme

$$\tau : (\frac{\mathbb{Z}}{m\mathbb{Z}}, +) \to \mathrm{Aut}((\mathbb{F}_{q^r}, +)) \text{ tel que } \tau((\frac{\mathbb{Z}}{m\mathbb{Z}}, +)) \neq \{\mathrm{Id}\} .$$

Soit $s : (\frac{\mathbb{Z}}{km\mathbb{Z}}, +) \to (\frac{\mathbb{Z}}{m\mathbb{Z}}, +)$ la surjection canonique et $\theta := s\tau$, alors

$$\theta : (\frac{\mathbb{Z}}{km\mathbb{Z}}, +) \to \mathrm{Aut}((\mathbb{F}_{q^r}, +))$$

est un homomorphisme de groupes avec

$$\theta((\frac{\mathbb{Z}}{km\mathbb{Z}}, +)) \neq \{\mathrm{Id}\} .$$

Il suit alors du lemme 1 que le produit semi-direct $(\mathbb{F}_{q^r}, +) \times_\theta (\frac{\mathbb{Z}}{km\mathbb{Z}}, +)$ relativement à θ est un groupe d'ordre $km q^r$ qui n'est pas abélien.

Bibliographie

[K] **Conrad K.** *When are all groups of order n cyclic ?* "Expository papers" https://kconrad.math.uconn.edu/blurbs

[D] **Dickson L.E.** *Definitions of a group and a field by independant postulates* Trans. Amer. Math. Soc. 6 (1905) 198- 204 URL

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

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

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

[M.-M.] **Miller A. and Morena C.** *Non-abelian groups in which every subgroup is abelian* Transactions of the American Mathematical Society oct. 1903, Vol. 4, n° 4 (Oct. 1903) pp. 350-404

[S] **Szele T.** *Über die endlichen Ordnungezahlen zu denen eine Gruppe gehört* Comm. Math. Helv 20 (1947) 265-267

page 133, ligne 2 du théorème 1.4, remplacer "les orbites de S sous cette" par "les orbites de S sous l'action de Σ"

page 136, ligne -2 avant la définition 2.5, lire "homomorphisme" au lieu de "homorphisme"

page 144, ligne -1, lire" proposition 5.3" au lieu de "proposition 1"

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 $(a_1,a_2,\dots,a_r)$ d'éléments de S telle que $a_1=x$, $a_r=y$ et $\{a_k,a_{k+1}\}$ est une arête pour $1\le k<r$.
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* $n\ge 2$, $\mathfrak{S}_n$ *le groupe des permutations de l'ensemble* $\{1,2,\dots,n\}$, 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* $\{1,2,\dots,n\}$ *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 $\sigma=(1,2,\dots,n)$.
De la même façon k est un sommet si $1\le k\le n$.
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 $A=\{1,2,\dots,n\}$. Supposons le contraire, on a donc $\{1,2,\dots,n\}=A\cup B$ 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 $\sigma=(1,2,\dots,n)$ et $\sigma^k(1)$ pour $1\le k\le n$.

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 $2\le k\le n$ puisque l'on sait que la famille $\{(1,k)\mid 2\le k\le n\}$ engendre $\mathfrak{S}_n$ (Fr.E. corollaire 2.2.1.3.4.).
Il suit du lemme ci-après qu'il existe un chemin $(b_1,b_2,\dots,b_s)$ qui relie 1 à k avec $1=b_1$, $k=b_s$, $b_1\notin\{b_2,b_3,\dots,b_s\}$ et $(b_i,b_{i+1})\in\Lambda$ pour $1\le i<s$.
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 $(b_1,b_2,\dots,b_s)$ avec $b_1=x$, $b_s=y$ et $b_1\notin\{b_2,b_3,\dots,b_s\}$.*

Démonstration Soit $(a_1,a_2,\dots,a_r)$ un chemin qui relie x à y , i.e. $x=a_1$, $y=a_r$ et $(a_i,a_{i+1})\in\Lambda$ pour $1\le i<r$. Comme $a_1\neq a_r$, il existe un plus grand entier $j<r$ tel que $a_j=a_1$. Ainsi $a_j\notin\{a_{j+1},a_{j+2},\dots,a_r\}$ et $(a_{j+1},a_{j+2},\dots,a_r)$ 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 $\{1,2,\dots,n\}$,
ii) $\{k\in\{1,2,\dots,n\}\mid t(k)=k \text{ pour tout } t\in\Lambda\}=\emptyset$.

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

p. 235 complément à IV.7.1. Sur le discriminant
(cet exercice nous a été suggéré par notre collègue Q. Liu)

1. Définition du discriminant d'un polynôme

Soient $(a_0,a_1,\dots,a_n)$ des variables sur $\mathbb{Z}$,
$P(X):=a_0X^n+a_1X^{n-1}+\dots+a_0\in\mathbb{Z}[a_0,a_1,\dots,a_n][X]$,
$P'(X):=n\,a_0X^{n-1}+(n-1)a_1X^{n-2}+\dots+a_{n-1}$.

Soit $\mathrm{res}_{n,n-1}(P(X),P'(X))$ l'élément de $\mathbb{Z}[a_0,a_1,\dots,a_n]$ défini par

$$\mathrm{res}_{n,n-1}(P(X),P'(X))=\begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} & a_n & & \\ & a_0 & a_1 & \dots & a_{n-1} & a_n & \\ & & a_0 & a_1 & \dots & a_{n-1} & a_n \\ n a_0 & (n-1)a_1 & \dots & a_{n-1} & & & \\ & n a_0 & (n-1)a_1 & \dots & a_{n-1} & & \\ & & & & & & \\ & & & n a_0 & (n-1)a_1 & \dots & a_{n-1} \end{bmatrix} \begin{matrix} \\ \\ \\ \Big\} n-1 \\ \\ \\ \Big\} n \end{matrix}$$

Facilement en considérant la première colonne on a

$$\mathrm{res}_{n,n-1}(P(X),P'(X))\in a_0\mathbb{Z}[a_0,a_1,\dots,a_n]\ .$$

Alors $\mathrm{disc}_n(P(X))$, le *discriminant en degré n de $P(X)$* est l'élément de $\mathbb{Z}[a_0,a_1,\dots,a_n]$ défini par

(0) $$\mathrm{res}_{n,n-1}(P(X),P'(X))=(-1)^{\frac{n(n-1)}{2}}a_0\mathrm{disc}_n(P(X))\ .$$

([B] IV.78, formule (47), [F] proposition 7.7.3.1, [F.M.2] IV.7 p. 235)

2. Une relation sur le discriminant ([B] corollaire 2, A.IV. 80, [G.K.Z] formule (1.41) p. 407)

Proposition *Soient $a_0,a_1,\dots,a_n$ des variables sur $\mathbb{Z}$,*
$f(X):=a_0X^n+a_1X^{n-1}+\dots+a_n$, $g(X):=a_1X^{n-1}+a_2X^{n-2}+\dots+a_0$.
Soit $\varphi:\mathbb{Z}[a_0,a_1,\dots,a_n]\to\mathbb{Z}[a_1,a_2,\dots,a_n]$ l'unique homomorphisme tel que $\varphi(a_0)=0$ et $\varphi(a_i)=a_i$ pour $1\le i\le n$ (c'est ce qu'on appelle parfois la spécialisation en $a_0=0$). *Alors on a*

$$\varphi(\mathrm{disc}_n(f(X)))=(a_1)^2\,\mathrm{disc}_{n-1}(g(X))\ ,$$

ou encore

$$\varphi(\mathrm{disc}_n(f(X)))=(a_1)^2\,\mathrm{disc}_{n-1}(\varphi(f(X)))\ ,$$

Démonstration
Il suit de la définition en (0) du discriminant de $f(X)$ en degré n que

(1) $$(-1)^{\frac{n(n-1)}{2}}\mathrm{disc}_n f(X)=\det A$$

avec

$$A=\begin{bmatrix} 1 & a_1 & \cdots & a_{n-1} & a_n & 0 & & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n & & \\ & & a_0 & a_1 & \cdots & a_{n-1} & a_n & \\ 0 & & & & & & & \\ n & (n-1)a_1 & \cdots & a_{n-1} & 0 & & & 0 \\ 0 & na_0 & (n-1)a_1 & \cdots & a_{n-1} & & & \\ & & & & & & & 0 \\ 0 & & & 0 & na_0 & (n-1)a_1 & \cdots & a_{n-1} \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \} n-1 \\ \\ \\ \\ \} n \\ \\ \\ \end{matrix}$$

Soit $\varphi : \mathbb{Z}[a_0, a_1, \ldots, a_n] \to \mathbb{Z}[a_1, a_2, \ldots, a_n]$ l'unique homomorphisme d'anneau défini par $\varphi(a_0)=0$ et $\varphi(a_i)=a_i$ pour $1 \le i \le n$. Il est clair que si $M=[m_{ij}]_{1\le i,j\le n} \in M_n(\mathbb{Z}[a_0, a_1, \ldots, a_n])$, alors φ induit un homomorphisme d'anneau

$$\Phi : (M_n(\mathbb{Z}[a_0, a_1, \ldots, a_n]) \to M_n(\mathbb{Z}[a_1, a_2, \ldots, a_n])$$

défini par $\Phi([m_{ij}]_{1\le i,j\le n}) := [\varphi(m_{i,j})]_{1\le i,j\le n}$.

Facilement, on a

(2) $$\varphi(\det[m_{i,j}]_{1\le i,j\le n}) = \det(\Phi([m_{ij}]_{1\le i,j\le n}))\ .$$

Alors en appliquant φ à (1) on obtient

(3) $$(-1)^{\frac{n(n-1)}{2}}\ \varphi(\mathrm{disc}_n(f(X)) = \varphi(\det A) = \det(\Phi(A))\ .$$

Soit

$$B := \Phi(A) = \begin{bmatrix} 1 & a_1 & \cdots & a_{n-1} & a_n & 0 & & 0 \\ 0 & 0 & a_1 & \cdots & a_{n-1} & a_n & & \\ & & 0 & a_1 & \cdots & a_{n-1} & a_n & \\ 0 & & & & & & & \\ n & (n-1)a_1 & \cdots & a_{n-1} & 0 & & & 0 \\ 0 & 0 & (n-1)a_1 & \cdots & a_{n-1} & & & \\ & & & & & & & 0 \\ 0 & & & 0 & 0 & (n-1)a_1 & \cdots & a_{n-1} \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \} n-1 \\ \\ \\ \\ \} n \\ \\ \\ \end{matrix}$$

Alors le calcul de $\det B$ en développant selon la première colonne s'écrit

(4) $$\det B = \det C + (-1)^{n-1} n\ \det D$$

avec

(5)
$$C := \begin{bmatrix} 0 & a_1 & \cdots & a_{n-1} & a_n & 0 & 0 \\ 0 & 0 & a_1 & \cdots & a_{n-1} & a_n & \\ & & & & & & \\ 0 & & & 0 & a_1 & \cdots & a_{n-1} & a_n \\ (n-1)a_1 & (n-2)a_2 & \cdots & a_{n-1} & 0 & & 0 \\ 0 & (n-1)a_1 & (n-2)a_2 & \cdots & a_{n-1} & & \\ & & & & & & 0 \\ 0 & & 0 & 0 & (n-1)a_1 & \cdots & a_{n-1} \end{bmatrix} \begin{matrix} \\ \\ \\ \} n-2 \\ \\ \\ \} n \end{matrix}$$

(6)
$$D := \begin{bmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_{n-1} & a_n & 0 \\ & & & & & & \\ 0 & 0 & 0 & a_1 & a_2 & \cdots & a_{n-1} & a_n \\ 0 & (n-1)a_1 & (n-2)a_2 & \cdots & a_{n-1} & 0 & 0 \\ 0 & 0 & (n-1)a_1 & (n-2)a_2 & \cdots & a_{n-1} & 0 \\ & & & & & & \\ 0 & 0 & 0 & (n-1)a_1 & (n-2)a_2 & \cdots & a_{n-1} \end{bmatrix} \begin{matrix} \\ \\ \} n-1 \\ \\ \\ \} n-1 \end{matrix}$$

Alors le développement de $\det C$ selon la première colonne dit que

(7) $$\det C = (-1)^{n-2}(n-1)\, a_1 \ \operatorname{res}_{n-1,n-2}(g(X), g'X) .$$

Ensuite le développement de $\det D$ selon la première colonne dit que

(8) $$\det D = a_1 \operatorname{res}_{n-1,n-2}(g(X), g'(X)) .$$

En résumé, compte tenu de (0) à (8), on a

(9) $$\det A = ((-1)^{n-2}(n-1)a_1 + (-1)^{n-1} n\, a_1) \operatorname{res}_{n-1,n-2}(g(X), g'(X))$$

Soit donc

(10) $$(-1)^{\frac{n(n-1)}{2}} \varphi(\operatorname{disc}_n(f)) = (-1)^{n-1} a_1 (-1)^{\frac{(n-1)(n-2)}{2}} a_1 \operatorname{disc}_{n-1}(g).$$

i.e. $$\varphi(\operatorname{disc}_n(f)) = (a_1)^2 \operatorname{disc}_{n-1}(g) .$$

Références

[B] Bourbaki N. Algèbre Ch. 4 à 7 *Masson* (1981)

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

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

[G.K.Z] Gelfand I.M. , Kapranov M.M. , Zelevinsky Discriminants, Resultants and Multidimensional Determinants *Birxhäuser* (1994)

p. 235 complément à IV.7.1. Quelques calculs de discriminants

0. Introduction

Si $P(X)$ est un polynôme à coefficients dans un anneau commutatif, le discriminant de $P(X)$, au signe près, est défini par le résultant des polynômes $P(X)$ et $P'(X)$ où $P'(X)$ est le polynôme dérivé de $P(X)$. C'est donc le déterminant de la matrice de Sylvester associée à $P(X)$ et $P'(X)$. Si donc $P(X)$ est de degré n, la matrice de Sylvester est une matrice carrée à $2n-1$ lignes et $2n-1$ colonnes. On sait qu'alors le calcul du déterminant devient délicat, même avec Maple, si n est assez grand.

Si $P(X)$ est un polynôme unitaire de degré n à coefficients dans un corps commutatif K, sous réserve de quelques conditions sur la caractéristique de K, le discriminant de $P(X)$ peut être évalué en considérant la factorisation dans la clôture algébrique de K en produit de polynôme unitaire de degré 1. C'est la méthode que l'on va utiliser sur quelques exemples lorsque le nombre de racines distinctes de $P'(X)$ est 1, 2 ou 3.

1. Les exemples

Soient $n \geq 1$ *un entier,* K *un corps commutatif avec* $\operatorname{car} K = 0$ *ou* $\operatorname{car} K \nmid n$.

1.1. *Soit* $P(X) \in K[X]$ *avec* $P(X) = X^n + a_n$. *Alors*

$$\operatorname{disc}_n P = (-1)^{\frac{n(n-1)}{2}} (a_n)^{n-1}.$$

1.2. *Soit* $P(X) = X^n + a_1 X^{n-1} + a_n \in K[X]$, *alors*

$$\operatorname{disc}_n P(X) = (-1)^{\frac{n(n-1)}{2}} \left((1-n)^{n-1} (2-n) (a_n)^{n-2} (a_1)^n + n^n (a_n)^{n-1} \right).$$

1.3. *Soit* $P(X) = X^n + a_2 X^{n-2} + a_n$.

On suppose que $n = 2m$, *alors on a*

$$\operatorname{disc}_n P(X) = (-1)^m \left(4(n-2)^{n-2} (a_2)^n (a_n)^{n-3} - 4(n-2)^{m-1} (a_2)^m (a_n)^{n-2} + (-1)^m n^n (a_n)^{n-1} \right)$$

On suppose que $n = 2m+1$, *alors on a*

$$\operatorname{disc}_n P(X) = (-1)^m \left(4(n-2)^{n-2} (a_2)^n (a_n)^{n-3} + n^n (a_n)^{n-1} \right).$$

2. Les formules

Soient $a_0, a_1, \ldots, a_n, X$ des indéterminées sur $\mathbb{Z}$,

$$P(X) := a_0 X^n + a_1 X^{n-1} + \ldots + a_n ,$$

alors

$$\operatorname{disc}_n P(X) := (-1)^{\frac{n(n-1)}{2}} \operatorname{res}_{n,n-1}(P(X), P'(X))$$

où $\operatorname{res}_{n,n-1}(P(X), P'(X))$ est le résultant en degré n et $n-1$ de $P(X)$ et $P'(X)$ ([B] IV.78, formule (47), [Fr] proposition 7.7.3.1 p. 273, [F.M.1] ex. 113, p. 321).

On sait alors que $\operatorname{disc}_n P(X) \in \mathbb{Z}[a_0, a_1, \ldots, a_n]$ est un polynôme homogène de degré $n(n-1)$, i.e. un polynôme homogène isobare de degré $n(n-1)$ sachant que a_i est de poids i.

On suppose maintenant que K est un corps commutatif avec $\operatorname{car} K = 0$ ou $\operatorname{car} K \nmid n$ et que $P(X) = X^n + a_1 X^{n-1} + \ldots + a_n$, alors on a

$$(1) \qquad \operatorname{disc}_n P(X) = (-1)^{\frac{n(n-1)}{2}} n^n \prod_{i=1}^{n-1} P(\alpha_i) ,$$

avec $\alpha_i \in K^{alg}$ et $P'(X) = n(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_{n-1})$ (([B] IV.75, formule (39), [Fr] proposition 7.7.3.1 p. 273, [F.M.1] ex. 113, p. 321, [F.M.2] , IV. 7 p. 235).

3. Démonstration de 1.1 , 1.2 , 1.3

1.1. On a $P(X) = X^n + a_n$, $P'(X) = nX^{n-1}$, ainsi en utilisant la fomule (1), on a bien

$$\operatorname{disc}_n P = (-1)^{\frac{n(n-1)}{2}} n^n (a_n)^{n-1} .$$

1.2. On a $P(X) = X^n + a_1 X^{n-1} + a_n$, $P'(X) = n(X^{n-2})(X - \frac{1-n}{n} a_1)$.

Si $a_1 \neq 0$, on a donc en utilisant (1)

$$\operatorname{dis}_n P = (-1)^{\frac{n(n-1)}{2}} n^n (P(0))^{n-2} P(\tfrac{1-n}{n} a_1)$$

On obtient donc

$$\operatorname{disc}_n P(X) = (-1)^{\frac{n(n-1)}{2}} \left((1-n)^{n-1}(2-n)(a_n)^{n-2}(a_1)^n + n^n (a_n)^{n-1} \right) .$$

Le cas $a_1 = 0$ se traite de la même façon.

1.3. On a $P(X)=X^n+a_2X^{n-2}+a_n$ et donc
$P'(X)=nX^{n-2}+(n-2)a_2X^{n-3}$, soit

$$P'(X)=nX^{n-3}(X^2-\frac{2-n}{n}a_2) .$$

Si $\frac{2-n}{n}a_2\neq 0$, il existe $\theta\in K^{alg}$ avec

(2) $$\theta^2=\frac{2-n}{n}a_2 .$$

$P'(X)=nX^{n-3}(X-\theta)(X+\theta)$. Si en plus $\mathrm{card}K\neq 2$ et $n\geq 3$, on a $\theta\neq-\theta$ et en utilisant (1) , on a

(3) $$\mathrm{disc}_n(P(X))=(-1)^{\frac{n(n-1)}{2}}n^n(a_n)^{n-3}P(\theta)P(-\theta) ,$$

On a donc

$$P(\theta)=\theta^{n-2}(\theta^2+a_2)+a_n .$$

En tenant compte de (2) , ça veut dire que

(4) $$P(\theta)=\theta^{n-2}(\frac{2}{n}a_2)+a_n .$$

1.3.1. On suppose maintenant que $n=2m$, ainsi toujours compte tenu de (2) et (4) il suit que

$$P(\theta)=(\frac{2-n}{n}a_2)^{m-1}+a_n .$$

De même

$$P(-\theta)=(\frac{2-n}{n}a_2)^{m-1}+a_n .$$

Ce qui implique

$$P(\theta)P(-\theta)=(\frac{2-n}{n}a_2)^{2(m-1)}+2((\frac{2-n}{n}a_2)^{m-1}a_n+(a_n)^2 .$$

Il suit facilement en utilisant (3) que 1.3. est vérifié pour $n=2m$.

1.3.2. On suppose que $n=2m+1$.
Il suit (4) et (2) que
$P(\theta)=\theta(\frac{2-n}{n}a_2)^m+a_n$ et aussi $P(-\theta)=-\theta(\frac{2-n}{n}a_2)^m+a_n$ et donc

$$P(\theta)P(-\theta)=a_n^2-\theta^2(\frac{2-n}{n}a_2)^{2m} .$$

Soit donc en tenant compte de (2)

$$P(\theta)P(-\theta)=a_n^2-(\frac{2-n}{n}a_2)^n .$$

Il suit facilement en utilisant (3) que 1.3. est vérifié pour $n=2m+1$.

Les cas $\mathrm{car}K=2$ ou $\frac{2-n}{n}a_2\neq 0$ sont immédiats.

Références

[B] Bourbaki N. Algèbre Ch. 4 à 7 *Masson* (1981)
[F] Fresnel J. Anneaux *Hermann* (2001)
[F.M.1] Fresnel J. & Matignon M. Algèbre et géométrie *Hermann* (2011)
[F.M.2] Fresnel J. & Matignon M. Algèbre et géométrie *Ellipses* (2017)

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 $\mathbb{U}_n$ le sous-groupe de $\mathbb{C}^\times$ constitué des racines n-ièmes de l'unité et $\mathbb{U}'_n$ le sous-ensemble de $\mathbb{U}_n$ constitué des éléments d'ordre n . Par définition le n-ième polynôme cyclotomique est $\Phi_n(X):=\prod_{z\in\mathbb{U}'_n}(X-z)$.
Soit $h\in\mathbb{N}$, on appelle h-ième somme de Newton relative aux racines du polynôme cyclotomique Φ_n , l'expression $p_h(n):=\sum_{z\in\mathbb{U}'_n}z^h$; 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*

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

Démonstration
On s'intéresse tout d'abord à la formule $p_h(n)=\sum_{d\mid \mathrm{pgcd}(n,h)} d\,\mu(\frac{n}{d})$.

1) Facilement, on a $\mathbb{U}_n=\biguplus_{d\mid n}\mathbb{U}'_d$. Il suit de cela que $\sum_{d\mid n} p_h(d)=\sum_{z\in U_n} z^h$. Il suit de cela que $\sum_{d\mid n} p_h(d)=0$ si $h\nmid n$ et que $\sum_{d\mid n} p_h(d)=n$ si $h\mid n$. Alors la formule $p_h(n)=\sum_{d\mid \mathrm{pgcd}(n,h)} d\,\mu(\frac{n}{d})$ 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 $f:\mathbb{U}_m\times\mathbb{U}_n\to\mathbb{U}_{m\,n}$ l'application définie par $f(z,z'):=z\,z'$. Facilement f est un homomorphisme de groupes. Montrons que f est injectif. Soit $(z,z')\in\ker f$, i.e. $z\,z'=1$. 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 $\mathbb{U}'_m\times\mathbb{U}'_n$ sur $\mathbb{U}'_{m\,n}$. Tout d'abord montrons que $f(\mathbb{U}'_m\times\mathbb{U}'_n)\subset\mathbb{U}'_{m\,n}$. Soient $z\in\mathbb{U}'_m$, $z'\in\mathbb{U}'_n$ il faut montrer que $o(z\,z')=m\,n$. Facilement $(z\,z')^{m\,n}=1$, supposons que $(z\,z')^d=1$, on a donc $(z\,z')^{d\,m}=1$ et donc $(z')^{d\,m}=1$, comme $o(z')=n$, on a $n\mid d\,m$, 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 $m\,n\mid d$; ce qui montre que $o(z\,z')=m\,n$. Ainsi f induit une injection de $\mathbb{U}'_m\times\mathbb{U}'_n$ dans $\mathbb{U}'_{m\,n}$.
Sachant que

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

il suit que f induit une bijection de $\mathbb{U}'_m\times\mathbb{U}'_n$ sur $\mathbb{U}'_{m\,n}$.

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 $\mathbb{U}'_m \times \mathbb{U}'_n$ sur $\mathbb{U}'_{m\,n}$ montre que

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

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

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

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. 278 IV.14 nouvelle version
Quels sont les anneaux commutatifs A unitaires dont le groupe des inversibles est fini.

Notre problème ici est de considérer le cas où le groupe des inversibles d'un anneau commutatif unitaire est fini.
Bien entendu si A est un anneau fini alors le groupe $A^\times$ des inversibles de A est fini. Si $A = \mathbb{Z}$, alors $\mathbb{Z}^\times = \{1, -1\}$ est fini. On traitera d'abord le cas où A

est un anneau principal, c'est la proposition 0 . A la proposition 1, on verra que que si $A^\times$ est fini et si le nombre de maximaux est fini, alors A est fini.

Proposition 0. *Soient A un anneau principal dont le groupe $A^\times$ des inversibles est fini. Alors A est soit un corps fini, soit un anneau admettant une infinité d'idéaux maximaux.*

Démonstration
1) Si A est un corps , alors $A^\times = A - \{0\}$, ainsi A est fini.

2) *On suppose maintenant que A n'est pas un corps.* Ainsi tout idéal maximal de A est non nul et A contient au moins un idéal maximal. Il s'agit de montrer que l'ensemble des idéaux maximaux de A est infini. Supposons le contraire, ainsi $\{\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_r\}$ est l'ensemble des idéaux maximaux de A . Il suit facilement de cela que

$A = (\mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_r) \cup A^\times$, en effet si $a \in A$ et $a \notin (\mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_r)$, alors a est inversible puisque tout élément non-inversible est contenu dans un idéal maximal.
2.1) Supposons $\mathrm{car} A = 0$, alors $\mathbb{Z} \subset A$. Facilement $\mathfrak{M}_i \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, ainsi $\mathfrak{M}_i \cap \mathbb{Z} = \{0\}$ ou $\mathfrak{M}_i \cap \mathbb{Z} = p_i\mathbb{Z}$ avec p_i irréductible. Si $\mathfrak{M}_i \cap \mathbb{Z} = \{0\}$ pour tout i , cela veut dire que $\mathbb{Z} - \{0\} \subset A^\times$, c'est impossible puisque $A^\times$ est fini. Sinon il existe $q_1, q_2, \ldots, q_s$ des irréductibles de $\mathbb{Z}$ avec $(\mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_r) \cap \mathbb{Z} = q_1\mathbb{Z} \cup q_2\mathbb{Z} \cup \ldots \cup q_s\mathbb{Z}$. Il existe un irréductible q de $\mathbb{Z}$ avec $q \nmid q_1 q_2 \ldots q_s$ dans $\mathbb{Z}$, ce qui veut dire que $q \notin q_1\mathbb{Z} \cup q_2\mathbb{Z} \cup \ldots \cup q_s\mathbb{Z}$, donc $q \in A^\times$. Comme l'application $z \mapsto q^z$ de $\mathbb{N}$ dans $\mathbb{Z}$ est injective, il suit que $A^\times$ serait infini. Ce qui est une contradiction.
2.2) On suppose que $\mathrm{car} A = p$, comme A est intègre, il suit que p est un nombre premier, alors on a $\mathbb{F}_p \subset A$. Si tout élément de A est algébrique sur $\mathbb{F}_p$, cela veut dire que A est un corps ; en effet si $\alpha \in A$ est algébrique sur $\mathbb{F}_p$ cela veut dire que l'anneau $\mathbb{F}_p[\alpha]$ est un corps ([Fr. F.] proposition 3.1.1.), si donc $\alpha \neq 0$ il suit que $\alpha^{-1} \in \mathbb{F}_p[\alpha] \subset A$. Ceci contredit notre hypothèse sur A . Ainsi il existe $T \in A$ qui est transcendant sur $\mathbb{F}_p$, alors le sous-anneau de A engendré par $\mathbb{F}_p$ et T est isomorphe à l'anneau des polynômes à une variable à coefficients dans $\mathbb{F}_p$. Ensuite on procède comme en 2.1) où $\mathbb{F}_p[T]$ joue le rôle de $\mathbb{Z}$ pour aboutir à une contradiction.

Proposition 1 *Soient A un anneau, commutatif, unitaire. On suppose que le groupe $A^\times$ des inversibles de A est fini et que le nombre d'idéaux maximaux de A est fini. Alors A est un anneau fini.*

Démonstration
1) Soit $\{\mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_r\}$ l'ensemble des idéaux maximaux de A avec $\mathfrak{M}_i \neq \mathfrak{M}_j$ si $i \neq j$. Soit $\rho_i : A \to \frac{A}{\mathfrak{M}_i}$ la surjection canonique et $\rho : A \to \frac{A}{\mathfrak{M}_1} \times \frac{A}{\mathfrak{M}_2} \times \dots \times \frac{A}{\mathfrak{M}_r}$ l'application diagonale définie par $\rho(x) := (\rho_1(x), \rho_2(x), \dots, \rho_r(x))$, alors $\ker \rho = \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \dots \cap \mathfrak{M}_r$.

2) *Montrons que ρ est surjectif.*
Soient $x_1, x_2, \dots, x_r \in A$, il faut donc montrer qu'il existe $x \in A$ avec $x - x_i \in \mathfrak{M}_i$ pour $1 \leq i \leq r$. Soit

$$\mathfrak{A} := \mathfrak{M}_2 \cap \mathfrak{M}_3 \cap \dots \cap \mathfrak{M}_r + \mathfrak{M}_1 \cap \mathfrak{M}_3 \cap \dots \cap \mathfrak{M}_r + \dots + \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \dots \cap \mathfrak{M}_{r-1}.$$

Montrons que $\mathfrak{A} = A$. Sinon l'idéal $\mathfrak{A}$ est contenu dans un idéal maximal, disons par exemple $\mathfrak{A} \subset \mathfrak{M}_1$, cela implique facilement que $\mathfrak{M}_2 \cap \mathfrak{M}_3 \cap \dots \cap \mathfrak{M}_r \subset \mathfrak{M}_1$. Comme $\mathfrak{M}_2 \neq \mathfrak{M}_1$ il existe $x_2 \in \mathfrak{M}_2$ et $x_2 \notin \mathfrak{M}_1$, de même il existe $x_3 \in \mathfrak{M}_3$ et $x_3 \notin \mathfrak{M}_1$, ..., il existe $x_r \in \mathfrak{M}_r$ et $x_r \notin \mathfrak{M}_1$. Clairement $x_2 x_3 \dots x_r \in \mathfrak{M}_2 \cap \mathfrak{M}_3 \cap \dots \cap \mathfrak{M}_r$, ainsi $x_2 x_3 \dots x_r \in \mathfrak{M}_1$; comme $\mathfrak{M}_1$ est maximal, donc premier, il existe i avec $2 \leq i \leq r$ avec $x_i \in \mathfrak{M}_1$, ce qui est une contradiction.
En conséquence de cela, il existe $y_1 \in \mathfrak{M}_2 \cap \mathfrak{M}_3 \cap \dots \cap \mathfrak{M}_r$, $y_2 \in \mathfrak{M}_1 \cap \mathfrak{M}_3 \cap \dots \cap \mathfrak{M}_r$, ..., $y_r \in \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \dots \cap \mathfrak{M}_{r-1}$ avec $y_1 + y_2 + \dots + y_r = 1$. Comme $y_2, y_3, \dots, y_r \in \mathfrak{M}_1$, on a $y_1 - 1 \in \mathfrak{M}_1$.
Soit $x := x_1 y_1 + x_2 y_2 + \dots + x_r y_r$, on a donc

$$x - x_1 = x_1(y_1 - 1) + x_2 y_2 + \dots + x_r y_r \ ;$$

il suit donc de ce qui précède que $x - x_1 \in \mathfrak{M}_1$. On montrerait de même que $x - x_i \in \mathfrak{M}_i$ pour $1 \leq i \leq r$.

3) *Montrons que* $1 + \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \dots \cap \mathfrak{M}_r \subset A^\times$.
En effet, soit $z \in \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \dots \cap \mathfrak{M}_r$, alors $1 + z \in A^\times$, sinon, il est contenu dans un maximal, disons $1 + z \in \mathfrak{M}_1$, et comme $z \in \mathfrak{M}_1$, cela implique que $1 \in \mathfrak{M}_1$, ce qui est exclu.
En particulier, comme $A^\times$ est fini, il suit que $\mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \dots \cap \mathfrak{M}_r$ est fini.

4) *Montrons que* ρ *induit un homomorphisme*
$\rho^\times : A^\times \to (\frac{A}{\mathfrak{M}_1} \times \frac{A}{\mathfrak{M}_2} \times ... \times \frac{A}{\mathfrak{M}_r})^\times$ *qui est surjectif.*
En effet soient $a, b \in A$ tels que $\rho(a)\rho(b) = \rho(1)$, on a donc
$ab - 1 \in \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap ... \cap \mathfrak{M}_r$, i.e. $ab \in 1 + \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap ... \cap \mathfrak{M}_r$, il suit de 3) que $a, b \in A^\times$, ça montre bien que $\rho^\times$ est surjectif, ainsi
$(\frac{A}{\mathfrak{M}_1} \times \frac{A}{\mathfrak{M}_2} \times ... \times \frac{A}{\mathfrak{M}_r})^\times = (\frac{A}{\mathfrak{M}_1})^\times \times (\frac{A}{\mathfrak{M}_2})^\times \times ... \times (\frac{A}{\mathfrak{M}_r})^\times$ est fini, et comme
$(\frac{A}{\mathfrak{M}_i})^\times = \frac{A}{\mathfrak{M}_i} - \{0\}$, il suit que $\frac{A}{\mathfrak{M}_1} \times \frac{A}{\mathfrak{M}_2} \times ... \times \frac{A}{\mathfrak{M}_r}$ est fini.
Sachant par 3) que $\ker\rho$ est fini, il suit que A est fini.

Corollaire *Soient* A *un anneau, commutatif, unitaire. On suppose que le groupe* $A^\times$ *des inversibles de* A *est fini. Alors* A *est un anneau fini ou le nombre d'idéaux maximaux de* A *est infini.*

Remarque de terminologie Un anneau commutatif unitaire A est dit *local* (resp. *semi-local*) s'il possède un unique idéal maximal (resp. un nombre fini d'idéaux maximaux).

Ainsi la proposition précédente dit qu'un anneau commutatif semi-local A dont le groupe $A^\times$ des inversibles est fini est un anneau fini. Bien entendu tout anneau commutatif fini est semi-local.

On possède beaucoup d'exemples d'anneaux commutatifs finis. Par exemple $\frac{\mathbb{Z}}{m\mathbb{Z}}$ si $m \neq 0$, $\frac{K[T]}{P(T)K[T]}$ si K est un corps fini et si $P(T) \neq 0$.

Proposition 2 *Soit* A *un anneau commutatif fini. Alors* A *est isomorphe à un produit fini d'anneaux locaux.*

Démonstration (ce n'est autre chose que le théorème des restes chinois, Fr Anneaux, ex. 1.9.14 p. 48).

1) *Le radical de Jacobson est nilpotent.*
Soient $\{\mathfrak{M}_1, \mathfrak{M}_2, ..., \mathfrak{M}_r\}$ l'ensemble des idéaux maximaux de A, avec $\mathfrak{M}_i \neq \mathfrak{M}_j$ si $i \neq j$, $\mathfrak{R} := \mathfrak{M}_1 \mathfrak{M}_2 ... \mathfrak{M}_r$; il s'agit de montrer qu'il existe $k \geq 1$ tel que $\mathfrak{R}^k = \{0\}$. Clairement la suite $(\mathfrak{R}^k)_k$ est décroissante, elle est donc

stationnaire, ce qui veut dire qu'il existe k avec $\mathfrak{R}^k=\mathfrak{R}^{k+1}$. Il faut en conclure que $\mathfrak{R}^k=\{0\}$.
Si ce n'est pas le cas, on a $\mathfrak{R}^k=A\,e_1+A\,e_2+\ldots+A\,e_s$, avec $s\geq 1$ et on suppose que la famille $\{e_1,e_2,\ldots,e_s\}$ est génératrice minimale. De $\mathfrak{R}^k=\mathfrak{R}^{k+1}$, il suit que $\mathfrak{R}^k=\mathfrak{R}\,e_1+\mathfrak{R}\,e_2+\ldots+\mathfrak{R}\,e_s$, ainsi $e_1=\lambda_1 e_1+\lambda_2 e_2+\ldots+\lambda_s e_s$, avec $\lambda_i\in\mathfrak{R}$. Soit $(1-\lambda_1)\,e_1=\lambda_2 e_2+\lambda_3 e_3+\ldots+\lambda_s e_s$;
facilement $1-\lambda_1\notin \mathfrak{M}_1\cup\mathfrak{M}_2\cup\ldots\cup\mathfrak{M}_r$, ainsi $1-\lambda_1\in A^\times$ ce qui implique que $e_1\in A\,e_2+A\,e_3+\ldots+A\,e_s$. Ce qui contredit la minimalité de la famille $\{e_1,e_2,\ldots,e_s\}$.
En conclusion on a bien $\mathfrak{R}^k=\{0\}$ (cette démonstration n'est autre chose que celle du lemme de Nakayama, Fr Anneaux lemme 8.2.1 , p. 300).

2) *Soit* $t\geq 1$, *alors on a* $\mathfrak{M}_1^t\mathfrak{M}_2^t\ldots\mathfrak{M}_r^t=\mathfrak{M}_1^t\cap\mathfrak{M}_2^t\cap\ldots\cap\mathfrak{M}_r^t$.
Il suffit de montrer l'égalité

$$\mathfrak{M}_1^t\mathfrak{M}_2^t\ldots\mathfrak{M}_h^t=\mathfrak{M}_1^t\cap\mathfrak{M}_2^t\cap\ldots\cap\mathfrak{M}_h^t$$

par récurrence sur h. L'égalité pour $h=1$ est triviale, on suppose $h<r$ et on veut passer de h à $h+1$.
Montrons d'abord que
(1) $$\mathfrak{M}_1^t\mathfrak{M}_2^t\ldots\mathfrak{M}_h^t+\mathfrak{M}_{h+1}^t=A\,.$$
Sinon, il existe un maximal $\mathfrak{M}$ avec $\mathfrak{M}_1^t\mathfrak{M}_2^t\ldots\mathfrak{M}_h^t+\mathfrak{M}_{h+1}^t\subset\mathfrak{M}$; ça montre qu'il existe $i\leq h$ avec $\mathfrak{M}_i\subset\mathfrak{M}$ et $\mathfrak{M}_{h+1}\subset\mathfrak{M}$, ce qui est impossible.
En conclusion, on a
(2) $u\in\mathfrak{M}_1^t\mathfrak{M}_2^t\ldots\mathfrak{M}_h^t$ et $v\in\mathfrak{M}_{h+1}^t$ avec $u+v=1$.
L'inclusion

$$\mathfrak{M}_1^t\mathfrak{M}_2^t\ldots\mathfrak{M}_h^t\mathfrak{M}_{h+1}^t\subset\mathfrak{M}_1^t\cap\mathfrak{M}_2^t\cap\ldots\cap\mathfrak{M}_t^t\cap\mathfrak{M}_{h+1}^t$$

est immédiate.
Soit maintenant $x\in(\mathfrak{M}_1^t\cap\mathfrak{M}_2^t\cap\ldots\cap\mathfrak{M}_h^t)\cap\mathfrak{M}_{h+1}^t$. Il suit de (2)
$x=x.1=x\,u+x\,v$, facilement $x\,u\in\mathfrak{M}_1^t\mathfrak{M}_2^t\ldots\mathfrak{M}_h^t\mathfrak{M}_{h+1}^t$ et
compte tenu de l'hypothèse de récurrence $x\,v\in\mathfrak{M}_1^t\mathfrak{M}_2^t\ldots\mathfrak{M}_h^t\mathfrak{M}_{h+1}^t$.
Ainsi, on a l'autre inclusion.

3) Soient k défini en 1), $\rho_i:A\to\frac{A}{\mathfrak{M}_i^k}$ la surjection canonique pour $1\leq i\leq r$ et $\rho:A\to\frac{A}{\mathfrak{M}_1^k}\times\frac{A}{\mathfrak{M}_2^k}\times\ldots\times\frac{A}{\mathfrak{M}_r^k}$ l'application diagonale définie par

$\rho(x) := (\rho_1(x), \rho_1(x), \ldots, \rho_1(x))$. On a donc $\ker\rho = \mathfrak{M}_1^k \cap \mathfrak{M}_2^k \cap \ldots \cap \mathfrak{M}_r^k$. Il suit donc de 1) et 2) que $\ker\rho = \{0\}$.

Il reste à montrer que ρ est surjectif et que $\frac{A}{\mathfrak{M}_i^k}$ est local pour $1 \le i \le r$.

Montrons que

(3) $\mathfrak{A} := \mathfrak{M}_2^k \mathfrak{M}_3^k \ldots \mathfrak{M}_r^k + \mathfrak{M}_1^k \mathfrak{M}_3^k \ldots \mathfrak{M}_r^k + \ldots + \mathfrak{M}_1^k \mathfrak{M}_2^k \ldots \mathfrak{M}_{r-1}^k = A$.

Supposons le contraire, on a par exemple $\mathfrak{A} \subset \mathfrak{M}_1$, cela implique $\mathfrak{M}_2^k \mathfrak{M}_3^k \ldots \mathfrak{M}_r^k \subset \mathfrak{M}_1$, il suit de cela qu'il existe i avec $2 \le i \le r$ avec $\mathfrak{M}_i \subset \mathfrak{M}_1$, ce qui est impossible.

Il suit donc qu'il existe

$$x_1 \in \mathfrak{M}_2^k \mathfrak{M}_3^k \ldots \mathfrak{M}_r^k ,\ x_2 \in \mathfrak{M}_1^k \mathfrak{M}_3^k \ldots \mathfrak{M}_r^k , \ldots , x_r \in \mathfrak{M}_1^k \mathfrak{M}_2^k \ldots \mathfrak{M}_{r-1}^k$$

tels que

(4) $$1 = x_1 + x_2 + \ldots + x_r .$$

Soient $y_1, y_2, \ldots, y_r \in A$, il faut montrer qu'il existe $y \in A$ avec $y - y_i \in \mathfrak{M}_i^k$ pour $1 \le i \le r$.

Montrons que $y := y_1 x_1 + y_2 x_2 + \ldots + y_r x_r$ convient. On a

$$y - y_1 = y_1(1 - x_1) + y_2 x_2 + \ldots + y_r x_r ,$$

or $y_i x_i \in \mathfrak{M}_1^k$ pour $2 \le i \le r$.

De plus de la relation (4) , on a aussi $1 - x_1 \in \mathfrak{M}_1^k$. Ainsi $y - y_1 \in \mathfrak{M}_1^k$. On aurait de même $y - y_i \in \mathfrak{M}_i^k$ pour $2 \le i \le r$.

4) Il reste à montrer que $\frac{A}{\mathfrak{M}_i^k}$ est local. En effet si $\mathfrak{N}$ est un idéal maximal de $\frac{A}{\mathfrak{M}_i^k}$, alors $\rho_i^{-1}(\mathfrak{N})$ est idéal premier de A avec $\mathfrak{M}_i^k \subset \rho_i^{-1}(\mathfrak{N})$. Il suit de cela que $\mathfrak{M}_i \subset \rho_i^{-1}(\mathfrak{N})$ et comme $\mathfrak{M}_i$ est maximal, on a bien $\mathfrak{M}_i = \rho_i^{-1}(\mathfrak{N})$, ce qui veut dire que $\mathfrak{N} = \rho_i(\mathfrak{M}_i)$. Ainsi $\rho_i(\mathfrak{M}_i)$ est l'unique idéal maximal de $\frac{A}{\mathfrak{M}_i^k}$.

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

page 299, complément : triangles rectangles isocèles et quadrilatère
(c'est la version géométrique de l'exercice 2.8.41 , p. 236 , de [Fr], version 1996)

Soient P *le plan affine euclidien orienté attaché au plan vectoriel euclidien* $(T,(.\,|\,.))$.
Soient a,b,c,d *quatre points de* P *avec* $a\neq b$, $b\neq c$, $c\neq d$, $d\neq a$. *Soient* m (resp. n,p,q) *le centre de l'unique rotation* r_m (resp. r_n,r_p,r_q) *de mesure d'angle* $\frac{\pi}{2}$ *telle que* $r_m(a)=b$ (resp. $r_n(b)=c$, , $r_p(c)=d$, $r_q(d)=a$, fig. 1).

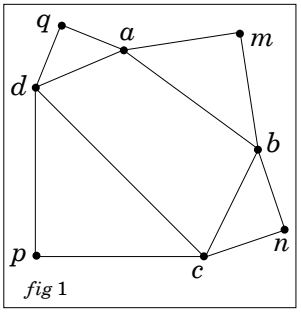


fig 1

1. *Alors on a* $\|m-p\|=\|n-q\|$ *et* $(m-p\,|\,n-q)=0$ (fig. 2).
2. *La suite* $(\frac{a+c}{2},\frac{m+p}{2},\frac{b+d}{2},\frac{n+q}{2})$ *est la suite des quatre sommets d'un carré* (fig.3).
3. *Les propriétés suivantes sont équivalentes.*
i) On a $\frac{m+p}{2}=\frac{n+q}{2}$,
ii) $a-b=d-c$ (i.e. *la suite* (a,b,c,d) *est la suite des sommets d'un parallélogramme*).

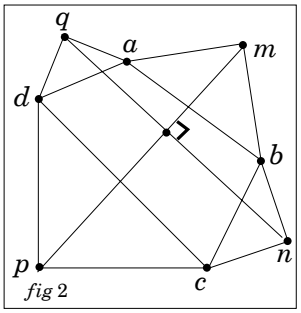


fig 2

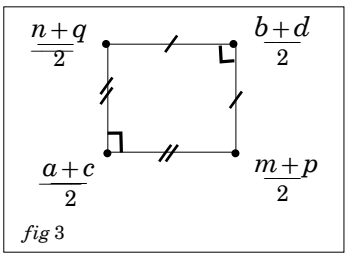


fig 3

Démonstration
Montrons 1.
1.1) L'isométrie $r_n r_m$ est une rotation de mesure d'angle $\pi=\frac{\pi}{2}+\frac{\pi}{2}$; ainsi pour tout $x\in P$, l'élément $\frac{x+r_n r_m(x)}{2}$ est le centre de la rotation $r_m r_n$; en particulier comme $r_n r_m(a)=r_n(b)=c$, il suit que $\frac{a+c}{2}$ est le centre de la rotation. C'est aussi l'homothétie de centre $\frac{a+c}{2}$ et de rapport -1 (fig. 4)

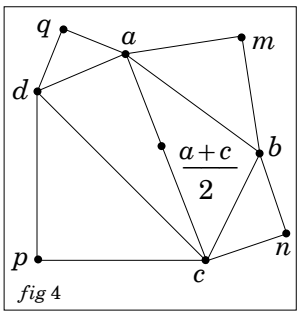


fig 4

De la même façon comme $r_q r_p(c) = a$, il suit que $r_q r_p$ est aussi la rotation de centre $\frac{c+a}{2} = \frac{a+c}{2}$ et de mesure d'angle π .

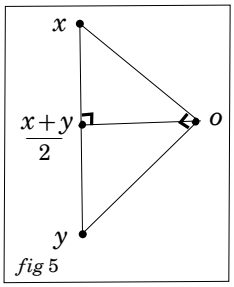


fig 5

1.2) Soient $o \in P$ et ρ la rotation de centre o et de mesure d'angle $\frac{\pi}{2}$. Soient $x \in P - \{o\}$, $y := \rho(x)$, r la rotation de centre $\frac{x+y}{2}$ et de mesure d'angle $-\frac{\pi}{2}$. Alors on a $r(x) = o$ (fig. 5).

1.3) On sait de 1) que $r_n r_m$ est la rotation de centre $\frac{a+c}{2}$ et de mesure d'angle π . On sait aussi de 1.1) que pout $z \in P$, on a $\frac{a+c}{2} = \frac{z + r_n r_m(z)}{2}$, en particulier pour $z = m$, on a $\frac{m + r_n r_m(m)}{2} = \frac{m + r_n(m)}{2}$ et donc $\frac{m + r_n(m)}{2} = \frac{a+c}{2}$ ((fig. 6). Il suit donc de 2) que si $o = n$, $\rho = r_n$, $x = m$ et si r est la rotation de centre $\frac{m + r_n(m)}{2}$ et de mesure d'angle $-\frac{\pi}{2}$, alors $r(m) = n$; par aillleurs il suit de ce qui précède que $\frac{m + r_n(m)}{2} = \frac{a+c}{2}$, ainsi r est la la rotation de centre $\frac{a+c}{2}$ et de mesure d'angle $-\frac{\pi}{2}$ avec $r(m) = n$. De façon analogue, compte tenu de 1.1) , si r est la rotation de centre $\frac{a+c}{2}$ et de mesure d'angle $-\frac{\pi}{2}$, on a $r(p) = q$.

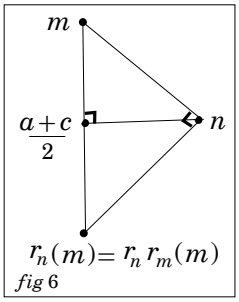


fig 6

1.4) Il suit donc de 1.1) et 1.3) que $r(m) = n$, $r(p) = q$ et $\theta(m - p) = n - q$ si θ est l'élément de $O(T)$ associé à r .
En conséquence, on a bien $\| m - p \| = \| n - q \|$ et $(m - p \mid n - q) = 0$; ce qui est 1.

2) Montrons 2.
2.1) Pour les mêmes raisons qu'en 1.3) , si r' est la rotation centre de $\frac{b+d}{2}$ et de mesure d'angle $-\frac{\pi}{2}$, on a $r'(n) = p$ et $r'(q) = m$.

2.2) Il suit alors de 3) et 4) que $r(\frac{a+c}{2})=\frac{a+c}{2}$, $r(\frac{m+p}{2})=\frac{n+q}{2}$, $r'(\frac{b+d}{2})=\frac{b+d}{2}$, $r'(\frac{n+q}{2})=\frac{p+m}{2}$ (fig. 3).
En résumé pour le quadrilatère de sommets $(\frac{a+c}{2},\frac{m+p}{2},\frac{b+d}{2},\frac{n+q}{2})$, les angles en $\frac{a+c}{2}$ et $\frac{b+d}{2}$ ont pour mesure $\frac{\pi}{2}$ et $\| \frac{m+p}{2}-\frac{a+c}{2} \| = \| \frac{n+q}{2}-\frac{a+c}{2} \|$, $\| \frac{n+q}{2}-\frac{b+d}{2} \| = \| \frac{m+p}{2}-\frac{b+d}{2} \|$.
Il suit facilement de cela que la suite $(\frac{a+c}{2},\frac{m+p}{2},\frac{b+d}{2},\frac{n+q}{2})$ est la suite des sommets d'un carré . Ainsi 2. est satisfait.

3) Montrons 3.
Il reste à montrer l'équivalence des propriétés *i)* et *ii)* ci-après.
i) On a $\frac{m+p}{2}=\frac{n+q}{2}$, *ii)* $a-b=d-c$.
Montrons que i) implique ii).
Il suit de 3) que $r(\frac{m+p}{2})=\frac{n+q}{2}$ et compte tenu de *i)*, cela veut dire que $r(\frac{m+p}{2})=\frac{m+p}{2}$ et donc que $\frac{m+p}{2}=\frac{a+c}{2}$ est le centre de rotation r.
De façon analogue, en utilisant 5) , on a $\frac{n+q}{2}=\frac{b+d}{2}$, il suit donc de *i)* que $a-b=d-c$; i.e. *ii)* est satisfait.

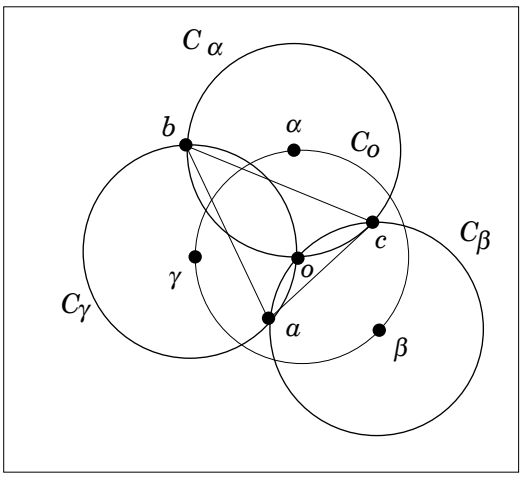
Montrons que ii) implique i).
Il suit de *ii)* que $\frac{a+c}{2}=\frac{b+d}{2}$, ainsi r et r' ont le même centre de rotation et même mesure d'angle, ce qui implique $r=r'$.
Il suit de 3) que $r(\frac{m+p}{2})=\frac{n+q}{2}$ et de 5) que $r'(\frac{n+q}{2})=\frac{p+m}{2}$.
Sachant que $r=r'$, on a $r^2(\frac{m+p}{2})=\frac{p+m}{2}$. Comme $\frac{a+c}{2}$ est le centre de la rotation r^2, on a $\frac{p+m}{2}=\frac{a+c}{2}$. De façon analogue $\frac{q+n}{2}=\frac{b+c}{2}$ Il suit de cela que *ii)* implique *i)*.

[Fr] Fresnel J. *Méthodes modernes en géométrie,* 1996 Hermann

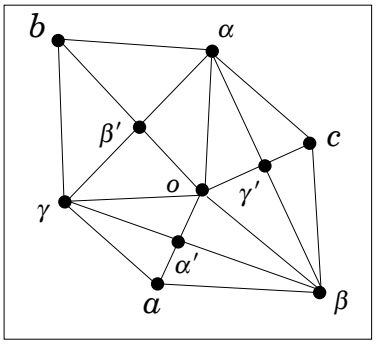
page 299, complément : sur trois cercles passant par un même point

Théorème (Johnson, 1916) *Soient* E *le plan euclidien,* $o \in E$, C_o *le cercle de centre* o *et de rayon* 1 . *Soient* α, β, γ *trois points distincts de* C_o , C_α (resp. C_β, C_γ) *le cercle de centre* α (resp. β, γ) *et de rayon* 1. *Alors le cercle circonscrit à* (a, b, c) *est de rayon* 1. *De plus* o *est l'orthocentre du triangle* (a, b, c) .

Théorème (Johnson, 1916) *Soient* E *le plan euclidien,* $o \in E$, C_o *le cercle de centre* o *et de rayon* 1 . *Soient* α, β, γ *trois points distincts de* C_o , C_α (resp. C_β, C_γ) *le cercle de centre* α (resp. β, γ) *et de rayon* 1. *Alors on a* $C_\alpha \cap C_\beta = \{o, c\}$, $C_\beta \cap C_\gamma = \{o, a\}$, $C_\gamma \cap C_\alpha = \{o, b\}$, *Alors le cercle circonscrit à* (a, b, c) *est de rayon* 1. *De plus* o *est l'orthocentre du triangle* (a, b, c) .



Démonstration



On a $\|o-\alpha\| = \|o-\beta\| = \|o-\gamma\| = 1$, de même $\|a-\beta\| = \|a-\gamma\| = \|b-\gamma\| = \|b-\alpha\| = \|c-\alpha\| = \|c-\beta\| = 1$. Il suit de cela que la droite $V(o, a)$ est la médiatrice de β et γ , que la droite $V(\beta, \gamma)$ est la médiatrice de a et o , ainsi $V(o, a)$ coupe $V(\beta, \gamma)$ en α' qui est le milieu de β et de γ et aussi le milieu de o et a . De même $V(o, b)$ coupe $V(\gamma, \alpha)$ en β' qui est le milieu de γ et de α et aussi le milieu de o et b ; $V(o, c)$ coupe $V(\alpha, \beta)$ enγ' qui est le milieu de α et de β et aussi le milieu de o et c .

Soit h l'homothétie de centre α et de rapport $\frac{1}{2}$, on a donc $h(\beta)=\gamma'$ et $h(\gamma)=\beta'$. Soit k l'homothétie de centre o et de rapport 2, on a donc $k(\gamma')=c$ et $k(\beta')=b$. Il suit de cela que $kh(\beta)=c$ et $kh(\gamma)=b$. Comme le produit des rapports de h et de k est 1, on sait que kh est une translation ([Fr] prop. 4.1.4, partie 4.1.4.2 a.v. p. 39, n.v. p. 43), en particulier on a $\|\beta-\gamma\|=\|b-c\|$. De la même façon on a $\|\gamma-\alpha\|=\|c-a\|$, $\|\alpha-\beta\|=\|a-b\|$. On sait alors qu'il existe une isométrie σ de E avec $\sigma(\alpha)=a$, $\sigma(\beta)=b$, $\sigma(\gamma)=c$ ([Fr] prop. 1.4.3.1, partie 2 a.v. p. 160, n.v. p. 154) ; ainsi le cercle circonscrit à (a,b,c) est isométrique du cercle circonscrit à (α,β,γ), or ce dernier est le cercle de centre o et de rayon 1, il suit de cela que le cercle circonscrit à (a,b,c) est de rayon 1.
Il reste à montrer que o est l'orthocentre du triangle (a,b,c).
Comme $\|\beta-a\|=\|\beta-o\|=\|\gamma-a\|=\|\gamma-o\|=1$, il suit que $V(o,a)$ et $V(\beta,\gamma)$ se coupent orthogonalement en α' qui est milieu de o et a et aussi milieu de β et γ. De même $V(o,b)$ et $V(\gamma,\alpha)$ se coupent orthogonalement en β' qui est milieu de o et b et aussi milieu de γ et α ; $V(o,c)$ et $V(\alpha,\beta)$ se coupent orthogonalement en γ' qui est milieu de o et c et aussi milieu de α et β.
Comme $V(\beta',\gamma')$ est parallèle à $V(\beta,\gamma)$, il suit que $V(o,\alpha')$ est orthogonal à $V(\beta',\gamma')$. De même $V(o,\beta')$ est orthogonal à $V(\gamma',\alpha')$; $V(o,\gamma')$ est orthogonal à $V(\alpha',\beta')$. Ainsi o est orthocentre du triangle (α',β',γ').
Soit h l'homothétie de centre o et de rapport 2, on a $h(\alpha')=a$, $h(\beta')=b$, $h(\gamma')=c$, sachant que h conserve l'orthogonalité, on a $V(o,a)$ orthogonal à $V(b,c)$, $V(o,b)$ orthogonal à $V(c,a)$ et $V(o,c)$ orthogonal à $V(a,b)$; ce qui montre que o est l'orthocentre du triangle (a,b,c).

Remarque Pour des commentaires, on peut consulter [P], p. 332.

[Fr] Fresnel Jean *Méthodes modernes en géométrie*, Hermann, a.v. 1996, n.v. 2010
[J] Johnson Roger A.. *A circle theorem*, The American Mathematical Monthly, Vol. 23, N° 5 (May, 1916), pp. 161-162
[P] Pickover Clifford A. *Le ßeau Livre des Maths*, Dunod, 2010

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) $\deg_T \widetilde{F}(X,Y,Z,T) + \deg_T U(X,Y,Z,T) =$

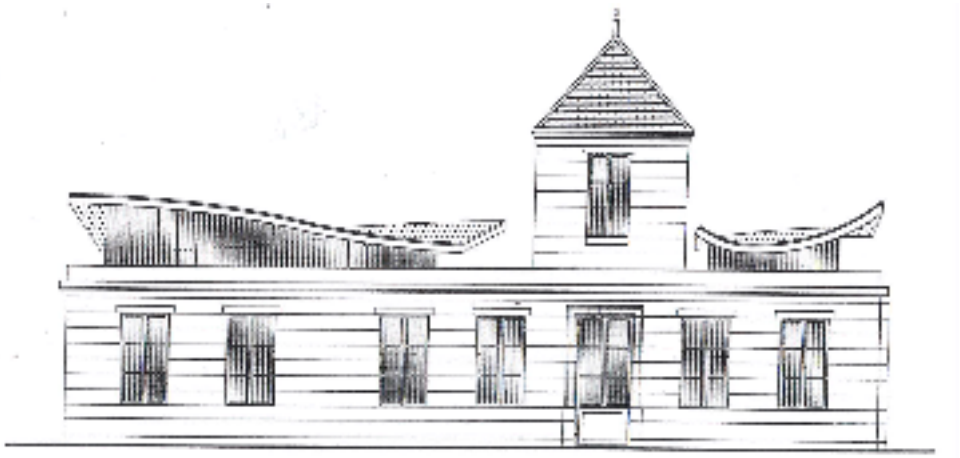
$$\deg_T \widetilde{G}(X,Y,Z,T) + \deg_T V(X,Y,Z,T).$$

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