ISM MP, Mathématiques
Année 2025/2026

Feuille d'exercices n°80

Exercice 1 (**)

Soit $(\mathrm{G}, \star)$ un groupe.

1. Montrer qu'une union de deux sous-groupes de $(\mathrm{G}, \star)$ est un sous-groupe si et seulement si l'un contient l'autre.
2. Le résultat se généralise-t-il à plus de deux sous-groupes ?

Corrigé : 1. Soit G un groupe et H_1, H_2 deux sous-groupes. Supposons qu'il existe $a \in \mathrm{H}_1 \setminus \mathrm{H}_2$. Soit $b \in \mathrm{H}_2$. On a $a \star b \in \mathrm{H}_1 \cup \mathrm{H}_2$, autrement dit $a \star b \in \mathrm{H}_1$ ou $a \star b \in \mathrm{H}_2$. Si $a \star b \in \mathrm{H}_2$, alors $(a \star b) \star b^{-1} = a \in \mathrm{H}_2$ ce qui est exclu. Il s'ensuit que $a \star b \in \mathrm{H}_1$ et par suite $a^{-1} \star (a \star b) = b \in \mathrm{H}_1$ ce qui prouve $\mathrm{H}_2 \subset \mathrm{H}_1$. Si un tel a n'existe pas, alors $\mathrm{H}_1 \subset \mathrm{H}_2$. On conclut

Une union de deux sous-groupes est un sous-groupe si et seulement si l'un contient l'autre.

2. En fait, non ! On a pour la loi multiplicative

$$(\pm 1, \pm 1) = (\pm 1, 1) \cup (1, \pm 1) \cup \pm(1, 1)$$

et aucun des sous-groupes exhibés ne contient les autres. Ainsi

Le résultat ne se généralise pas à plus de deux sous-groupes.

Remarques : (a) Si on connaît les groupes quotients, on peut considérer :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle (1,0) \rangle \cup \langle (0,1) \rangle \cup \langle (1,1) \rangle$$

(b) Il faut chercher un contre-exemple de groupe qui ne soit pas cyclique car un sous-groupe contenant un générateur serait le groupe lui-même.

Exercice 2 (***)

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 $x^{-1} \in \mathrm{C}(\mathrm{A})$. Enfin, pour $(x, y) \in \mathrm{C}(\mathrm{A})^2$, 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

Le *centralisateur* de A noté C(A) est un sous-groupe de $(\mathrm{G}, \times)$ 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

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

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

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

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

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

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

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 3 (***)

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 $k \in \mathbb{Z}$, $\delta = d \wedge k$ non nul car d non nul 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 $d' | k' \ell$ car δ non nul. 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 4 (***)

Soit $(\mathrm{G}, \times)$ un groupe. Pour $a \in \mathrm{G}$, on note

$$\forall x \in \mathrm{G} \qquad \varphi_a(x) = axa^{-1}$$

1. Montrer que φ_a est un automorphisme de G pour tout $a \in \mathrm{G}$.
2. Montrer que $\mathcal{I} = \{\varphi_a, a \in \mathrm{G}\}$ est un sous-groupe du groupe des automorphismes de G.
3. Montrer que si $(\mathcal{I}, \circ)$ est monogène, alors $(\mathrm{G}, \times)$ est commutatif.

Corrigé : 1. Soit $a \in \mathrm{G}$. On a

$$\forall (x,y) \in \mathrm{G}^2 \qquad \varphi_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y)$$

Puis

$$y = \varphi_a(x) \iff y = axa^{-1} \iff x = a^{-1}ya$$

Ainsi

$$\boxed{\text{L'application } \varphi_a \text{ est un automorphisme de G pour tout } a \in \mathrm{G}.}$$

2. D'après le calcul précédent, pour $b \in \mathrm{G}$, on a $(\varphi_b)^{-1} = \varphi_{b^{-1}}$ puis

$$\forall (a,b) \in \mathrm{G}^2 \qquad \varphi_a \circ (\varphi_b)^{-1} = \varphi_{ab^{-1}} \in \mathcal{I}$$

et $\mathrm{id} = \varphi_e \in \mathcal{I}$ d'où

$$\boxed{\text{L'ensemble } \mathcal{I} \text{ est un sous-groupe du groupe des automorphismes de G.}}$$

3. Si $(\mathcal{I}, \circ)$ est monogène, alors il existe $a \in \mathrm{G}$ tel que

$$\mathcal{I} = \langle \varphi_a \rangle = \{\varphi_{a^k}, k \in \mathbb{Z}\}$$

Soit $(b,c) \in \mathrm{G}^2$. Il existe $(p,q) \in \mathbb{Z}^2$ tel que $\varphi_b = \varphi_{a^p}$ et $\varphi_c = \varphi_{a^q}$. Puis

$$\begin{aligned} bcb^{-1}c^{-1} &= \varphi_b(c)c^{-1} = \varphi_{a^p}(c)c^{-1} = a^pca^{-p}c^{-1} \\ &= a^p\varphi_c(a^{-p}) = a^p\varphi_{a^q}(a^{-p}) = a^pa^qa^{-p}a^{-q} = a^{p+q-p-q} = e \end{aligned}$$

Ainsi

$$\boxed{\text{Le groupe } (\mathrm{G}, \times) \text{ est commutatif.}}$$

Remarque : On peut alors observer que $\mathcal{I} = \{\mathrm{id}\}$.

Exercice 5 (***)

Soient $(\mathrm{G}_1, \times)$ et $(\mathrm{G}_2, \times)$ deux groupes cycliques.

1. Pour $(x,y) \in \mathrm{G}_1 \times \mathrm{G}_2$, déterminer l'ordre de (x,y) en fonction de $o(x)$ et $o(y)$.
2. Déterminer une condition nécessaire et suffisante pour avoir $\mathrm{G}_1 \times \mathrm{G}_2$ cyclique.

Corrigé : 1. On notera $o(x,y)$ l'ordre de (x,y). Soit k entier non nul tel que $(x,y)^k = (e_1,e_2)$, ce qui équivaut à $(x^k,y^k) = (e_1,e_2)$. Un tel entier existe comme par exemple $o(x)o(y)$. Puis, comme $(x^k,y^k) = (e_1,e_2)$, il vient $o(x)|k$ et $o(y)|k$. Or, on veut l'entier minimal vérifiant ces conditions et on conclut

$$\boxed{o(x,y) = o(x) \vee o(y)}$$

2. Notons $n = \mathrm{Card}\ \mathrm{G}_1$ et $m = \mathrm{Card}\ \mathrm{G}_2$. Supposons $\mathrm{G}_1 \times \mathrm{G}_2$ cyclique. Il existe donc un élément (x,y) tel $o(x,y) = nm$. Or, on a $o(x,y) = o(x) \vee o(y)$. Puis

$$(o(x) \wedge o(y))(o(x) \vee o(y)) = o(x)o(y) \quad \Longrightarrow \quad o(x) \vee o(y) | o(x)o(y)$$

et enfin $o(x)|n$ et $o(y)|m$. Ainsi, on a

$$nm = o(x,y) = o(x) \vee o(y) | o(x)o(y) | nm$$

d'où $o(x) \vee o(y) = o(x)o(y) = nm$ et $o(x) = n$, $o(y) = m$. Il en résulte que x et y sont des générateurs respectifs de G_1 et G_2 et les ordres n et m sont premiers entre eux. Réciproquement, supposons $n \wedge m = 1$. Alors, considérant x et y générateurs respectifs de G_1 et G_2, on a

$$o(x,y) = o(x) \vee o(y) = n \vee m = nm$$

ce qui prouve que $\mathrm{G}_1 \times \mathrm{G}_2$ est cyclique. On conclut

$$\boxed{\mathrm{G}_1 \times \mathrm{G}_2 \text{ cyclique} \iff \mathrm{Card}\ \mathrm{G}_1 \wedge \mathrm{Card}\ \mathrm{G}_2 = 1}$$

Exercice 6 (***)

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

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

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 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 $(\Omega, \mathscr{A}, \mathbb{P})$ un espace probabilisé, n un entier non nul et $(\mathrm{X}_i)_{1 \leqslant i \leqslant n}$ une famille de variables aléatoires indépendantes avec $\mathrm{X}_i \sim \mathscr{U}_{[\![1\,;\,i]\!]}$ pour tout $i \in [\![\, 1\,;\, n \,]\!]$. On pose

$$\sigma_n = \begin{pmatrix} 1 & \mathrm{X}_1 \end{pmatrix} \begin{pmatrix} 2 & \mathrm{X}_2 \end{pmatrix} \ldots \begin{pmatrix} n & \mathrm{X}_n \end{pmatrix}$$

Montrer que $\sigma_n \sim \mathscr{U}_{\mathrm{S}_n}$.

Corrigé : On procède par récurrence sur n. Le cas $n = 1$ est immédiat. Supposons la propriété vraie pour $n \geqslant 1$ fixé. Soit $\sigma \in \mathrm{S}_{n+1}$. On a

$$\begin{aligned}\mathbb{P}(\sigma_{n+1}=\sigma) &= \mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}\begin{pmatrix}n+1 & \mathrm{X}_{n+1}\end{pmatrix}=\sigma\right)\\ &= \mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}=\sigma\begin{pmatrix}n+1 & \mathrm{X}_{n+1}\end{pmatrix}\right)\end{aligned}$$

D'après la formule des probabilités totales, on a

$$\mathbb{P}(\sigma_{n+1}=\sigma)=\sum_{i=1}^{n+1}\mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}=\sigma\begin{pmatrix}n+1 & i\end{pmatrix},\mathrm{X}_{n+1}=i\right)$$

Par indépendance, il vient

$$\mathbb{P}(\sigma_{n+1}=\sigma)=\sum_{i=1}^{n+1}\mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}=\sigma\begin{pmatrix}n+1 & i\end{pmatrix}\right)\mathbb{P}(\mathrm{X}_{n+1}=i)$$

La permutation $\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}$ admet $n+1$ comme point fixe. La permutation $\sigma\begin{pmatrix}n+1 & i\end{pmatrix}$ admet $n+1$ comme point fixe si et seulement $i=\sigma^{-1}(n+1)$. Par suite, on a

$$\mathbb{P}(\sigma_{n+1}=\sigma)=\mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}=\sigma\begin{pmatrix}n+1 & \sigma^{-1}(n+1)\end{pmatrix}\right)\mathbb{P}(\mathrm{X}_{n+1}=\sigma^{-1}(n+1))$$

En confondant $\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}$ et $\sigma\begin{pmatrix}n+1 & \sigma^{-1}(n+1)\end{pmatrix}$ avec leurs restrictions à $[\![1\,;n]\!]$ puisqu'elles admettent $n+1$ comme point fixe, on obtient

$$\mathbb{P}(\sigma_{n+1}=\sigma)=\frac{1}{n!}\times\frac{1}{n+1}=\frac{1}{(n+1)!}$$

Par récurrence, on conclut $\boxed{\sigma_n\sim\mathscr{U}_{\mathrm{S}_n}}$

Remarque : C'est le principe de l'algorithme de *Fisher-Yates* implémenté dans la méthode `numpy.random.shuffle` en python. Cet algorithme agit en place avec une complexité temporelle en $\mathrm{O}(n)$.

Exercice 9 (***)

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 $\sum_{\sigma\in\mathrm{D}_n}\varepsilon(\sigma)$.

Corrigé : On peut interpréter $\sum_{\sigma\in\mathrm{D}_n}\varepsilon(\sigma)$ 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 $\prod_{i=1}^{n}m_{i,\sigma(i)}=1$ 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 10 (****)

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*

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

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

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

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 $a < c < a + (b - a) = b$.

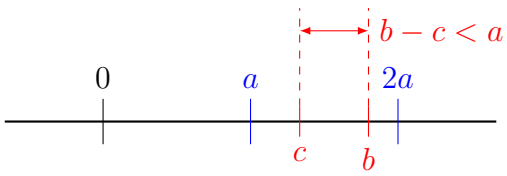

FIGURE 2 – Sous-groupe discret de $\mathbb{R}$

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.