ISM MP, Mathématiques
Année 2024/2025

Feuille d'exercices n°80

Exercice 1 (***)

Soit $(\mathrm{G}, \times)$ un groupe et $\mathrm{A} \subset \mathrm{G}$. On définit le *centralisateur* de A noté C(A) par

$$\mathrm{C}(\mathrm{A}) = \{x \in \mathrm{G} \mid \forall a \in \mathrm{A} \quad ax = xa\}$$

1. Montrer que C(A) est sous-groupe de G et $\mathrm{C}(\mathrm{G}) \subset \mathrm{C}(\mathrm{A})$.
2. Montrer que $\mathrm{C}(\mathrm{A}) = \mathrm{C}(\langle \mathrm{A} \rangle)$.
3. Déterminer $\mathrm{C}(\mathrm{S}_n)$ pour $n \geqslant 3$.

Corrigé : 1. On a clairement $e \in \mathrm{C}(\mathrm{A})$ puis soit $x \in \mathrm{C}(\mathrm{A})$. On a

$$\forall a \in \mathrm{A} \qquad ax = xa \quad \Longrightarrow \quad \forall a \in \mathrm{A} \qquad x^{-1}a = ax^{-1}$$

c'est-à-dire $x^{-1} \in \mathrm{A}$. Enfin, pour $(x, y) \in \mathrm{C}(\mathrm{A})$, on a

$$\forall a \in \mathrm{A} \qquad axy = xay = xya$$

L'inclusion $\mathrm{C}(\mathrm{G}) \subset \mathrm{C}(\mathrm{A})$ est immédiate et on conclut

$$\boxed{\text{Le } \textit{centralisateur} \text{ de A noté C(A) est un sous-groupe de } (\mathrm{G}, \times) \text{ contenant C(G).}}$$

Vocabulaire : Le centralisateur C(G) du groupe tout entier est aussi appelé *centre* du groupe et noté Z(G) (Z pour *zentrum*, centre en allemand).

2. Soient X, Y des parties de G. On a sans difficulté

$$\mathrm{X} \subset \mathrm{Y} \quad \Longrightarrow \quad \mathrm{C}(\mathrm{Y}) \subset \mathrm{C}(\mathrm{X})$$

Avec $\mathrm{A} \subset \langle \mathrm{A} \rangle$, il s'ensuit $\mathrm{C}(\langle \mathrm{A} \rangle) \subset \mathrm{C}(\mathrm{A})$. Montrons l'inclusion réciproque $\mathrm{C}(\mathrm{A}) \subset \mathrm{C}(\langle \mathrm{A} \rangle)$. On a la propriété

$$\mathrm{X} \subset \mathrm{C}(\mathrm{Y}) \iff \mathrm{Y} \subset \mathrm{C}(\mathrm{X})$$

puisque $\quad \forall x \in \mathrm{X} \quad \forall y \in \mathrm{Y} \quad xy = yx \iff \forall y \in \mathrm{Y} \quad \forall x \in \mathrm{X} \quad xy = yx$

On en déduit $\mathrm{A} \subset \mathrm{C}(\mathrm{C}(\mathrm{A}))$ puisqu'on a $\mathrm{C}(\mathrm{A}) \subset \mathrm{C}(\mathrm{A})$ et comme $\mathrm{C}(\mathrm{C}(\mathrm{A}))$ est un sous groupe de $(\mathrm{G}, \times)$, il s'ensuit $\langle \mathrm{A} \rangle \subset \mathrm{C}(\mathrm{C}(\mathrm{A}))$. D'après la propriété précédente, il s'ensuit $\mathrm{C}(\mathrm{A}) \subset \mathrm{C}(\langle \mathrm{A} \rangle)$. Ainsi

$$\boxed{\mathrm{C}(\mathrm{A}) = \mathrm{C}(\langle \mathrm{A} \rangle)}$$

Variante : On peut aussi faire sans la propriété qui échange les rôles. Notons $\mathrm{B} = \mathrm{C}(\mathrm{A})$. On a $\mathrm{A} \subset \mathrm{C}(\mathrm{B})$ et C(B) est un sous-groupe de $(\mathrm{G}, \times)$ contenant A d'où $\langle \mathrm{A} \rangle \subset \mathrm{C}(\mathrm{B})$ et par suite $\mathrm{C}(\mathrm{C}(\mathrm{B})) \subset \mathrm{C}(\langle \mathrm{A} \rangle)$ et on conclut en observant $\mathrm{B} \subset \mathrm{C}(\mathrm{C}(\mathrm{B}))$.

3. Soit $\sigma \in \mathrm{C}(\mathrm{S}_n)$ avec $\sigma \neq \mathrm{id}$. Ainsi, il existe $(i, j) \in [\![1 ; n]\!]^2$ avec $i \neq j$ tel que $\sigma(i) = j$. On choisit $k \in [\![1 ; n]\!] \setminus \{i, j\}$ (possible car $n \geqslant 3$) et $\tau = \begin{pmatrix} j & k \end{pmatrix}$. On a

$$\sigma \circ \tau(i) = \sigma(i) = j \quad \text{et} \quad \tau \circ \sigma(i) = \tau(j) = k \neq j$$

d'où la contradiction. On conclut

$$\boxed{\forall n \geqslant 3 \qquad \mathrm{C}(\mathrm{S}_n) = \{\mathrm{id}\}}$$

Exercice 2 (***)

Soit G un groupe fini vérifiant $\forall x \in \mathrm{G} \quad x^2 = e$

1. Montrer que G est un groupe abélien.
2. On suppose que G est fini non réduit à $\{e\}$.
   (a) Justifier l'existence de $n = \min\{\text{Card P, P} \subset \mathrm{G} \text{ tel que } \langle \mathrm{P}\rangle = \mathrm{G}\}$ entier non nul.
   (b) Soit $(x_1, \dots, x_n) \in \mathrm{G}^n$ tel que $\mathrm{G} = \langle x_1, \dots, x_n\rangle$. On pose
   $$\varphi : (\mathbb{Z}/2\mathbb{Z})^n \to \mathrm{G},\ (\overline{\alpha_1}, \dots, \overline{\alpha_n}) \mapsto x_1^{\alpha_1} \dots x_n^{\alpha_n} \quad \text{avec} \quad \alpha_i \in \{0, 1\}$$
   Justifier que φ est bien définie et vérifier que φ est un morphisme de de groupes.
   (c) Conclure que $\mathrm{G} \simeq (\mathbb{Z}/2\mathbb{Z})^n$

Corrigé : 1. Soit $(x, y) \in \mathrm{G}^2$. On a
$$(xy)^2 = e \iff xyxy = e \iff yxy = x \iff xy = yx$$
Ainsi $\boxed{\text{Le groupe G est abélien.}}$

2.(a) L'ensemble $\{\text{Card P, P} \subset \mathrm{G} \text{ tel que } \langle \mathrm{P}\rangle = \mathrm{G}\}$ est non vide puisque $\langle \mathrm{G}\rangle = \mathrm{G}$ et il s'agit d'une partie non vide de $\mathbb{N}$ qui admet donc un plus petit élément n. Enfin, comme $\langle \varnothing\rangle = \{e\} \neq \mathrm{G}$ et que l'ensemble vide est l'unique partie de cardinal nul, on conclut
$$\boxed{\text{Il existe } n = \min\{\text{Card P, P} \subset \mathrm{G} \text{ tel que } \langle \mathrm{P}\rangle = \mathrm{G}\} \text{ entier non nul.}}$$

2.(b) Soit $(\alpha_i)_{i\in[\![1\,;n]\!]}$ et $(\beta_i)_{i\in[\![1\,;n]\!]}$ dans $\mathbb{Z}^n$ tel que $\overline{\alpha_i} = \overline{\beta_i}$ pour tout $i \in [\![1\,;\,n]\!]$. Il s'ensuit
$$x_1^{\alpha_1} \dots x_n^{\alpha_n} = x_1^{\beta_1} \dots x_n^{\beta_n}$$
ce qui prouve que l'application φ est bien définie et ne dépend pas du choix des représentants des classes $\overline{\alpha_i}$. Puis, par commutativité, on a
$$\begin{aligned}\varphi\left((\overline{\alpha_1}, \dots, \overline{\alpha_n}) + (\overline{\beta_1}, \dots, \overline{\beta_n})\right) &= \varphi\left(\overline{\alpha_1 + \beta_1}, \dots, \overline{\alpha_n + \beta_n}\right)\\ &= x_1^{\alpha_1+\beta_1} \dots x_n^{\alpha_n+\beta_n} = x_1^{\alpha_1} \dots x_n^{\alpha_n} x_1^{\beta_1} \dots x_n^{\beta_n}\\ &= \varphi(\overline{\alpha_1}, \dots, \overline{\alpha_n})\varphi(\overline{\beta_1}, \dots, \overline{\beta_n})\end{aligned}$$
Ainsi $\boxed{\text{L'application } \varphi \text{ est un morphisme de groupes.}}$

2.(c) On note $\mathrm{H} = \left\{x_1^{\alpha_1} \dots x_n^{\alpha_n}, (\alpha_i)_{i\in[\![1\,;n]\!]} \in \mathbb{Z}^n\right\}$. L'ensemble H est clairement un sous-groupe de G contenant $\{x_1, \dots, x_n\}$ d'où $\mathrm{G} \subset \mathrm{H}$ et on a clairement $\mathrm{H} \subset \mathrm{G}$ d'où l'égalité $\mathrm{G} = \mathrm{H}$. Par définition, on a $\mathrm{Im}\,\varphi = \mathrm{H}$ d'où la surjectivité de φ. Enfin, soit $(\alpha_i)_{i\in[\![1\,;n]\!]} \in \mathbb{Z}^n$ tel que $(\overline{\alpha_i})_{i\in[\![1\,;n]\!]} \in \mathrm{Ker}\,\varphi$. Supposons α_{i_0} impair avec $i_0 \in [\![1\,;\,n]\!]$. Il vient par commutativité
$$x_{i_0} = \prod_{i\in[\![1\,;n]\!]\setminus\{i_0\}} x_i^{\alpha_i}$$
Ceci contredirait la minimalité de n, cardinal d'une famille génératrice minimale. On en déduit que tous les α_i sont pairs d'où
$$\mathrm{Ker}\,\varphi = \{(\bar{0}, \dots, \bar{0})\}$$
Le morphisme de groupes φ est donc un isomorphisme et on conclut
$$\boxed{\mathrm{G} \simeq (\mathbb{Z}/2\mathbb{Z})^n}$$

Remarque : On peut observer que le cardinal d'une famille génératrice minimale vérifie $n = \log_2 \mathrm{Card\ G}$.

Exercice 3 (***)

Soient p et q des entiers non nuls premiers entre eux. Montrer que l'application $\varphi : \mathbb{U}_p \times \mathbb{U}_q \to \mathbb{U}_{pq}, (x,y) \mapsto xy$ est un isomorphisme de groupes.

Corrigé : L'application est bien définie puisque pour $(x,y) \in \mathbb{U}_p \times \mathbb{U}_q$, on a $(xy)^{pq} = (x^p)^q (y^q)^p = 1$ et est clairement un morphisme puisque

$$\forall (x,x') \in \mathbb{U}_p^2 \qquad \forall (y,y') \in \mathbb{U}_q^2 \qquad \varphi(xx', yy') = xx'yy' = xyx'y' = \varphi(x,y)\varphi(x',y')$$

On pose $\alpha = \mathrm{e}^{\frac{2\mathrm{i}\pi}{p}} \qquad \beta = \mathrm{e}^{\frac{2\mathrm{i}\pi}{q}} \qquad \gamma = \mathrm{e}^{\frac{2\mathrm{i}\pi}{pq}}$

L'application φ réalise la transformation suivante :

$$\forall (k,\ell) \in \mathbb{Z}^2 \qquad \varphi(\alpha^k, \beta^\ell) = \gamma^{qk+\ell p}$$

Posons $\psi : \begin{cases} \mathbb{Z}^2 & \longrightarrow \mathbb{Z} \\ (k,\ell) & \longmapsto qk + p\ell \end{cases}$

L'application ψ est clairement un morphisme de groupes donc Im ψ est un sous-groupe de $\mathbb{Z}$. Or, d'après le théorème de Bézout, comme $p \wedge q = 1$, il s'ensuit que $1 \in \text{Im } \psi$ d'où Im $\psi = \mathbb{Z}$ et la surjectivité de φ s'ensuit. On a donc une surjection entre deux ensembles de même cardinaux d'où la bijectivité de φ et on conclut

$$\boxed{\text{L'application } \varphi \text{ est un morphisme de groupes.}}$$

Variante : Déterminons Ker φ, ou de manière équivalente les couples $(k,\ell) \in \mathbb{Z}^2$ tels que $qk + p\ell \equiv 0\ [qp]$, c'est-à-dire $qk + p\ell = rpq$ avec $r \in \mathbb{Z}$. En isolant les facteurs en q puis les facteurs en p, on en déduit à l'aide du théorème de Gauss que $p|qk$ donc $p|k$ puis $q|p\ell$ donc $q|\ell$ et par conséquent $\alpha^k = 1$ et $\beta^\ell = 1$, autrement dit

$$\text{Ker } \varphi = \{(1,1)\}$$

d'où l'injectivité de φ entre deux ensembles de même cardinal et on conclut comme précédemment. On peut aussi utiliser la relation de Bézout pour établir la surjectivité plutôt que passer par l'argument sur les cardinaux. Enfin, cet exercice est un jumeau du théorème chinois qui fournit directement

$$qk + p\ell \equiv 0\ [pq] \iff \begin{cases} qk + p\ell \equiv 0\ [p] \\ qk + p\ell \equiv 0\ [q] \end{cases}$$

avec l'isomorphisme d'anneaux $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Exercice 4 (***)

Soit $n \geqslant 2$. On note D_n les *dérangements* de S_n, c'est-à-dire les permutations de S_n sans point fixe. Calculer $\displaystyle\sum_{\sigma \in \mathrm{D}_n} \varepsilon(\sigma)$.

Corrigé : On peut interpréter $\displaystyle\sum_{\sigma \in \mathrm{D}_n} \varepsilon(\sigma)$ comme un déterminant. On a pour $\mathrm{M} \in \mathscr{M}_n(\mathbb{R})$

$$\det(\mathrm{M}) = \sum_{\sigma \in \mathrm{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{i,\sigma(i)}$$

Ainsi, on cherche une matrice M telle que, pour $\sigma \in \mathrm{D}_n$, on ait $\displaystyle\prod_{i=1}^{n} m_{i,\sigma(i)} = 1$ et si $\sigma \notin \mathrm{D}_n$ ce qui signifie qu'il existe un $k \in [\![1\,;\, n]\!]$ tel que $\sigma(k) = k$ autrement dit un terme diagonal apparaît

dans le produit $\prod_{i=1}^{n} a_{i,\sigma(i)}$, on veut que celui-ci soit nul. Il suffit donc de considérer la matrice constituée de 1 sauf pour les termes diagonaux qui sont tous nuls. Notant J la matrice de $\mathscr{M}_n(\mathbb{R})$ constituée de 1. On a

$$\sum_{\sigma\in \mathrm{D}_n} \varepsilon(\sigma) = \det(\mathrm{J}-\mathrm{I}_n)$$

Par des arguments classiques de réduction, on a l'existence de $\mathrm{P}\in \mathrm{GL}_n(\mathbb{R})$ telle que $\mathrm{P}^{-1}\mathrm{JP} = \mathrm{diag}(n,0,\dots,0)$ puis $\mathrm{P}^{-1}(\mathrm{J}-\mathrm{I}_n)\mathrm{P} = \mathrm{diag}(n-1,-1,\dots,-1)$ et on conclut

$$\boxed{\sum_{\sigma\in \mathrm{D}_n} \varepsilon(\sigma) = (n-1)(-1)^{n-1}}$$

Exercice 5 (***)

Soit $(\mathrm{G},\star)$ un groupe cyclique et H un sous-groupe de G. Démontrer que H est cyclique.

Corrigé : Soit $a\in \mathrm{G}$ tel que $\langle a\rangle = \mathrm{G}$. L'ensemble $\left\{k\in\mathbb{N}^* \mid a^k\in \mathrm{H}\right\}$ est une partie de $\mathbb{N}^*$ non vide puisque $a^{\mathrm{Card\ G}} = e\in \mathrm{H}$. Notons n son minimum. On a clairement $\langle a^n\rangle \subset \mathrm{H}$. Soit $x\in \mathrm{H}$. En particulier, on a $x\in \mathrm{G}$ d'où l'existence de $\ell\in\mathbb{Z}$ tel que $x = a^\ell$. D'après le théorème de la division euclidienne, il existe un unique couple $(q,r)\in\mathbb{Z}\times[\![\,0\,;\,n-1\,]\!]$ tel que $\ell = nq+r$. Puis

$$x\star a^{-nq} = x^{nq+r-nq} = x^r \quad \text{et} \quad x\star a^{-nq} = x\star (a^n)^{-q}\in \mathrm{H}$$

Par minimalité de n, on en déduit $r=0$ d'où $x = (a^n)^q\in\langle a^n\rangle$ ce qui prouve $\mathrm{H} = \langle a^n\rangle$. On conclut

$$\boxed{\text{Tout sous-groupe d'un groupe cyclique est cyclique.}}$$

Exercice 6 (***)

Soit $(\mathrm{G},\times)$ une groupe fini d'ordre n et $x\in\mathrm{G}$ avec $o(x) = d$. Montrer

$$\forall k\in\mathbb{Z} \qquad o(x^k) = \frac{d}{d\wedge k}$$

Corrigé : Soit $k\in\mathbb{Z}$, $\delta = d\wedge k$ et on note $d = \delta d'$ et $k = \delta k'$ avec d', k' entiers relatifs premiers entre eux. On a

$$(x^k)^{d'} = x^{\delta k' d'} = (x^d)^{k'} = e \quad\Longrightarrow\quad o(x^k)|d'$$

Par ailleurs, pour ℓ entier tel que $x^{k\ell} = (x^k)^\ell = e$, il vient $d|k\ell$ autrement dit $\delta d'|\delta k'\ell$ d'où $d'|k'\ell$. D'après le théorème de Gauss, comme $d'\wedge k' = 1$, on obtient $d'|\ell$ donc en particulier $d'|o(x^k)$. Les entiers d' et $o(x^k)$ sont associés donc égaux et on conclut

$$\boxed{\forall k\in\mathbb{Z} \qquad o(x^k) = \frac{d}{d\wedge k}}$$

Exercice 7 (***)

Quel est l'ordre maximal d'un élément de S_8 ?

Corrigé : Soit $\sigma\in\mathrm{S}_8$. La permutation σ se décompose en $\sigma = \prod_{i=1}^{r} c_i$, produit de cycles à supports disjoints. Par commutativité, on a pour k entier $\sigma^k = \prod_{i=1}^{r} c_i^k$ et comme les supports des c_i^k sont disjoints, on a l'équivalence

$$\sigma^k = \mathrm{id} \iff \forall i \in [\![1\,;\, r]\!] \qquad c_i^k = \mathrm{id}$$

Ainsi, l'ordre $o(\sigma)$ divise l'ordre de tous les cycles et par définition et par minimalité, on en déduit

$$o(\sigma) = o(c_1) \vee \ldots \vee o(c_r)$$

Les décompositions possibles pour les longueurs de cycle sont les suivantes :

$$\begin{aligned} 8 &= 7+1 \\ &= 6+2 = 6+1+1 \\ &= 5+3 = 5+2+1 \\ &= 4+4 = 4+3+1 = 4+2+2 = 4+2+1+1 \\ 8 &= 3+3+2 = 3+3+1+1 = 3+2+2+1 = \ldots \\ &= \ldots \end{aligned}$$

On constate que le ppcm maximal est obtenu avec la configuration $5 \vee 3$ et on conclut

$$\boxed{\text{L'ordre maximal d'un élément de } \mathrm{S}_8 \text{ est } 15.}$$

Exercice 8 (***)

Soit φ un morphisme d'un groupe fini $(\mathrm{G}, \times)$ vers un autre groupe. Établir

$$\mathrm{Card\ G} = \mathrm{Card\ Ker}\ \varphi \times \mathrm{Card\ Im}\ \varphi$$

Corrigé : On définit la relation binaire $\mathcal{R}$ par

$$\forall (x,y) \in \mathrm{G}^2 \qquad x \mathcal{R} y \iff \varphi(x) = \varphi(y)$$

On vérifie sans difficulté que $\mathcal{R}$ est une relation d'équivalence. L'ensemble des classes d'équivalence est exactement le cardinal de Im φ. Pour $(x,y) \in \mathrm{G}^2$, par propriété de morphisme de groupes, on a

$$\begin{aligned} x \mathcal{R} y &\iff \varphi(x) = \varphi(y) \iff \varphi(y)^{-1}\varphi(x) = 1 \\ &\iff \varphi(y^{-1}x) = 1 \iff x^{-1}y \in \mathrm{Ker}\ \varphi \iff y \in x\,\mathrm{Ker}\ \varphi \end{aligned}$$

Ainsi, une classe d'équivalence pour $\mathcal{R}$ est de la forme $x\,\mathrm{Ker}\ \varphi$. Or, l'application $\mathrm{G} \to \mathrm{G}, u \mapsto xu$ est une permutation de G ce qui prouve que les classes d'équivalence sont toutes en bijection avec Ker φ. Notant $x_1, \ldots, x_p$ des représentants des classes d'équivalence, la famille $\overline{x_1}, \ldots, \overline{x_p}$ est une partition de G d'où

$$\mathrm{Card\ G} = \mathrm{Card} \bigsqcup_{i=1}^{p} \overline{x_i} = \sum_{i=1}^{p} \mathrm{Card}\ \overline{x_i} = p\,\mathrm{Card\ Ker}\ \varphi$$

On conclut $\boxed{\mathrm{Card\ G} = \mathrm{Card\ Ker}\ \varphi \times \mathrm{Card\ Im}\ \varphi}$

Remarque : C'est exactement la démonstration du théorème de Lagrange.

Exercice 9 (****)

Décrire les sous-groupes de $(\mathbb{R}, +)$.

Corrigé : On rappelle que le corps $\mathbb{R}$ vérifie la propriété de la borne supérieure et inférieure.

Théorème 1. *Soit* A *partie non vide de* $\mathbb{R}$. *Si* A *est majorée, elle possède une borne supérieure* M *caractérisée par*

$$\forall \varepsilon > 0 \qquad \exists a \in \mathrm{A} \quad | \quad \mathrm{M} - \varepsilon < a \leqslant \mathrm{M}$$

Si A *est minorée, elle possède une borne inférieure* m *caractérisée par*

$$\forall \varepsilon > 0 \qquad \exists a \in \mathrm{A} \quad | \quad m \leqslant a < m + \varepsilon$$

Soit G un sous-groupe de $\mathbb{R}$. On suppose $\mathrm{G} \neq \{0\}$ sinon il n'y a rien à faire. On dispose de $x \in \mathrm{G} \setminus \{0\}$ et quitte à considérer $-x$ qui est toujours dans G (son symétrique pour la loi $+$), on dispose de $x \in \mathrm{G} \cap]\,0\,;+\infty\,[$. On note

$$a = \inf \mathrm{G} \cap]\,0\,;+\infty\,[$$

L'ensemble $\mathrm{G} \cap]\,0\,;+\infty\,[$ est une partie non vide minorée de $\mathbb{R}$ et admet donc une borne inférieure finie.

• Supposons $a = 0$. Soit $x \in \mathbb{R}$ et $\varepsilon > 0$. Il existe $b \in \mathrm{G} \cap]\,0\,;+\infty\,[$ tel que $0 < b < \varepsilon$ par définition de la borne inférieure (on est assuré d'avoir $b > 0$ puisque $b \in \mathrm{G} \cap]\,0\,;+\infty\,[$). On a

$$0 \leqslant x - bn < b < \varepsilon \quad \text{avec} \quad n = \left\lfloor \frac{x}{b} \right\rfloor \in \mathbb{Z}$$

FIGURE 1 – Sous-groupe dense dans $\mathbb{R}$

Ainsi $$-\varepsilon < x - bn < \varepsilon$$

Comme $nb \in \mathrm{G}$, ceci prouve la densité de G dans $\mathbb{R}$ puisque $nb \in]\,x - \varepsilon\,;x + \varepsilon\,[\cap \mathrm{G}$ autrement dit toute boule ouverte centrée en x rencontre G.

• Supposons $a > 0$. Montrons que $a \in \mathrm{G}$. Si $a \notin \mathrm{G}$, d'après la propriété de la borne inférieure, il existe $b \in \mathrm{G}$ tel que $a < b < 2a$, la première inégalité étant stricte du fait que $a \notin \mathrm{G}$. Puis, comme $b - a > 0$, il existe $c \in \mathrm{G}$ tel que $a < c < a + (b - a) = b$.

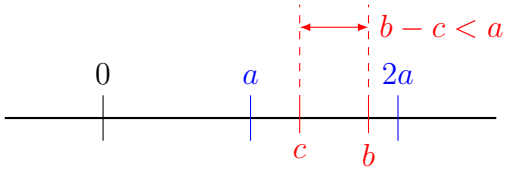

FIGURE 2 – Sous-groupe discret de $\mathbb{R}$

On aurait alors $0 < b - c < 2a - a = a$ et $b - c \in \mathrm{G}$. Ceci contredit la définition de a donc on obtient que $a \in \mathrm{G}$. Puis, pour $x \in \mathrm{G}$, il vient

$$0 \leqslant x - na < a \quad \text{avec} \quad n = \left\lfloor \frac{x}{a} \right\rfloor \in \mathbb{Z}$$

Or, on a $x - na \in \mathrm{G}$ donc, par définition de a, il vient $x - na = 0$ d'où $x \in a\mathbb{Z}$. On a donc prouvé $\mathrm{G} \subset a\mathbb{Z}$ et l'inclusion réciproque est immédiate.

Les sous-groupes de $(\mathbb{R}, +)$ sont soit denses dans $\mathbb{R}$, soit discrets de la forme $a\mathbb{Z}$ avec a réel.