Groupes finis. Exemples et applications.

Mohamed NASSIRI

Après avoir introduit les généralités sur les groupes finis (*ordre*, *exposant*, ...) et rappelé le très célèbre *théorème de Lagrange*, on parlera des *actions de groupes*. En considérant G un groupe et X un ensemble, on peut définir une action de groupe. Plus précisement, on va dire que G agit (à gauche) sur X si on a

OU

une application α défini par

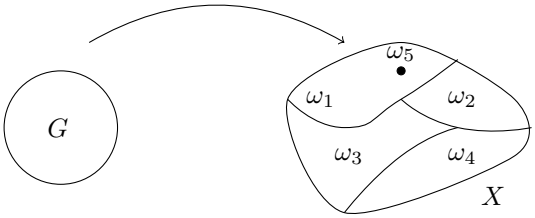
$$\alpha \ : \ G \times X \to X$$
$$(g, x) \mapsto g.x \quad (resp.\ x.g)$$

telle que
$\forall x \in X, \ 1.x = x$
$\forall (g, g') \in G^2, \ \forall x \in X, \ g.(g'.x) = gg'.x$

un morphisme Φ défini par

$$\Phi \ : \ G \to \mathfrak{S}(X)$$
$$g \mapsto \varphi_g \ : \ \begin{cases} X & \to X \\ x & \mapsto g.x \end{cases}$$

Même si la donnée de α et Φ sont équivalentes, il ne faut pas les confondre ! En effet, α n'est pas un morphisme, alors que Φ oui ! Cela provient du fait que X peut être un ensemble quelconque et pas forcément un groupe ...



Une des premières propriétés importantes d'une action de groupe est qu'elle partitionne l'ensemble X.

Les actions de groupes, même les plus simples, sont très efficaces. Par exemple, avec la simple action par translation on obtient le très célèbre théorème de Cayley. L'action par conjugaison nous conduit à deux résutats importants : l'équation aux classes et la formule de Burnside. La première nous donne le théorème de Wedderburn : *"Tout corps fini est commutatif."*.

Le théorème chinois donne des exemples de groupes abéliens finis qui se décomposent en un produit de groupes cycliques plus simples. Par exemple $Z/6Z$ est isomorphe à $Z/2Z * Z/3Z$. D'autre part $(Z/2Z)^2$ est un groupe abélien d'ordre 4 qui n'est pas cyclique puisque tous ses éléments sont d'ordre au plus 2. Il n'est donc pas isomorphe à $Z/4Z$. Un des problèmes que l'on va étudier ici est celui de l'existence et de l'unicité de la décomposition, à isomorphisme près, d'un groupe abélien fini en un produit de groupes cycliques.

La géométrie du triangle est une source intarissable de problèmes, simples dans leur énoncé, mais très difficiles. Du côté des polygones réguliers, on a un résultat sympathique : l'ensemble des points ayant pour affixe les racines n-ièmes de l'unité est l'ensemble des n sommets d'un polygone régulier de centre O et inclus dans le cercle trigonométrique. De plus, avec la notion de *racines primitives*, on a l'interprétation suivante :

Théorème
Soient $m \in \mathbb{N}^*$ et ξ une racine primitive n-ièmes de l'unité dans $\mathbb{C}$. Alors les (autres) racines primitives m-ièmes de l'unité sont les ξ^k, où $1 \leq k \leq n$ $\text{pgcd}(k, n) = 1$.
En particulier, si n est premier, toutes les racines n-ièmes de l'unité dans $\mathbb{C}$ sont primitives.

Interprétation géométrique
Les polygones réguliers étoilés à n sommets d'un seul tenant s'obtiennent en joignant de k en k, avec $\text{pgcd}(k, n) = 1$, les sommets d'un polygone régulier à n sommets.
En particulier, si n est premier, tous les polygones réguliers étoilés à n sommets sont d'un seul tenant.

Après avoir parlé du groupe symétrique et du groupe diédral, on va s'intéresser au groupe des quaternions de norme 1. On sait que $\mathbb{C}$ est algébriquement clos d'après le théorème de D'Alembert-Gauss, donc il est inutile de vouloir chercher un sur-corps de $\mathbb{C}$. Cepedant, si l'on sacrifie la commutativité, on peut créer un sur-corps de $\mathbb{C}$: le corps des quaternions $\mathbb{H}$. Le lien entre quaternions et transformations géométriques est donné par l'isomorphisme :

$$G/\{-1,1\} \xrightarrow{\sim} SO_3(\mathbb{R})$$

Ce qui permet de faire explicitement le lien entre les quaternions et les rotations dans l'espace sont les *formules de rotation d'Olinde Rodrigues.*

Lorsque $X = V$ est un $\mathbb{C}$-espace vectoriel de dimension finie n, on a même une nouvelle théorie : celles des *représentations linéaires de groupes.* Une représentation linéaire d'un groupe G dans V est la donnée d'un morphisme $\rho : G \to \mathrm{GL}(V)$. Ceci correspond à la donnée d'une action linéaire du groupe G sur V :

$$G \times V \to V$$
$$(g, v) \mapsto g.v = \rho(g)(v)$$

Références

[GOUal] Les maths en tête : Algèbre, Xavier Gourdon
[PER] Cours d'algèbre, Daniel Perrin ♠
[TAU] Algèbre pour l'agrégation interne, Patrice Tauvel
[PEY] L'algèbre discrète de la transformée de Fourier, Gabriel Peyré ♠
[MER] Cours de géométrie, Dany-Jack Mercier
[OTZ] Exercices d'algèbre, Pascal Ortiz
[BIA] Mathématiques pour le CAPES et l'Agrégation Interne, Jean de Biasi
[COL] Éléments d'analyse et d'algèbre (et de théorie des nombres), Pierre Colmez
[DEL] Théorie des groupes 2e édition, Jean Delcourt
[ML3al] Mathématiques L3 Algèbre, Aviva Szpirglas

Développements

$SO_3(\mathbb{R})$ et les quaternions
Théorème de Wedderburn
Table des caractères de $\mathfrak{S}_4$ et les isométries du tétraèdre
Noyaux de caractères et sous-groupes distingués

1 Groupes finis

1.1 Définitions et premières propriétés

Définition 1 *Un groupe G est dit fini s'il n'a qu'un nombre fini d'éléments.*
Dans ce cas, le cardinal de G s'appelle l'ordre du groupe G et est noté $|G|$. **[CAL] p.9**

Exemple 2 *Soit $n \in \mathbb{N}^*$. Le groupe des classes de congruence de $\mathbb{Z}$ modulo n est un groupe fini d'ordre n.* **[CAL] p.14**

Définition 3 *Soit G un groupe fini et $g \in G$. Le cardinal du sous-groupe $\langle g \rangle$ s'appelle l'ordre de g dans G et est noté* $\mathrm{ord}(g)$. **[CAL] p.30**

Exemple 4 *Dans le groupe symétrique $\mathfrak{S}_3$ (que l'on définit plus loin)* (12), (23) *et* (13) *sont d'ordre* 2 *et* (123) *et* (132) *sont d'ordre* 3. **[CAL] p.30**

Définition 5 *Soit G un groupe fini. L'exposant de G est le* ppcm *des ordres des éléments de G, et est noté* $\exp(G)$. **[ML3al] p.253**

Proposition 6 *Soif G un groupe abélien fini d'ordre $|G|$ et d'exposant* $\exp(G)$. *Alors $|G|$ et* $\exp(G)$ *ont les mêmes diviseurs premiers.*
En particulier, $|G|$ divise une puissance de $\exp(G)$.
[ML3al] p.253

1.2 Sous-groupes et théorème de Lagrange [CAL] p.71 → 77, p.149 → 152

Proposition-Définition 7 *A tout sous-groupe H d'un groupe G, on peut associer deux relations d'équivalences $\mathcal{R}_H$ et ${}_H\mathcal{R}$, dites respectivement relation d'équivalence à droite et à gauche modulo H dans G, définies dans G par :*

$$x\mathcal{R}_H y \Leftrightarrow xy^{-1} \in H \quad \text{et} \quad x\,{}_H\mathcal{R}\,y \Leftrightarrow x^{-1}y \in H$$

Les ensembles $Hx := \{hx \ ; \ h \in H\}$ et $xH := \{xh \ ; \ h \in H\}$ sont respectivement appelés classes à droite et à gauche de x modulo H.
Les ensembles quotients $\frac{G}{\mathcal{R}_H}$ et $\frac{G}{{}_H\mathcal{R}}$ sont respectivement notés $\left(\frac{G}{H}\right)_d$ et $\left(\frac{G}{H}\right)_g$.

Le cardinal de $\left(\frac{G}{H}\right)_d$ $\left(= \text{card}\left(\left(\frac{G}{H}\right)_d\right)\right)$ *s'appelle l'indice de H dans G et se note* $[G : H]$.

Définition 8 *Dans un groupe G, un sous-groupe H est dit distingué (ou normal) si* $\mathcal{R}_H = {}_H\mathcal{R}$. *On notera* $H \lhd G$.
Si $H \lhd G$, *le groupe* $\frac{G}{H}$ *est appelé groupe quotient de G par le sous-groupe distingué H.*

Théorème 9 *Théorème de Lagrange*
Si G est un groupe fini, alors l'ordre de tout sous-groupe H de G divise l'ordre de G (i.e.)

$$|G| = [G : H]|H|$$

Théorème 10 *Dans un groupe G, on a* $H \lhd G$ *si et seulement s'il existe un groupe G' et un morphisme* $f \in \text{Hom}(G, G')$ *tel que* $H = \text{Ker} f$.

Proposition 11 *Soient G un groupe et H un sous-groupe de G, alors :*

$$[G : H] = 2 \;\Rightarrow\; H \lhd G$$

Exemple 12 *Dans tout groupe G,* $\{e\}$ *et G sont distingués.*
Dans un groupe abélien, tout sous-groupe est distingué.

1.3 Actions de groupe [ML3al] p.238 → 242

Dans cette partie, G est un groupe et X un ensemble.

Définition 13 *On dit que G agit à gauche (resp. à droite) sur X si on a une application*

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g.x \quad (resp.\ x.g) \end{aligned}$$

telle que
(i) $\forall x \in X,\ 1.x = x \quad (resp.\ x.1 = x)$
(ii) $\forall (g, g') \in G^2,\ \forall x \in X,\ g.(g'.x) = gg'.x \quad (resp.\ (x.g).g' = x.gg')$

Remarque 14 *(i) Dans la suite, on considère les actions à gauche.*
(ii) Se donner une action de groupe, c'est se donner un morphisme Φ *défini par*

$$\begin{aligned} \Phi \;:\; G &\to \mathfrak{S}(X) \\ g \mapsto \varphi_g \;:\; &\begin{cases} X & \to X \\ x & \mapsto g.x \end{cases} \end{aligned}$$

Exemple 15 *Soit G un groupe (noté multiplicativement). La multiplication (ou translation) à gauche :*

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto g.h = gh \end{aligned}$$

est une action de groupe.

Définition 16 *On dit que l'action est fidèle si*

$$(\forall x \in X,\ g.x = x) \Rightarrow g = 1$$

Elle est dite transitive si

$$(\forall x, y \in X, \exists g \in G \text{ tel que } g.x = y)$$

Définition 17 *La relation*

$$x \mathcal{R} y \Leftrightarrow \exists g \in G \text{ tel que } g.x = y$$

est une relation d'équivalence et ses classes sont appelées orbites de G sous X. L'orbite d'un élément $x \in X$ *est noté* $\omega(x)$.

Définition 18 *Le stabilisateur de x, noté* $\text{Stab}(x)$, *est le sous-groupe de G défini par*

$$\text{Stab}(x) = \{g \in G \mid g.x = x\}$$

On dit que x est un point fixe pour l'action de G si $\text{Stab}(x) = G$.

Exemple 19 *Soit G un groupe (noté multiplicativement). La conjugaison :*

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto g.h = ghg^{-1} \end{aligned}$$

est une action de groupe.
Les orbites sont appelées classes de conjugaison et le stabilisateur de x est appelé centralisateur (noté $C_G(x)$*).*

Théorème 20 *Théorème de Cayley*
Tout groupe est isomorphe à un sous-groupe de permutations.

Proposition 21 *Les orbites de X sous l'action de G forment une partition de X et il existe une bijection*

$$\begin{aligned} f_x \;:\; G\backslash\text{Stab}(x) &\to \omega(x) \\ g\text{Stab}(x) &\mapsto g.x \end{aligned}$$

De plus, l'action induite sur $\omega(x)$ *est compatible avec l'action naturelle de G sur le quotient* $G\backslash\text{Stab}(x)$ *dans le sens suivant :*

$$\forall \kappa \in G\backslash\text{Stab}(x),\ \forall g \in G,\quad f_x(g\kappa) = g.f_x(\kappa)$$

Corollaire 22 *Si G et X sont finis, alors* $\text{Card}(\omega(x))$ *divise* $|G|$.

Proposition 23 *Si* $x, y \in X$ *sont dans la même orbite, alors* $\text{Stab}(x)$ *et* $\text{Stab}(y)$ *sont conjugués.*

Proposition 24 *Equation aux classes*
On a l'égalité

$$|G| = |Z(G)| + \sum_i \text{Card}(\omega_i)$$

où la somme porte sur toutes les classes de conjugaison de cardinal strictement supérieur à 1.

Corollaire 25 *(i) Si G est un p-groupe, on a $|Z(G)| \geq p$.*
(ii) Tout groupe d'ordre p^2 est abélien.

Application 26 ♠ *Théorème de Wedderburn* ♠
Tout corps fini est commutatif. **[PER] p.82**

Proposition 27 *On suppose que G est un p-groupe et que X est fini. Soit*

$$X^G = \{x \in X \mid \forall g \in G,\ g.x = x\}$$

l'ensemble des points fixes de X sous l'action de G. Alors

$$\text{Card}(X) \equiv \text{Card}(X^G) \pmod{p}$$

Définition 28 *On pose, pour $g \in G$,*

$$\text{Fix}(g) = \{x \in X \mid g.x = x\}$$

Remarque 29 *On a, par définition,*

$$X^G = \bigcap_{g \in G} \text{Fix}(g)$$

Proposition 30 *Formule de Burnside*
On suppose G et X finis. Alors

$$\sum_{g \in G} \text{Card}(\text{Fix}(g)) = \sum_{x \in X} |\text{Stab}(x)|$$

Le nombre d'orbites de X sous l'action de G, noté $\text{Card}(\text{Orb}_X(G))$, est donné par la formule :

$$\text{Card}(\text{Orb}_X(G)) = \frac{1}{|G|} \sum_{g \in G} \text{Card}(\text{Fix}(g))$$

2 Exemples de groupes finis

2.1 Groupes abéliens finis

2.1.1 Groupes cycliques [ML3ag] p.233-234

Définition 31 *Un groupe G de cardinal fini est dit cyclique s'il est engendré par un seul élément (i.e.) s'il existe $g \in G$ tel que*

$$G = \{g^n \ ;\ n \in \mathbb{Z}\}$$

Proposition 32 *Si le groupe G est cyclique, alors il est abélien.*

Proposition 33 *Les groupes cycliques sont les $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{Z}^*$.*

Proposition 34 *Soient $G_1, ..., G_n$ des groupes cycliques d'ordres respectifs $\alpha_1, ..., \alpha_n$. Alors le groupe $G = G_1 \times ... \times G_n$ est cyclique si et seulement si les α_i sont premiers entre eux deux à deux.* **[GOUal] p.24**

2.1.2 Théorème de structure des groupes abéliens finis

Théorème 35 (admis) *Théorème de structure des groupes abéliens finis*
Si G est un groupe abélien fini, il existe un entier $r \in \mathbb{N}$, et des entiers $N_1, ..., N_r$, où N_1 est l'exposant de G et $N_{i+1} \mid N_i$ si $i \leq r-1$, tels que

$$G \cong \bigoplus_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$$

[COL] p.251-252

Exemple 36 *Soit G le groupe*

$$G = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$$

Alors

$$G \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$

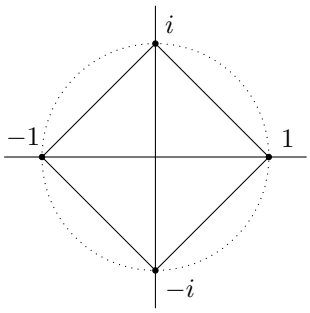
[DEL] p.111-112

2.1.3 Racines n-ième de l'unité et polygones réguliers [BIA] p.79-80

Définition 37 *Soit $n \in \mathbb{N}^*$. On note l'ensemble $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ des racines n-ièmes de l'unité dans $\mathbb{C}$.*
On appelle racine primitive n-ièmes de l'unité tout générateur de $\mathbb{U}_n$.
On note $\mathcal{U}_n(\mathbb{C})$ l'ensemble des racines primitives n-ièmes de l'unité et $\mathcal{P}_n$ l'ensemble des points ayant pour affixe les racines n-ièmes de l'unité.

Proposition 38 *$\mathcal{P}_n$ est l'ensemble des n sommets d'un polygone régulier de centre O et inclus dans le cercle trigonométrique.*

Exemple 39 $\mathcal{U}_n(\mathbb{C}) = \{1, -1, i, -i\}$.



Proposition 40 *Soient $m \in \mathbb{N}^*$ et ξ une racine primitive n-ièmes de l'unité dans $\mathbb{C}$. Alors les (autres) racines primitives m-ièmes de l'unité sont les ξ^k, où $1 \leq k \leq n$ $\text{pgcd}(k, n) = 1$.*
En particulier, si n est premier, toutes les racines n-ièmes de l'unité dans $\mathbb{C}$ sont primitives.

Remarque 41 *Interprétation géométrique*
Les polygones réguliers étoilés à n sommets d'un seul tenant s'obtiennent en joignant de k en k, avec $\text{pgcd}(k,n)=1$*, les sommets d'un polygone régulier à n sommets.*
En particulier, si n est premier, tous les polygones réguliers étoilés à n sommets sont d'un seul tenant. Voir Figure 1, Figure 2 *et* Figure 3.

2.2 Groupes symétriques

2.2.1 Définitions et premières propriétés [TAU] p.45→47

Définition 42 *Soit E un ensemble. Une bijection de E sur lui-même est appelée une permutation de E. On note l'ensemble des permutations de E* $\mathcal{S}(E)$*. Lorsque* $E=[\![1,...,n]\!]$*, on note* $\mathcal{S}_n=\mathcal{S}(E)$*.*
Un permutation σ *sera notée :*

$$\sigma=\begin{pmatrix}1 & 2 & ... & n-1 & n\\ \sigma(1) & \sigma(2) & ... & \sigma(n-1) & \sigma(n)\end{pmatrix}$$

Remarque 43 *On se place dans le cadre* $\mathcal{S}_n$*.*

Proposition 44 *Muni de la composition des applications,* $\mathcal{S}_n$ *est un groupe, appelé groupe symétrique, et on a* $|\mathcal{S}_n|=n!$*.*

Proposition 45 *Théorème de Cayley : Tout groupe fini G de cardinal est isomorphe à un sous-groupe de* $\mathcal{S}_n$*.*

Définition 46 *Pour* $x\in[\![1,...,n]\!]$*,* $\sigma\in\mathcal{S}_n$*, on note* $\mathcal{O}_\sigma(x)=\{\sigma^k(x);k\in\mathbb{Z}\}$ *et on dit que* $\mathcal{O}_\sigma(x)$ *est une* σ*-orbite de x.*

Exemple 47 *Soit* $\sigma\in\mathcal{S}_7$ *définie par :*

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&4&6&7&5\end{pmatrix}$$

On a $\mathcal{O}_\sigma(1)=\{1,2,3\}$*,* $\mathcal{O}_\sigma(4)=\{4\}$ *et* $\mathcal{O}_\sigma(5)=\{5.6.7\}$*.*

Définition 48 *On dit que* $\sigma\in\mathcal{S}_n$ *est un cycle s'il existe une unique orbite* $\mathcal{O}$ *tel que* $\text{card}(\mathcal{O})>1$*.*
Alors, le cardinal de $\mathcal{O}$ *est appelé la longueur du cycle et* $\mathcal{O}$ *son support.*
Un q-cycle est un cycle de longueur q et un 2-cycle est une transposition.

Exemple 49 *Soient* $\sigma,\tau\in\mathcal{S}_5$ *définies par :*

$$\sigma=\begin{pmatrix}1&2&3&4&5\\1&3&4&2&5\end{pmatrix}\quad\tau=\begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix}$$

Alors σ *est un 3-cycle et* τ *une transposition.*

Proposition 50 *Soit* $\sigma,\tau\in\mathcal{S}_n$*,* $\mathcal{O}$ *une* σ*-orbite de cardinal* $p>1$*. Si* $a\in\mathcal{O}$*, on a* $\mathcal{O}=\{a,\sigma(a),...\sigma^{p-1}(a)\}$*, et* $\sigma^p(x)=x$ *pour tout* $x\in\mathcal{O}$*. Si* σ *est un cycle, il est donc d'ordre p.*

Remarque 51 *Un p-cycle dont l'unique orbite non trivial est* $\{a_1,...,a_p\}$ *avec* $a_i=s^{i-1}(a_1)$ *pour* $1\leq i\leq p$ *sera noté* $(a_1...a_p)$

Proposition 52 • *Soient* s,t *des p-cycles. Il existe* $u\in\mathcal{S}_n$ *telle que* $t=usu^{-1}$
• *Deux cycles à support disjoints commutent.*

Proposition 53 *Principe de conjugaison : Si* $\sigma=(a_1...a_p)\in\mathcal{S}_n$ *est un cycle d'ordre p et* $\tau\in\mathcal{S}_n$*, on a*

$$\tau\sigma\tau^{-1}=(\tau(a_1)...\tau(a_p))$$

[PER] p.15

Corollaire 54 *Classes de conjugaisons de Sn*

2.2.2 Décompositions et parties génératrices [TAU] p.47

Théorème 55 *Tout* $\sigma\in\mathcal{S}_n$ *différent de l'identité est produit de cycles à supports deux à deux disjoints, et un tel produit est unique à l'ordre près des facteurs.*

le ppcm des longueurs de ces derniers est égal à l'ordre de la permutation

Exemple 56

$$\sigma=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(12)(34)$$

Théorème 57 ♠ *Générateurs de* $\mathcal{S}_n$ ♠
Soit $n\geq 2$*.*
(i) Les transpositions engendrent $\mathcal{S}_n$*.*
(ii) L'ensemble $\{(1\ i),2\leq i\leq n\}$ *engendre* $\mathcal{S}_n$*.*
(iii) Le nombre minimal de transpositions engendrant $\mathcal{S}_n$ *est* $n-1$*.*

Corollaire 58 *(i) L'ensemble* $\{(i\ i+1),1\leq i\leq n-1\}$ *engendre* $\mathcal{S}_n$*.*
(ii) La transposition $(1\ 2)$ *et le n-cycle* $(1\ 2...n)$ *engendrent* $\mathcal{S}_n$*.*

2.2.3 Le groupe alterné [GOUal] p.21

Définition 59 *Soit* $\sigma\in\mathcal{S}_n$*. On appelle signature de* σ *le produit*

$$\epsilon(\sigma)=\prod_{1\leq i<j\leq n}\frac{\sigma(j)-\sigma(i)}{j-i}$$

Proposition 60 *Soient* $\sigma,\tau\in\mathcal{S}_n$*. Alors*
(i) $\epsilon(\sigma)\in\{-1,1\}$*,*
(ii) $\epsilon(\sigma\tau)=\epsilon(\sigma)\epsilon(\tau)$*.*

Proposition 61 ϵ *est l'unique morphisme de groupe non trivial de* $\mathcal{S}_n$ *dans* $\mathbb{R}^*$*.*

Définition 62 *On définit le groupe alterné* $\mathcal{A}_n=\text{Ker}\epsilon$*.*

Proposition 63 *$\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ et on a $|\mathcal{A}_n| = n!/2$*

Proposition 64 *Pour $n \geq 3$,*
(i) $Z(\mathcal{S}_n) = \{Id\}$, et $\mathcal{S}_n$ n'est pas abélien.
(ii) $\mathcal{A}_n$ est engendré par les permutations $(1\ i)(1\ j)$, où $2 \leq i, j \leq n$.
(ii) $\mathcal{A}_n$ est engendré par les 3-cycles de la forme $(1\ 2\ i)$, où $3 \leq i \leq n$.
$\mathcal{A}_n$ est engendré par les éléments σ^2, $\sigma \in \mathcal{S}_n$.
[TAU] p.49

Théorème 65 *$\mathcal{A}_n$ est simple pour $n \geq 5$*

2.3 Le groupe diédral [MER] p.304 → 311

Définition 66 *On appelle groupe diédral D_n le groupe des isométries du plan qui conservent un polygone régulier P_n à n côtés.*

Théorème 67 *Le groupe diédral D_n est un groupe fini d'ordre $2n$ engendré par un élément r d'ordre n et un élément s d'ordre 2.*
Il contient n rotations d'angle $\frac{k\pi}{n}$, $k = 0, ..., n-1$ ainsi que n symétries. En notant r la rotation d'angle $\frac{2\pi}{n}$ et s une des symétries, on a

$$r^n = 1 \qquad s^2 = 1 \qquad (sr)^2 = 1$$

Exemple 68 *Le groupe du triangle équilatéral est isomorphe au groupe $\mathfrak{S}_3$ des permutations d'un ensemble de trois éléments. On peut donc écrire*

$$D_3 \approx \mathfrak{S}_3$$

Remarque 69 *On peut identifier les isométries de $\mathrm{Is}(P_n)$ à leurs parties linéaires et aux matrices de ces parties linéaires dans une base orthonormale directe. On a donc*

$$\mathrm{Is}^+(P_n) = \left\{ \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} \ ; \ k = 0, ..., n-1 \right\}$$

$$\mathrm{Is}^-(P_n) = \left\{ \begin{pmatrix} \cos k\theta & \sin k\theta \\ \sin k\theta & -\cos k\theta \end{pmatrix} \ ; \ k = 0, ..., n-1 \right\}$$

Proposition 70 *Les classes de conjugaison du groupe diédral D_n sont :*
- Pour n est pair : on a $\frac{n}{2}+3$ classes de conjugaison

$$\{Id\}, \{-Id\}, \{r, r^{n-1}\}, ..., \{r^{n/2-1}, r^{n/2+1}\}$$

$$\{s, sr^2, ..., sr^{n-2}\}, ..., \{sr, sr^3, ..., s^{n-1}\}$$

- Pour n est impair : on a $\frac{n+1}{2}+1$ classes de conjugaison

$$\{Id\}, \{r, r^{n-1}\}, ..., \{r^{\frac{n-1}{2}}, r^{\frac{n+1}{2}}\}$$

$$\{s, sr, sr^2, ..., sr^{n-1}\}$$

[OTZ] p.17

2.4 Groupe des quaternions de norme 1 [PER] p.160 → 164

Proposition-Définition 71 *Il existe une algèbre $\mathbb{H}$ de dimension 4 sur $\mathbb{R}$, appelé algèbre des quaternions, muni d'une base 1,i,j,k telle que :*
(i) 1 est élément neutre pour la multiplication,
(ii) on a les formules

$$jk = -kj = i, \quad ki = -ik = j, \quad ij = -ji = k$$

$$i^2 = j^2 = k^2 = -1$$

Un quaternions s'écrit alors

$$q = a + bi + cj + dk, \quad avec\ a, b, c, d \in \mathbb{R}$$

Définition 72 *$\mathbb{H}$ est muni de la norme algébrique N suivante : $\forall\ q = a + bi + cj + dk \in \mathbb{H}$*

$$N(q) = a^2 + b^2 + c^2 + d^2$$

Proposition 73 *Le groupe G des quaternions de norme 1 est le groupe*

$$\{\pm 1, \pm i, \pm j, \pm k\}$$

Ce groupe est d'ordre 8 et non abélien.

Théorème 74 ♠ *$SO_3(\mathbb{R})$ et les quaternions* ♠
Soit G le groupe des quaternions de norme 1. On a l'isomorphisme suivant :

$$G/\{-1, 1\} \xrightarrow{\sim} SO_3(\mathbb{R})$$

3 Représentations linéaires de groupes

3.1 Définitions et premières propriétés [PEY] p.194 → 205

Définition 75 *Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n. Une représentation linéaire d'un groupe G dans V est la donnée d'un morphisme $\rho : G \to \mathrm{GL}(V)$. Ceci correspond à la donnée d'une action linéaire du groupe G sur V :*

$$G \times V \to V$$
$$(g, v) \mapsto g.v = \rho(g)(v)$$

Une représentation ρ est dite fidèle si G agit fidèlement sur V.

Exemple 76 *Fort de l'isomorphisme $Is(\Delta_4) \approx \mathfrak{S}_4$, on peut établir une représentation du groupe $\mathfrak{S}_4$ sur l'espace vectoriel $\mathbb{R}^3$ comme un groupe de transformations orthogonales.*

Définition 77 • *Soient ρ et ρ' deux représentations d'un même groupe G respectivement sur deux $\mathbb{C}$-espace vectoriel V et V'. Un opérateur d'entrelacement est une application linéaire $\tau : V \to V'$ tel que pour tout $g \in G$, $\tau \circ \rho(g) = \rho'(g) \circ \tau$*

$$\begin{array}{ccc} V & \xrightarrow{\tau} & V' \\ {\scriptstyle \rho(g)}\downarrow & & \downarrow{\scriptstyle \rho'(g)} \\ V & \xrightarrow{\tau} & V' \end{array}$$

• *Deux représentations ρ et ρ' d'un même groupe G respectivement sur deux $\mathbb{C}$-espace vectoriel V et V' sont dites isomorphes si τ est bijective.*

Définition 78 • *Si une représentation ρ de G sur V admet un sous-espace vectoriel $W \subset V$ stable pour tous les $\rho(g) \in \mathrm{GL}(V)$, elle induit une représentation ρ_W sur W appelée sous-représentation.*
• *Une représentation sur un espace V est dite irréductible si elle admet exactement deux sous-représentations : $\{0\}$ et V tout entier.*

Proposition 79 *Toute représentation peut s'écrire comme somme de représentations irréductibles.*

Proposition 80 *Lemme de Schur :*
Soient ρ et ρ' deux représentations irréductibles d'un groupe G respectivement sur deux $\mathbb{C}$-espace vectoriel V et V' et $f \in \mathcal{L}(V, V')$ un opérateur d'entrelacement. Alors
(i) si ρ et ρ' ne sont pas isomorphes, $f = 0$.
(ii) Si $f \neq 0$, alors f est un isomorphisme.
Si on suppose $V = V'$, alors f est une homothétie.

3.2 Caractères [PEY] p.207 → 226

Définition 81 *Soit ρ une représentation d'un groupe G sur un $\mathbb{C}$-espace vectoriel V de dimension n.*
On lui associe son caractère χ_ρ défini par $\chi_\rho(g) = \mathrm{tr}(\rho(g))$, où tr désigne la trace.
C'est une fonction de G dans $\mathbb{C}$, (i.e.) $\chi_\rho \in \mathbb{C}[G]$.

Proposition 82 *Soient χ_ρ et $\chi_{\rho'}$ deux caractères de représentations irréductibles. Alors*
(i) χ_ρ est le caractère d'une représentation irréductible si et seulement si

$$\langle \chi_\rho, \chi_\rho \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \overline{\chi_\rho(g)} = 1$$

(ii) Si χ_ρ et $\chi_{\rho'}$ deux caractères de représentations irréductibles non isomorphes, alors $\langle \chi_\rho, \chi_{\rho'} \rangle = 0$

Proposition 83 *En notant $(\chi_i)_{i=1}^p$ les caractères irréductibles de G et $(C_i)_{i=1}^p$ les classes de conjugaison de G, on a :*
(i) Formule de Burnside : $\sum_{i=1}^p \chi_i(1)^2 = |G|$
(ii) Orthogonalité des caractères :
$\sum_{i=1}^p \chi_i(C_k)\overline{\chi_i(C_l)} = 0$ pour $k \neq l$.

Définition 84 *Une table des caractères est un tableau constitué des éléments de la matrice $(\chi_i(C_j))_{1 \leq i,j \leq p}$.*

	1 *1*	$\lvert C_1 \rvert$ C_1	...	$\lvert C_p \rvert$ C_p
$\chi_1 = \mathbb{1}$	*1*	*1*	...	*1*
χ_2	$\chi_2(1)$	$\chi_2(C_2)$	...	$\chi_2(C_p)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_p	$\chi_p(1)$	$\chi_p(C_2)$	...	$\chi_p(C_p)$

3.3 Noyau de caractères [PEY] p.230 → 232

Proposition 85 *Soit G un groupe fini et $\rho : G \to \mathrm{GL}(V)$ une représentation, de caractère χ_V sur un espace V de dimension d. On note $g \in G$ un élément d'ordre k. Alors :*
(i) $\rho(g)$ est diagonalisable.
(ii) χ_V est somme de $\chi_V(1) = \dim V = d$ racines k^{ieme} de l'unité.
(iii) $|\chi_V(g)| \leq \chi_V(1) = d$.
(iv) $K_{\chi_V} := \{g \in G \mid \chi_V(g) = \chi_V(1)\}$ est un sous-groupe distingué de G. On le nomme le noyau de la représentation.

Proposition 86 ♠ *Noyaux de caractères et sous-groupes distingués* ♠
Soient G un groupe fini, et $\widehat{G} = \{\rho_1, ..., \rho_r\}$ son dual, formé de représentants des représentations irréductibles non isomorphes. Les sous-groupes dinstingués d'un groupe fini G sont exactement du type

$$\bigcap_{i \in I} \{g \in G \mid \chi_i(g) = \chi_i(e)\} \text{ où } I \subset \{1, ..., r\}$$

Corollaire 87 ♠ *G est simple si et seulement si pour tout $i \neq 1$, pour tout $g \in G \backslash \{e\}$, $\chi_i(g) = \chi_i(e)$.*

Illustrations

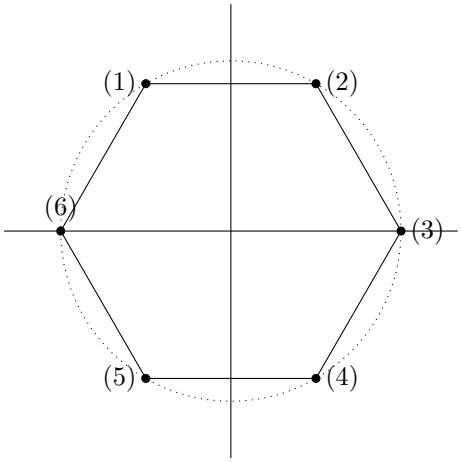


Figure 1 : Polygone régulier étoilé d'un seul tenant avec $n = 6$ et $k = 5$.

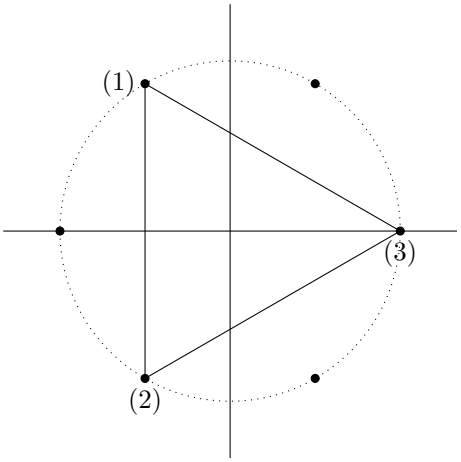


Figure 2 : Echec du polygone régulier étoilé d'un seul tenant avec $n = 6$ et $k = 2$.

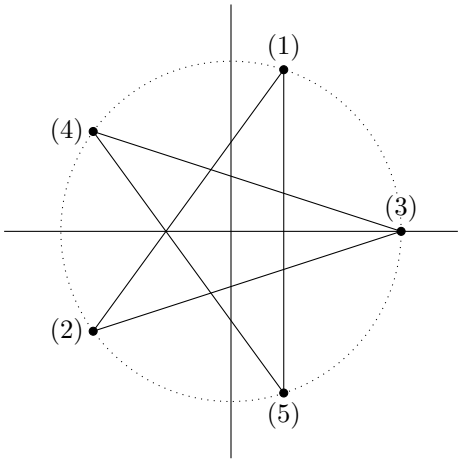


Figure 3 : Polygone régulier étoilé d'un seul tenant avec $n = 5$ et $k = 2$.

Questions

Exercice : Soit G un groupe abélien fini. Montrer que :
(i) Si $g \in G$ est d'ordre a, et si $h \in G$ est d'ordre b, et si a et b sont premiers entre eux, alors xy est d'ordre ab.
(ii) Si $a, b \in \mathbb{N}^*$, et si G contient des éléments d'ordre a et b, alors G contient un élément d'ordre $\text{ppcm}(a, b)$.
(iii) Soit N le maximum des ordres des élements de G. Alors $g^N = e$ pour tout $g \in G$.

Solution : (i) Comme g et h commutent, on a $(xy)^n = x^n y^n$ pour tout $n \in \mathbb{N}$. En particulier

$$(xy)^{ab} = x^{ab} y^{ab} = 1$$

Donc l'ordre de xy divise ab.
Réciproquement, si $(xy)^n = 1$, alors

$$1 = (xy)^{an} = y^{an} \quad \text{et} \quad 1 = (xy)^{bn} = x^{bn}$$

Ainsi an est un multiple de b et bn est un multiple de a. Mais comme a et b sont premiers entre eux, alors n est multiple de a et b, donc aussi de ab $(i.e.)$ l'ordre de xy est un multiple de ab.
Donc l'ordre de xy est ab.

(ii) Soit $\mathcal{P}_1$ (resp. $\mathcal{P}_2$) l'ensemble des p premiers tels que $v_p(a) > 0$ et $v_p(a) \geq v_p(b)$ (resp. $v_p(b) > v_p(a)$). Alors $\mathcal{P}_1$ et $\mathcal{P}_2$ sont disjoints et donc

$$k = \prod_{p \in \mathcal{P}_1} p^{v_p(a)} \quad \text{et} \quad l = \prod_{p \in \mathcal{P}_2} p^{v_p(b)}$$

sont premiers entre eux. De plus, on a

$$v_p(kl) = v_p(a), \text{ si } v_p(a) \geq v_p(b) \quad \text{et} \quad v_p(kl) = v_p(b), \text{ si } v_p(b) > v_p(a)$$

et donc $kl = \text{ppcm}(a, b)$.
Considérons $g \in G$ est d'ordre a, et si $h \in G$ est d'ordre b. Comme $k \mid a$, alors $g' = g^{\frac{a}{k}}$ est d'ordre k. De même $h' = h^{\frac{a}{l}}$ est d'ordre l. Par ce qui précède, on a que $g'h'$ est d'ordre $kl = \text{ppcm}(a, b)$.

(iii) D'après (ii), G contient un élément d'ordre $\text{ppcm}(a, N)$ avec $g \in G$ un élément d'ordre a. Comme $\text{ppcm}(a, N) \geq N$, on a donc $\text{ppcm}(a, N) = N$ (par définition de N) et donc que $a \mid N$. D'où le résultat.

Exercice : Exposant d'un groupe
$1)a)$ Donner un exemple de groupe tel que tout élément de ce groupe soit d'ordre fini, alors que le cardinal de ce groupe est infini.
$b)$ Donner un exemple de groupe tel que l'exposant de ce groupe soit fini, alors que le cardinal de ce groupe est infini.
2) Soit G un groupe. Montrer que si $(\exp(G) = 2)$ alors (G est abélien).
3) Soit G un groupe abélien fini d'ordre $|G|$ et d'exposant $\exp(G)$. Montrer que $|G|$ et $\exp(G)$ ont les mêmes diviseurs premiers. En particulier, $|G|$ divise une puissance de $\exp(G)$.
4) Montrer qu'un sous-groupe de $\text{GL}_n(\mathbb{C})$ est fini si et seulement si son exposant est fini.

Solution : $1)a)$ Tout élément de $\mathbb{Q}/\mathbb{Z}$ est d'ordre fini (pour tout nombre rationnel $\frac{p}{q} \in \mathbb{Q}$, on a $q\overline{\frac{p}{q}} = \overline{0}$), bien que $|\mathbb{Q}/\mathbb{Z}| = +\infty$.
$b)$ En considérant $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$, manifestement, $\exp((\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}) = 2$, alors que $|(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}| = +\infty$.

2) On suppose que pour tout $x \in G$, on a $x^2 = 1$ (*i.e.*) $x^{-1} = x$. Par ailleurs, pour $x, y \in G$ on a

$$(xy)^2 = xyxy = 1$$

En multipliant à gauche par $x^{-1} = x$ et à droite par $y^{-1} = y$, on obtient $yx = xy$, et donc G est abélien.

3) Soit p un diviseur premier de $\exp(G)$. Par définition, il existe $g \in G$ tel que p divise l'ordre de g, et par le théorème de Lagrange, $p \mid |G|$.
Pour démontrer la réciproque, on raisonne par récurrence sur $|G| = n$.
Pour $n = 1$, le résultat est évident.
On suppose le résultat vrai jusqu'au rang $n-1$ et on le montre au rang n.
- Si G est cyclique, le résultat est acquis.
- Sinon, il existe un élément $g \neq e$ de G engendrant un sous-groupe non trivial (*i.e.*) $H = \langle g \rangle$ avec $|H| = q$ $(1 < q < n)$. Si p est un diviseur premier qui divise n, soit $p \mid q = \text{ord}(g)$, soit $p \mid k/q$. Or $|G/H| = k$, et par hypothèse de récurrence, tout diviseur premier de k divise l'ordre d'un élément de G/H, donc divise encore l'ordre de cet élément dans G. D'où le résultat.

4) On aura besoin de la caractérisation (que l'on ne démontre pas !) des endormorphismes nilpotents suivante :

Proposition :
Soient E un $\mathbb{C}$-.e.v. de dimension n et $f \in \mathcal{L}(E)$ tel que car$K = 0$, alors

$$f \text{ est nilpotent} \Leftrightarrow \forall k \in [\![1, n]\!],\ \text{Tr}(u^k) = 0$$

$\Rightarrow$: Si G est fini, alors $\exp(G) \leq |G|$ d'après le théorème de Lagrange, et donc $\exp(G)$ est fini.

$\Leftarrow$: Supposons donc $\exp(G) = e < +\infty$. On note $\mathcal{G}$ la sous-algèbre de $\mathcal{L}(\mathbb{C}^n)$ engendrée par G. Elle a donc un nombre fini de générateurs que l'on note $v_1, ..., v_r$.

Ou ... On peut aussi voir la chose de la façon suivante : On note vect(G), le sous-espace de $\mathcal{M}_n(\mathbb{C})$ engendrée par G (c'est en particulier un $\mathbb{C}$-.e.v. de dimension finie, comme s.e.v. de $\mathcal{M}_n(\mathbb{C})$). Par constuction, les éléments de G forment une famille génératrice de vect(G). On peut donc en extraire une sous-famille finie à la fois libre et génératrice $v_1, ..., v_r$ qui formera une base du $\mathbb{C}$-.e.v. vect(G). Ainsi tout $v \in G \subset \text{vect}(G)$ s'écrira comme une combinaison linéaire non triviale des éléments $v_1, ..., v_r$.

Considérons l'application

$$\begin{aligned} T : G &\to \mathbb{C}^r \\ u &\mapsto (\text{Tr}(u \circ v_1), ..., \text{Tr}(u \circ v_r)) \end{aligned}$$

Montrons que cette application est injective et d'image finie (ainsi, on aura que G est fini !).
Supposons donc $T(u) = T(w)$. Alors,

$$\begin{aligned} \text{Tr}(u \circ v_i) = \text{Tr}(w \circ v_i),\ \ \forall i = 1, ..., r \quad &\Rightarrow \quad \text{Tr}(u \circ v) = \text{Tr}(w \circ v),\ \ \forall v \in \mathcal{G} \\ &\Rightarrow \quad \text{Tr}(u \circ v) = \text{Tr}(w \circ v),\ \ \forall v \in G \\ &\Rightarrow \quad \text{Tr}(u \circ v - w \circ v) = 0,\ \ \forall v \in G \\ &\Rightarrow \quad \text{Tr}[(u \circ w^{-1} - \text{Id}) \circ w \circ v] = 0,\ \ \forall v \in G \end{aligned}$$

Considérons l'endomorphisme $n = u \circ w^{-1} - \text{Id}$ et montrons que $n = 0$ (et on aura donc l'injectivité !) en montrant qu'il est diagonalisable et nilpotent.
n est diagonalisable car $u \circ w^{-1}$ est diagonalisable car c'est un élément de G (et les éléments de G sont annulés par le polynôme $X^e - 1$ qui est scindé à racines simples).

De plus,

$$\begin{aligned}
\mathrm{Tr}(n^p) &= \mathrm{Tr}((u\circ w^{-1}-\mathrm{Id})^p)\\
&= \mathrm{Tr}((u\circ w^{-1}-\mathrm{Id})\circ(u\circ w^{-1}-\mathrm{Id})^{p-1})\\
&= \mathrm{Tr}(u\circ \underbrace{(w^{-1}\circ(u\circ w^{-1}-\mathrm{Id})^{p-1})}_{\in G}) - \mathrm{Tr}((u\circ w^{-1}-\mathrm{Id})^{p-1}) \quad \text{or } \mathrm{Tr}(u\circ v)=\mathrm{Tr}(w\circ v),\quad \forall v\in G\\
&= \mathrm{Tr}(w\circ(w^{-1}\circ(u\circ w^{-1}-\mathrm{Id})^{p-1})) - \mathrm{Tr}((u\circ w^{-1}-\mathrm{Id})^{p-1})\\
&= \mathrm{Tr}((u\circ w^{-1}-\mathrm{Id})^{p-1}) - \mathrm{Tr}((u\circ w^{-1}-\mathrm{Id})^{p-1}) = 0
\end{aligned}$$

On a donc $\mathrm{Tr}(n^p)$ pour tout $p\in\mathbb{N}^*$. Par la caractérisation des endormorphismes nilpotents, on a donc que n est nilpotent.
n est diagonalisable et nilpotent, donc $n=0$ (*i.e.*) $u=w$. Donc T est injective.

De plus, comme tous les éléments de G sont annulés par le polynôme X^e-1, ils sont tous diagonalisables et leurs valeurs propres appartiennent à l'ensemble des racines $e^{\text{ièmes}}$ de l'unité. Par conséquent, l'ensemble des traces possibles pour les éléments de G est fini, donc $\mathrm{im}(T)$ est fini. Donc comme T est injectif, et $\mathrm{im}(T)$ est fini, on a donc que G est fini.

Exercice : Soient $G_1,...,G_n$ des groupes cycliques d'ordres respectifs $\alpha_1,...,\alpha_n$. Alors le groupe $G=G_1\times...\times G_n$ est cyclique si et seulement si les α_i sont premiers entre eux deux à deux.

Solution : On aura besoin du petit lemme suivant :

Lemme :
Pour tout $i\in[\![1,n]\!]$, soit $g_i\in G_i$ d'ordre β_i. Alors $g=(g_1,...,g_n)$ est d'ordre $\mathrm{ppcm}(\beta_1,...,\beta_n)$ dans $G_1\times...\times G_n$.

Démonstration :
Pour $1\le i\le n$, notons e_i l'élément neutre de G_i d'ordre β_i. Alors $e(e_1,...,e_n)$ est l'élément neutre de G. On a donc

$$(x^p=e)\quad\Leftrightarrow\quad(\forall i,\ x_i^p=e_i)\quad\Leftrightarrow\quad(\forall i,\ \beta_i\mid p)$$

Le plus petit $p\in\mathbb{N}^*$ tel que $x^p=e$ est le donc le ppcm des β_i.

□

Revenons à notre question.
$\underline{\Rightarrow :}$ Soit $g=(g_1,...,g_n)\in G$ engendrant G. Manifestement, pour tout $1\le i\le n$, g_i engendre G_i, donc d'ordre α_i. D'après le lemme, $\mathrm{ord}g=\mathrm{ppcm}(\alpha_1,...,\alpha_n)$. Mais comme g engendre G, son ordre est aussi $|G|=\alpha_1...\alpha_n$. Donc $\mathrm{ppcm}(\alpha_1,...,\alpha_n)=\alpha_1...\alpha_n$ et par conséquent les α_i sont premiers entre eux deux à deux.

$\underline{\Leftarrow :}$ Pour tout $1\le i\le n$, on considère $g_i\in G_i$ d'ordre α_i (ce g_i existe bien car G_i est supposé cyclique). D'après le lemme, $\mathrm{ord}((g_1,...,g_n))=\mathrm{ppcm}(\alpha_1,...,\alpha_n)$ dans G. Mais $\mathrm{ppcm}(\alpha_1,...,\alpha_n)=\alpha_1...\alpha_n$ puisque les α_i sont premiers entre eux deux à deux et $\alpha_1...\alpha_n=|G|$. Donc $G=\langle g\rangle$ est cyclique.

Exercice :
1) Donner un exemple de groupe abélien fini qui n'est pas cyclique.
2) On rappelle le *théorème de structure des groupes abéliens finis* :
Si G est un groupe abélien fini, montrer qu'il existe un entier $r\in\mathbb{N}$, et des entiers $N_1,...,N_r$, où N_1 est l'exposant de G et $N_{i+1}\mid N_i$ si $i\le r-1$, tels que

$$G\cong\bigoplus_{i=1}^{r}\mathbb{Z}/N_i\mathbb{Z}$$

Application. Trouver l'entier $r \in \mathbb{N}$, et les entiers $N_1, ..., N_r$ du groupe suivant

$$G = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$$

Solution : 1) L'exemple le plus simple est le groupe de Klein $\mathcal{K} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Les éléments $(1,0)$, $(1,1)$ et $(0,1)$ sont d'ordre 2. C'est le groupe non cyclique de cardinal possible le plus petite possible car tout groupe de cardinal premier est cyclique et 2 et 3 sont premiers.

2) Une technique efficace est d'utiliser le théorème chinois et d'ensuite réarranger les termes de façon à avoir $N_{i+1} \mid N_i$. Plus précisement

$$\begin{aligned}&\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}\\ \cong&(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})\end{aligned}$$

Ensuite, on ordonne les puissances des nombres premiers (qui apparaissent dans la décomposition) comme suit :

$$\begin{vmatrix} 2^2 & 2^2 & 2^2 \\ 3 & 3 & 3^2 \\ & 5 & 5 \end{vmatrix}$$

$$\downarrow \quad \downarrow \quad \downarrow$$

$$12 \quad 60 \quad 180$$

On a donc

$$G \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$