Groupes

Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP517, Abymes, cedex 97178, France
dany-jack.mercier@univ-ag.fr

4 octobre 2006

Introduction

Ce cours s'adresse prioritairement aux candidats au CAPES ou à l'agrégation, et devrait constituer une bonne révision des chapitres concernant la structure de groupe. Il pourra néanmoins être utilisé, en complément d'un cours plus détaillé et comportant de nombreux exercices gradués, par des étudiants de première année de faculté.

1 Définitions et premiers résultats

On considère un couple $(G,.)$ formé par un ensemble G et une loi interne

$$\begin{array}{ccc} G\times G & \to & G \\ (x,y) & \mapsto & x.y. \end{array}$$

La loi . est dite **associative** si l'égalité $(x.y).z = x.(y.z)$ est vraie pour tous $x,y,z \in G$. L'élément $e \in G$ est l'**élément neutre** de G s'il vérifie $x.e = e.x = x$ pour tout $x \in G$. S'il existe, un tel élément est unique. En effet, si e et e' sont deux éléments neutres de G, alors $e' = e'.e = e$. Si la loi est associative et si $x \in G$, tout élément x' tel que $x.x' = x'.x = e$ est unique. En effet si x'' vérifie les mêmes égalités,

$$x' = x'.e = x'.x.x'' = e.x'' = x''.$$

[0] [cgpe0001] v1.05 Site web MéhaMaths

L'élément x' s'appelle **le symétrique de** x, et se note x^{-1}, et l'on a $(xy)^{-1} = y^{-1}x^{-1}$ pour tous x, y. Enfin la loi est dite **commutative** si $x.y = y.x$ pour tous $x, y \in G$.

Définition 1 *Un ensemble $(G, .)$ muni d'une loi interne est un* ***groupe*** *si la loi . est associative, s'il existe un élément neutre et si tout élément x de G possède un symétrique. Le groupe est dit* ***commutatif****, ou* ***abélien****, si la loi . est commutative.*

Pour se souvenir des axiomes d'un groupe, on peut retenir les trois lettres ANS (ou CANS si le groupe est commutatif).

Définition 2 *Une partie H d'un groupe G est un* ***sous-groupe*** *de G si elle est elle-même structurée en groupe pour la loi . de G.*

Le lecteur vérifiera les deux caractérisation suivantes d'un sous-groupe de G :

Théorème 1 *Une partie H de G est un sous-groupe de G si et seulement si*
1) $H \neq \emptyset$,
2) $\forall x, y \in H \quad xy \in H$,
3) $\forall x \in H \quad x^{-1} \in H$.

Théorème 2 *Une partie H de G est un sous-groupe de G si et seulement si*
1) $H \neq \emptyset$,
2) $\forall x, y \in H \quad xy^{-1} \in H$.

L'intersection de sous-groupes est encore un sous-groupe, et cela nous permet de définir **le sous-groupe engendré par une partie** A de G comme le plus petit sous-groupe de G contenant A (pour l'inclusion).
Soit G un groupe. Si $x \in G$ et $n \in \mathbb{Z}$, on définit x^n par récurrence de la façon suivante :

$$\begin{cases} x^0 = e, \\ x^n = x^{n-1}.x \quad \text{si } n \in \mathbb{N}^*, \\ x^{-n} = (x^n)^{-1} \quad \text{si } n \in \mathbb{N}^*. \end{cases}$$

On vérifie ensuite les formules usuelles $a^n.a^m = a^{n+m}$ et $(a^n)^m = a^{nm}$ valables pour tous $a \in G$ et $n, m \in \mathbb{Z}$, et la formule $(a.b)^n = a^n.b^n$ lorsque G est commutatif. On a aussi $x^{-n} = (x^n)^{-1} = \left(x^{-1}\right)^n$ pour tout $n \in \mathbb{Z}$.
L'ensemble $\langle x \rangle = \{x^n \,/\, n \in \mathbb{Z}\}$ est un sous-groupe de G et tout sous-groupe H de G contenant x contiendra $\langle x \rangle$. Par conséquent $\langle x \rangle$ est le sous-groupe engendré par x. De façon plus générale, si A est une partie non vide de G, on vérifie que le sous-groupe $\langle A \rangle$ engendré par A est

$$\langle A \rangle = \left\{a_1^{n_1}...a_k^{n_k} \,/\, k \in \mathbb{N},\, a_i \in A,\, n_i \in \mathbb{Z}\right\}.$$

2 Sous-groupes de $(\mathbb{Z},+)$ et de $(\mathbb{R},+)$

Théorème 3 *Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$ où $n\in\mathbb{N}$.*

Preuve : Soit G un sous-groupe de $\mathbb{Z}$. Si $G=\{0\}$, il n'y a rien à démontrer. Si $G\neq\{0\}$, soit n le plus petit entier naturel non nul appartenant à G. Si $m\in G$, on obtient $m=nq+r$ (avec $0\leq r<n$) par division euclidienne, et $r=m-nq\in G$ puisque G est un groupe. Le choix de n montre que $r=0$, d'où $m=nq\in n\mathbb{Z}$. On a prouvé l'inclusion $G\subset n\mathbb{Z}$. La réciproque est triviale. ■

Théorème 4 *Les sous-groupes de $(\mathbb{R},+)$ sont discrets (c'est-à-dire de la forme $a\mathbb{Z}$ avec $a\in\mathbb{R}_+$) ou partout denses.*

Preuve : Soit G un sous-groupe additif de $\mathbb{R}$. Si $G=\{0\}$, $G=a\mathbb{Z}$ avec $a=0$ et c'est fini. Supposons donc $G\neq\{0\}$. Soit $x\in G\setminus\{0\}$. Alors x et $-x$ sont dans G, et il existera au moins un élément strictement positif dans G. Posons $a=\mathrm{Inf}\left(G\cap\mathbb{R}_+^*\right)$.

• Si $a=0$, fixons un réel quelconque x_0. Pour tout $\varepsilon>0$ il existe $x\in G\cap\mathbb{R}_+^*$ tel que $0\leq x<\varepsilon$. Il existe un entier n tel que $nx\leq x_0<nx+x$ (prendre $n=\left[\frac{x_0}{x}\right]$ où $[z]$ désigne la partie entière de z), et l'on peut écrire

$$\forall\varepsilon>0\quad\exists nx\in G\quad |x_0-nx|<x<\varepsilon.$$

Cela montre que x_0 appartient à l'adhérence de G. Comme x_0 est quelconque, on en déduit que l'adhérence de G est $\mathbb{R}$ tout entier, autrement dit que G est dense dans $\mathbb{R}$.

• Si $a>0$, montrons l'égalité $G=a\mathbb{Z}$. Comme $a=\mathrm{Inf}\left(G\cap\mathbb{R}_+^*\right)$, il existe $x\in G$ tel que $a\leq x<2a$. Si l'on avait $a<x$, il existerait $y\in G$ tel que $a\leq y<x<2a$, d'où $0<x-y<a$ en contradiction avec la définition de a. Donc $x=a\in G$ et $a\mathbb{Z}\subset G$.
Réciproquement, si $x\in G$, il existe $n\in\mathbb{Z}$ tel que $na\leq x<na+a$. Les inégalités $0\leq x-na<a$ et la définition de a entraînent $x-na=0$ donc $x\in a\mathbb{Z}$. On obtient bien $G\subset a\mathbb{Z}$. ■

3 Groupe quotient

Soient G un groupe, et $\mathcal{R}$ est une relation d'équivalence sur G. On désire définir une loi sur l'ensemble quotient $G/\mathcal{R}$ de la façon la plus naturelle possible, c'est-à-dire en posant $\overline{x}.\overline{y}=\overline{xy}$. Cette définition a un sens si et seulement si

la classe $\overline{xy}$ ne dépend pas du choix des représentants x et y des classes $\overline{x}$et $\overline{y}$, autrement dit si :

$$(C) \quad x\mathcal{R}x' \text{ et } y\mathcal{R}y' \Rightarrow xy\mathcal{R}x'y'.$$

Définition 3 *La relation d'équivalence $\mathcal{R}$ est* ***compatible avec la loi*** *. si l'affirmation (C) est vérifiée. La relation $\mathcal{R}$ est dite* ***compatible à droite (resp. à gauche) avec la loi .*** *si*

$$\forall x, y, z \in G \quad x\mathcal{R}y \Rightarrow xz\mathcal{R}yz \quad (resp.\ \forall x, y, z \in G \quad x\mathcal{R}y \Rightarrow zx\mathcal{R}zy)\,.$$

Théorème 5 *La relation $\mathcal{R}$ est compatible avec la loi du groupe si et seulement si elle est compatible à droite et à gauche.*

Preuve : Le sens non trivial ($\Leftarrow$) se montre ainsi :

$$x\mathcal{R}x' \text{ et } y\mathcal{R}y' \Rightarrow xy\mathcal{R}x'y \text{ et } x'y\mathcal{R}x'y' \Rightarrow xy\mathcal{R}x'y'. \blacksquare$$

Théorème 6 *Il y a équivalence entre :*
1) La relation d'équivalence $\mathcal{R}$ est compatible à droite,
2) Il existe un sous-groupe H tel que

$$x\mathcal{R}y \Leftrightarrow xy^{-1} \in H \Leftrightarrow x \in Hy.$$

Preuve : Si $\mathcal{R}$ est compatible à droite,

$$x\mathcal{R}y \Leftrightarrow xy^{-1}\mathcal{R}e \Leftrightarrow xy^{-1} \in \overline{e}$$

et l'on vérifie que $H = \overline{e}$ est bien un sous-groupe de G. Réciproquement, si 2) a lieu,

$$xy^{-1} \in H \Leftrightarrow (xz)\,(yz)^{-1} \in H$$

montre que $\mathcal{R}$ est compatible à droite. $\blacksquare$

Définition 4 *Si H est un sous-groupe de G, la relation $\mathcal{R}$ définie par*

$$x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$$

est appelée ***relation d'équivalence à droite suivant le sous-groupe*** *H. Si $x \in G$, la classe de x suivant cette relation est $\overline{x} = Hx$ et s'appelle* ***classe à droite de*** *x* ***suivant*** *H.*

Des deux Théorèmes précédents on déduit :

Théorème 7 *Soit G un groupe et $\mathcal{R}$ une relation d'équivalence dans G. Il y a équivalence entre :*
1) $\overline{x}.\overline{y} = \overline{xy}$ *définit une loi de groupe sur* $G/\mathcal{R}$,
2) La relation$\mathcal{R}$ *est compatible à droite et à gauche avec la loi du groupe,*
3) Il existe un sous groupe H *tel que*
i) $\forall x \in G \quad xH = Hx$,
ii) $x\mathcal{R}y \Leftrightarrow xy^{-1} \in H \Leftrightarrow x^{-1}y \in H$.

Les sous-groupes H vérifiant $xH = Hx$ pour tout $x \in G$ sont très précieux, et justifient la définition :

Définition 5 *Un sous-groupe H est dit* ***distingué*** *(ou* ***normal****) dans G si $xH = Hx$ pour tout $x \in G$. On note alors $H \lhd G$.*

Théorème 8 *Les propriétés suivantes sont équivalentes :*

$$\begin{array}{l}(1)\ \forall x \in G \quad xH = Hx,\\ (2)\ \forall x \in G \quad xH \subset Hx,\\ (3)\ \forall x \in G \quad xHx^{-1} = H,\\ (4)\ \forall x \in G \quad xHx^{-1} \subset H.\end{array}$$

Preuve : (1) est clairement équivalent à (3), et (2) à (4). Montrons que (2) entraîne (1). Pour tout x on a $x^{-1}H \subset Hx^{-1}$ donc $x\left(x^{-1}H\right)x \subset x\left(Hx^{-1}\right)x$, i.e. $Hx \subset xH$. ■

Définition 6 *Soit $H \lhd G$. La relation $\mathcal{R}$ définie par*

$$x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$$

est appelée ***relation d'équivalence suivant le sous-groupe*** *H. L'ensemble quotient $G/\mathcal{R}$ est alors un groupe pour la loi naturelle et se note G/H.*

4 Homorphismes de groupes

Définition 7 *Une application $f : (G, .) \to (G', .)$ entre deux groupes G et G' notés multiplicativement est un* ***homomorphisme*** *(ou simplement un* ***morphisme****) de groupes si*

$$\forall x, y \in G \quad f(x.y) = f(x).f(y).$$

Dans ce cas, les éléments neutres respectifs e et e' des groupes G et G' se correspondent et l'on a $f(e) = e'$, et l'on vérifie que $f\left(x^{-1}\right) = f(x)^{-1}$ pour

tout $x \in G$. Le noyau de f est la partie de G formée des antécédents de e'. On le note $\operatorname{Ker} f$. L'image de f est notée $\operatorname{Im} f$ ou $f(G)$ comme d'habitude. Ainsi :

$$\operatorname{Ker} f = \left\{x \in G \,/\, f(x) = e'\right\} \text{ et } \operatorname{Im} f = \left\{y \in G' \,/\, y = f(x)\right\}.$$

Définition 8 *Un **isomorphisme** (resp. **monomorphisme**, **épimorphisme**) de groupes est, par définition, un homomorphisme bijectif (resp. injectif, surjectif) de groupes.*

Théorème 9 *Un homomorphisme de groupes $f : G \to G'$ est injectif si et seulement si*

$$\operatorname{Ker} f = \{e\}.$$

Preuve : La condition est nécessaire, montrons qu'elle est suffisante. Si $\operatorname{Ker} f = \{e\}$,

$$\begin{aligned} f(x) = f(y) \quad &\Rightarrow f(x) f(y)^{-1} = e' \Rightarrow f\left(xy^{-1}\right) = e' \\ &\Rightarrow xy^{-1} = e \Rightarrow x = y. \blacksquare \end{aligned}$$

Les démonstrations des quatre Théorèmes suivants est laissée en exercice.

Théorème 10 *Soient $f : G \to G'$ un morphisme de groupes, et H (resp. H') un sous-groupe de G (resp. G').*
1) $f(H)$ est un sous-groupe de G',
2) $H \lhd G \Rightarrow f(H) \lhd f(G)$,
3) $f^{-1}(H')$ est un sous-groupe de G,
2) $H' \lhd G' \Rightarrow f^{-1}(H') \lhd G$.

On notera en particulier que $\operatorname{Im} f$ et $\operatorname{Ker} f$ sont des sous-groupes de G et de G', et que le noyau $\operatorname{Ker} f$ de f est toujours distingué dans G. Les trois Théorèmes d'isomorphismes suivants sont dûs à E. Noether.

Théorème 11 ***Premier Théorème d'isomorphisme, ou Théorème de décomposition canonique**. Si $f : G \to G'$ est un homomorphisme de groupes, alors il existe un isomorphisme de groupes g rendant le diagramme suivant commutatif :*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow \pi & & \uparrow i \\ G/\operatorname{Ker} f & \xrightarrow{g} & \operatorname{Im} f \end{array}$$

Ici π désigne la surjection canonique et i l'injection canonique.

Les deux Théorèmes suivant généralisent d'une certaine manière le Théorème 11 :

Théorème 12 *Soient $f : G \to G'$ un morphisme de groupes, et H' un sous-groupe distingué de G'. Alors $H = f^{-1}(H')$ est sous-groupe distingué de G et il existe un unique monomorphisme g rendant le diagramme suivant commutatif :*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow \pi & & \downarrow \pi' \\ G/H & \xrightarrow{g} & G'/H' \end{array}$$

Si f est surjectif, alors g est un isomorphisme.

Théorème 13 *On considère un morphisme de groupes $f : G \to G'$ et des sous-groupes distingués H et H' respectifs de G et G', tels que $f(H) \subset H'$. Il existe un unique homomorphisme g rendant le diagramme suivant commutatif :*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow \pi & & \downarrow \pi' \\ G/H & \xrightarrow{g} & G'/H' \end{array}$$

Si f est surjectif, alors g l'est aussi.

Préparons le second Théorème d'isomorphisme :

Lemme 1 *Si H et K sont deux sous-groupes d'un groupe G,*
1) Si $H \lhd G$, alors $HK = KH$ est un sous-groupe de G.
2) Si $H \lhd G$ et $K \lhd G$, alors $HK \lhd G$.

Preuve : On a posé, par définition, $HK = \{hk \,/\, h \in H \text{ et } k \in K\}$.
1) $H \lhd G$ entraîne

$$\forall h \in H \quad \forall k \in K \quad \exists h' \in H \quad hk = kh' \quad (*)$$

d'où $HK \subset KH$. L'inclusion réciproque se montre de la même façon, donc $HK = KH$. D'autre part HK est un sous-groupe de G : c'est une partie non vide de G (elle contient e), et si $h, h' \in H$ et $k, k' \in K$, $hk(h'k')^{-1} = hkk'^{-1}h'^{-1}$ sera encore dans HK grâce à $(*)$.
2) Pour tout $g \in G$, $gHK = HgK = HKg$. ■

Théorème 14 ***Deuxième Théorème d'isomorphisme.***
Soit H un sous-groupe distingué d'un groupe G, et K un sous-groupe de G. Alors
1) $K \cap H \lhd K$,
2) $H \lhd KH$,
3) $K/K \cap H \simeq KH/H$.

Preuve : L'application

$$\begin{array}{rccc} f: & K & \to & KH/H \\ & k & \mapsto & \dot{k} \end{array}$$

est un morphisme, surjectif car un élément quelconque de $KH = HK$ est de la forme $\overline{\dot{hk}}$, et $\overline{\dot{hk}} = \dot{k}$ (en effet, $(hk)\,k^{-1} \in H$). Comme $\operatorname{Ker} f = K \cap H$, on trouve $K/K \cap H \simeq KH/H$ par décomposition canonique de f. ■

Théorème 15 ***Troisième Théorème d'isomorphisme.***
Soit H un sous-groupe distingué d'un groupe G. On note $\pi : G \to G/H$ la projection canonique.
1) Les sous-groupes distingués de G/H sont de la forme K/H où K est un sous-groupe de G tel que $H \subset K \lhd G$. L'application

$$\begin{array}{rccc} \Psi: & \mathcal{G} & \to & \mathcal{G}' \\ & K & \mapsto & \pi(K) = K/H \end{array}$$

est une bijection décroissante de l'ensemble $\mathcal{G}$ des sous-groupes distingués de G contenant H sur l'ensemble $\mathcal{G}'$ des sous-groupes distingués de G/H.
2) Si $H \subset K \lhd G$, alors $(G/H)/(K/H) \simeq G/K$.

Preuve : 1) Si $H \subset K \lhd G$, alors $\pi(K) = K/H$ est un sous-groupe distingué de $\pi(G) = G/H$ comme l'image d'un sous-groupe distingué par un morphisme de groupes. L'application Ψ est bien définie.
Si T est un sous-groupe distingué de G/H, $\pi^{-1}(T)$ sera un sous-groupe distingué de G comme image réciproque d'un sous-groupe distingué par un morphisme de groupes. Comme π est surjective, on aura $\pi\left(\pi^{-1}(T)\right) = T$, soit $\pi(K) = T$ en posant $K = \pi^{-1}(T)$. On a montré que Ψ est surjective.
L'injectivité de Ψ provient de l'égalité $\pi^{-1}(\pi(K)) = K$ que l'on démontre ici. L'inclusion $\pi^{-1}(\pi(K)) \supset K$ est toujours vraie, et si $x \in \pi^{-1}(\pi(K))$, alors $\pi(x) = \pi(k)$ où $k \in K$, et l'on déduit $xk^{-1} \in \ker \pi = H$, d'où $x \in Hk \subset K$.
On remarquera que l'application réciproque de Ψ est donnée par $T \mapsto \pi^{-1}(T)$ (cela provient directement des deux égalités $\pi\left(\pi^{-1}(T)\right) = T$ et de $\pi^{-1}(\pi(K)) = K$).
2) L'application

$$\begin{array}{rccc} \varphi: & G/H & \to & G/K \\ & \dot{x} & \mapsto & \overline{x} \end{array}$$

est bien définie puisque $H \subset K$ (en effet $\dot{x} = \dot{x}'$ entraîne $xx'^{-1} \in H \subset K$). L'égalité $\overline{x} = \overline{e}$ équivaut à $x \in K$, ou encore à $\dot{x} \in K/H$, et la décomposition canonique de φ donne l'isomorphisme $(G/H)/(K/H) \simeq G/K$ désiré. ■

5 Théorème de Lagrange

Soient G un groupe fini et H un sous-groupe de G. De façon générale, notons $|E|$ le cardinal d'un ensemble E. Les classes à droite Hx et celles à gauche xH ont le même cardinal que H puique l'on dispose des bijections

$$\begin{array}{ccc} H & \to & Hx \\ h & \mapsto & hx \end{array} \quad \text{et} \quad \begin{array}{ccc} H & \to & xH \\ h & \mapsto & xh. \end{array}$$

Soient $\mathcal{R}_d$ et $\mathcal{R}_g$ les relations à droite et à gauche suivant le sous-groupe H. Les classes à droites Hx forment une partition de G et $|Hx| = |H|$ pour tout x, donc $|G| = |G/\mathcal{R}_d| \times |H|$. De la même façon $|G| = |G/\mathcal{R}_g| \times |H|$. Si l'on précise que le cardinal $|G|$ d'un groupe fini G est encore appelé **ordre** de ce groupe, on a montré le Théorème :

Théorème 16 ***Théorème de Lagrange***
L'ordre d'un sous-groupe d'un groupe fini divise l'ordre de ce groupe.

Définition 9 ***L'indice de*** H ***dans*** G *est le nombre de classes à droite (ou à gauche) suivant* H*. On le note* $[G : H]$*, de sorte que*

$$[G : H] = |G/\mathcal{R}_d| = |G/\mathcal{R}_g| = \frac{|G|}{|H|}.$$

6 Groupes cycliques

Définition 10 *Un groupe est dit* ***monogène*** *s'il est engendré par un seul élément. Il est dit* ***cyclique*** *s'il est monogène et fini.*

Notons $\langle x \rangle$ le sous-groupe engendré par x. On a vu que $\langle x \rangle = \{x^n \,/\, n \in \mathbb{Z}\}$. Si G est monogène, il existe x tel que $G = \langle x \rangle$ et

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & x^n \end{array}$$

est un épimorphisme de groupes. Le noyau de φ est un sous-groupe de $\mathbb{Z}$, de sorte que :

- Si $\operatorname{Ker} \varphi = \{0\}$, φ est un isomorphisme et $\mathbb{Z} \simeq G$,
- Sinon, $\operatorname{Ker} \varphi = p\mathbb{Z}$ avec $p \neq 0$, et $G \simeq \mathbb{Z}/p\mathbb{Z}$ par décomposition canonique.

Concluons :

Théorème 17 *Un groupe est monogène (resp. cyclique) si et seulement si il est isomorphe à* $\mathbb{Z}/p\mathbb{Z}$ *(resp. à* $\mathbb{Z}/p\mathbb{Z}$ *avec* $p \neq 0$*).*

7 Ordre d'un élément

Définition 11 *Un élément x d'un groupe G est **d'ordre fini** si le sous-groupe $\langle x\rangle$ qu'il engendre est de cardinal fini. Dans ce cas, l'**ordre** de x est égal au cardinal de $\langle x\rangle$. On le note $\omega(x)$, et l'on peut écrire $\omega(x) = |\langle x\rangle|$.*

Le Théorème de Lagrange montre que si G est un groupe fini, alors l'ordre de tout élément de G divise l'ordre du groupe. Les deux résultats essentiels à connaître concernant l'ordre d'un élément sont :

Théorème 18 *L'élément x est d'ordre fini si et seulement si il existe $p \in \mathbb{N}^*$ tel que $x^p = e$. Dans ce cas*

$$\langle x\rangle = \left\{e, x, x^2, ..., x^{\omega(x)-1}\right\} \text{ et } \omega(x) = \operatorname{Min}\left\{p \in \mathbb{N}^* / x^p = e\right\}.$$

Preuve : ($\Rightarrow$) Si x est d'ordre fini, $\langle x\rangle = \{x^n / n \in \mathbb{Z}\}$ est fini, donc il existe $p > q$ tels que $x^p = x^q$, soit $x^{p-q} = e$. L'ensemble $\{p \in \mathbb{N}^* / x^p = e\}$ inclus dans $\mathbb{N}^*$ n'est pas vide, donc possède un élément minimum $m > 0$. Pout tout $n \in \mathbb{Z}$, la division euclidienne de n par m permet d'écrire

$$n = mq + r \text{ avec } 0 \leq r < m$$

donc $x^n = (x^m)^q . x^r = x^r$ et $\langle x\rangle = \left\{e, x, x^2, ..., x^{m-1}\right\}$. Montrons que les éléments x^r avec $r \in [0, m[\cap\mathbb{N}$ sont distincts deux à deux, ce qui prouvera que $\omega(x) = |\langle x\rangle| = m$ et achèvera la preuve. Si $r, r' \in \mathbb{N} \cap [0, m[$ vérifient $x^r = x^{r'}$, alors $x^{r-r'} = e$ avec $0 \leq |r - r'| < m$, d'où $r = r'$ compte tenu du choix de m. ($\Leftarrow$) Si $x^p = e$, on montre l'inclusion $\langle x\rangle \subset \{x^r / 0 \leq r < p\}$ comme ci-dessus et en utilisant la division euclidienne dans $\mathbb{Z}$. Par conséquent le cardinal de $\langle x\rangle$ est fini et x est d'ordre fini. ■

Remarque : On peut aussi utiliser l'épimorphisme $\varphi : \mathbb{Z} \to \langle x\rangle$ défini par $\varphi(n) = x^n$ pour obtenir :

$$\begin{aligned} x \text{ est d'ordre fini} &\Leftrightarrow \langle x\rangle \simeq \mathbb{Z}/\operatorname{Ker}\varphi \text{ fini} \\ &\Leftrightarrow \operatorname{Ker}\varphi = m\mathbb{Z} \text{ avec } m \neq 0 \Leftrightarrow \exists p \in \mathbb{N}^* \quad x^p = e. \end{aligned}$$

Si x est d'ordre fini, on sait que le sous-groupe $\operatorname{Ker}\varphi$ est de la forme $m\mathbb{Z}$ où m est le plus petit entier strictement positif p tel que $p \in \operatorname{Ker}\varphi$, autrement dit tel que $\varphi(p) = x^p = e$. On déduit

$$\omega(x) = |\langle x\rangle| = |\mathbb{Z}/\operatorname{Ker}\varphi| = m = \operatorname{Min}\left\{p \in \mathbb{N}^* / x^p = e\right\}.$$

Théorème 19 *Si x est d'ordre fini, alors $x^p = e$ si et seulement si $\omega(x)$ divise p.*

Preuve : La condition est suffisante : s'il existe un entier s tel que $p = s \times \omega(x)$, alors $x^p = x^{s\omega(x)} = \left(x^{\omega(x)}\right)^s = e$. Montrons qu'elle est nécessaire. Si p vérifie $x^p = e$, par division euclidienne $p = \omega(x)\, q + r$ avec $0 \leq r < \omega(x)$, donc $x^p = \left(x^{\omega(x)}\right)^q . x^r = x^r = e$. La définition de $\omega(x)$ entraîne alors $r = 0$. ■

Corollaire 1 *Si $|G| = n$, alors $x^n = e$ pour tout $x \in G$.*

Preuve : L'ordre $\omega(x)$ de x divise n par le Théorème de Lagrange, et il suffit d'appliquer le Théorème précédent. ■

8 Exercices

♠ **ugpe0007.** Soit φ une application de $\mathbb{R}^*$ dans $\mathbb{R}$. On définit la loi de composition interne $*$ sur l'ensemble $G = \mathbb{R}^* \times \mathbb{R}$ par :

$$\forall (a,b) \in G \quad \forall (c,d) \in G \quad (a,b) * (c,d) = (ac, bc + \varphi(a)\, d).$$

Quelles conditions doit satisfaire l'application φ pour que G soit structuré en groupe pour la loi $*$? Donner un exemple simple d'application vérifiant ces conditions.

♠ **ugpe0008.** Soient $(G,+)$ et $(G',+)$ deux groupes abéliens d'éléments neutres notés 0. On considère deux homomorphismes de groupes $f : G \to G'$ et $g : G' \to G$ tels que $g \circ f = Id_G$.
1) Montrer que f est injective et que g est surjective.
2) Montrer que $\operatorname{Ker} g = \operatorname{Ker} f \circ g$ et que $\operatorname{Ker} g \cap \operatorname{Im} f = \{0\}$.
3) Démontrer que tout élément de G' s'écrit de façon unique comme la somme d'un élément de $\operatorname{Ker} g$ et d'un élément de $\operatorname{Im} f$.
4) Décrire brièvement la situation lorsque G et G' coïncident avec l'ensemble $C^\infty(\mathbb{R})$ des fonctions numériques indéfiniment dérivables de la variable réelle muni de l'addition, et que

$$f : y(x) \mapsto \int_0^x y(t)\, dt \quad \text{et} \quad g : y(x) \mapsto y'(x).$$

♠ **ugpe0004.** Soient A et B deux sous-groupes d'un groupe G. On note S le sous-groupe de G engendré par $A \cup B$. Montrer que

$$S = \{x \in G \,/\, \exists n \in \mathbb{N}^* \; \forall i \in \mathbb{N}_n \; \exists a_i \in A \; \exists b_i \in B \quad x = a_1 b_1 a_2 b_2 ... a_n b_n\}$$

Démontrer ensuite l'équivalence entre les assertions :
i) AB est un groupe,

ii) $S = AB$,
iii) $AB = BA$.

♠ **ugpe0006. Transport de structure.**
1) On munit l'ensemble des réels $\mathbb{R}$ de la loi $*$ définie par :

$$\forall x, y \in \mathbb{R} \quad x * y = \sqrt[3]{x^3 + y^3}.$$

Montrer directement que $(\mathbb{R}, *)$ est un groupe abélien isomorphe au groupe $(\mathbb{R}, +)$.
2) Soit f une bijection d'un ensemble E vers un groupe $(G, \intercal)$. Montrer qu'il existe une et une seule loi de composition interne $*$ sur E telle que $(E, *)$ soit un groupe et que f soit un isomorphisme de groupes de E sur G.
3) Retrouver le résultat de la première question.

♠ **ugpe0010.** Soient a et b deux éléments d'un groupe G d'ordres respectifs m et p. Si $x \in G$, on note $< x >$ le sous-groupe de G engendré par x.
1) Montrer que $(ab)^k = a^k b^k$ pour tout entier k si, et seulement si, $ab = ba$.
2) On suppose que a et b sont des éléments de G d'ordre fini, que $ab = ba$ et que $< a > \cap < b >= \{e\}$ où e désigne l'élément neutre de G. Montrer que l'ordre de ab est le plus petit commun multiple des ordres de a et b.
3) Dans cette question $G = \mathbb{Z}/12\mathbb{Z}$, $a = \dot{2}$ et $b = \dot{6}$. Vérifier que $< a > \cap < b > \neq \left\{\dot{0}\right\}$ et que l'ordre de $a+b$ n'est pas égal au plus petit commun multiple des ordres de a et b.

♠ **ugpe0005. Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.**

1) Soit n un entier ≥ 2. Si d est un diviseur de n, montrer qu'il il existe un et un seul sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ possédant d éléments, et qu'il s'agit de

$$G_d = \left\{\dot{0}, \frac{\dot{n}}{d}, ..., (d-1)\frac{\dot{n}}{d}\right\}.$$

Ainsi G_d est le sous-groupe engendré par $\frac{\dot{n}}{d}$.

2) Montrer que tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme G_d où d est un diviseur de n.

3) Montrer que tout sous-groupe d'un groupe cyclique est cyclique.

♠ **ugpe0011. Morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z}$.**

1) Soit $f : G \to G'$ un morphisme de groupes. On suppose que a est un élément de G d'ordre fini n. Montrer que $f(a)$ est un élément d'ordre fini, et que cet ordre divise n.

2) Soit d un diviseur de p. Montrer qu'il existe un unique sous-groupe G_d d'ordre d de $\mathbb{Z}/p\mathbb{Z}$, et que $G_d = \left\langle \frac{\dot{n}}{d} \right\rangle = \left\{\dot{0}, \frac{\dot{n}}{d}, ..., (d-1)\frac{\dot{n}}{d}\right\} = \left\{\dot{x} \in \mathbb{Z}/p\mathbb{Z} \,/\, d\dot{x} = \dot{0}\right\}$.

3) Soient n et p deux entiers naturels supérieurs ou égaux à 2.

a) On considère un morphisme de groupes

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & \dot{x} & \mapsto & f\left(\dot{x}\right) \end{array}$$

et l'on pose $\overline{a} = f\left(\dot{1}\right)$.
Montrer que $\overline{a}$ appartient à l'unique sous-groupe G_δ d'ordre $\delta = \text{pgcd}\,(n,p)$ de $\mathbb{Z}/p\mathbb{Z}$.

b) Réciproquement, si $\overline{a} \in G_\delta$, montrer qu'il existe un et un seul homomorphisme de groupes $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ tel que $f\left(\dot{1}\right) = \overline{a}$.

c) En déduire que $\text{Hom}\,(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/\delta\mathbb{Z}$.

4) Application : déterminer explicitement tous les homomorphismes de groupes de $\mathbb{Z}/15\mathbb{Z}$ vers $\mathbb{Z}/23\mathbb{Z}$, puis de $\mathbb{Z}/3\mathbb{Z}$ vers $\mathbb{Z}/12\mathbb{Z}$.

♠ ugpe0009. Sous-groupes de $\mathbb{Z}^2$.

Le produit cartésien $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ muni de la loi "produit"

$$\forall\,(x,y) \in \mathbb{Z}^2 \quad \forall\left(x',y'\right) \in \mathbb{Z}^2 \quad (x,y) + \left(x',y'\right) = \left(x+x', y+y'\right)$$

est un groupe. Notons p_1 (resp. p_2) la projection canonique de $\mathbb{Z}^2$ sur $\mathbb{Z}$ définie par $p_1\,(x,y) = x$ (resp. $p_2\,(x,y) = y$). On considère un sous-groupe G de $\mathbb{Z}^2$.

1) Soit G un sous-groupe de $\mathbb{Z}^2$. Montrer qu'il existe un unique entier b dans $p_2\,(G)$ tel que tout élément de $p_2\,(G)$ soit un multiple de b.

2) Soit (a,b) un élément de G dont la seconde projection est b.

a) Montrer que tout élément (x,y) de G s'écrit de façon unique $(x,y) = q\,(a,b) + (r,0)$ où $q \in \mathbb{Z}$ et $r \in \mathbb{Z}$. Vérifier que l'application

$$\begin{array}{rccc} f: & G & \to & \mathbb{Z} \\ & (x,y) & \mapsto & r \end{array}$$

est un homomorphisme de groupes. Quel est son noyau ?

b) En déduire l'existence de deux éléments g_1 et g_2 de G tels que $G = \mathbb{Z}g_1 + \mathbb{Z}g_2$.

4) Quelle est la forme générale des sous-groupes de $\mathbb{Z}^2$?

5) Peut-on généraliser cette méthode dans le cas des sous-groupes de $\mathbb{Z}^n$, où $n \in \mathbb{N}^*$?

♠ ugpe0001. Ordre d'un élément dans un groupe.

$(G,.)$ désigne un groupe multiplicatif d'élément neutre e. Un élément x de G est dit d'ordre fini si le sous-groupe $\langle x \rangle$ qu'il engendre est de cardinal fini. Dans ce cas l'ordre $\omega\,(x)$ de x est égal au cardinal du sous-groupe $\langle x \rangle$.

1) Montrer que x est d'ordre fini si, et seulement si, il existe $p \in \mathbb{N}^*$ tel que $x^p = e$, et que dans ce cas $\langle x \rangle = \left\{e, x, x^2, ..., x^{\omega(x)-1}\right\}$ et $\omega(x) = \text{Min}\left\{p \in \mathbb{N}^* / x^p = e\right\}$.

2) Si x est d'ordre fini, vérifier que $x^p = e$ si et seulement si $\omega(x) | p$. En déduire que, si G est fini d'ordre n, alors $x^n = e$ pour tout $x \in G$.

3) Montrer que si x est d'ordre fini et si $t \in \mathbb{Z}$, alors

$$\omega\left(x^t\right) = \frac{\omega(x)}{\text{pgcd}\left(t, \omega(x)\right)}.$$

4) On suppose dans cette question que G est commutatif. Montrer l'équivalence

$$\text{pgcd}\left(\omega(x), \omega(y)\right) = 1 \Leftrightarrow \omega(xy) = \omega(x)\,\omega(y).$$

♠ ugpe0002. Sous-groupes d'un groupe cyclique et morphisme $x \mapsto x^m$.

On considère un groupe cyclique multiplicatif $(G, .)$ d'ordre n, et l'on note e son élément neutre. Soit g un générateur de G. Si $m \in \mathbb{Z}$, on note G^m l'ensemble de tous les éléments x^m où x décrit G. On pose aussi $G_m = \{x \in G / x^m = e\}$. En d'autres termes, les ensembles G^m et G_m sont respectivement l'image et le noyau de l'homomorphisme de groupes

$$\begin{array}{rccc} \varphi : & G & \to & G \\ & x & \mapsto & x^m. \end{array}$$

1) Soit d un diviseur positif de n. Montrer qu'il existe un et un seul sous-groupe H d'ordre d dans G, que $H = G_d = G^{\frac{n}{d}}$ et que H est cyclique et engendré par $g^{\frac{n}{d}}$.

2) Soit m un entier relatif et $\delta = \text{pgcd}(m, n)$.

a) Montrer que $G_m = G_\delta$. En déduire que φ est un isomorphisme si, et seulement si, $\delta = 1$.

b) Montrer l'égalité $G^m = G^\delta$.

3) Si d_1 et d_2 désignent deux diviseurs de n, démontrer les égalités suivantes

$$\text{a)} \quad G_{d_1} \cap G_{d_2} = G_{\text{pgcd}(d_1, d_2)} \qquad \text{b)} \quad G_{d_1} G_{d_2} = G_{\text{ppcm}(d_1, d_2)}.$$

4) Si m et s désignent deux entiers relatifs quelconques, exprimer les ensembles $G_m \cap G_s$ et $G_m G_s$ sous la forme d'un ensemble G_p où l'entier p est à déterminer.

5) Si d_1 et d_2 désignent deux diviseurs de n, montrer l'égalité

$$\text{pgcd}\left(\frac{n}{d_1}, \frac{n}{d_2}\right) \times \text{ppcm}(d_1, d_2) = n$$

puis en déduire l'égalité $G^{d_1} \cap G^{d_2} = G^{\mathrm{ppcm}(d_1,d_2)}$.

6) Application : On rappelle que le groupe multiplicatif $\mathbb{F}_q^*$ de n'importe quel corps fini $\mathbb{F}_q$ à q éléments est cyclique. Soit m un entier naturel. Combien y-a-t'il de racines m-ième de l'unité dans $\mathbb{F}_q$? Et dans $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier ? Rechercher toutes les racines 22-ièmes de l'unité dans $\mathbb{Z}/79\mathbb{Z}$.