

## Structures algébriques

### Lois de compositions internes

#### Exercice 19.1 (★)

On pose pour tout  $(x, y) \in [0, 1] \times [0, 1]$  :

$$x \star y = x + y - xy$$

1. Montrer que  $\star$  définit une loi de composition interne commutative et associative sur  $[0, 1]$  avec élément neutre.
  2. Quels sont les éléments inversibles de  $([0, 1], \star)$  ?
- 

### Groupes

#### Exercice 19.2 (★★)

On munit  $E = ]-1, 1[$  de la loi de composition  $*$  définie pour tout  $(x, y) \in E^2$  par :

$$x * y = \frac{x + y}{1 + xy}.$$

1. Montrer que  $*$  est une loi de composition interne sur  $E$ .
  2. Montrer que  $(E, *)$  est un groupe commutatif.
  3. Montrer que la fonction tangente hyperbolique  $\text{th}$  est un isomorphisme de groupes de  $(\mathbb{R}, +)$  sur  $(E, *)$ .
- 

#### Exercice 19.3 (★★)

Dans chacun des cas suivants, déterminer si  $H$  est ou non un sous-groupe de  $G$ .

- |  |   |
|--|---|
| <p>(i) <math>G = (\mathbb{C}^*, \times)</math>, <math>H = \bigcup_{n \in \mathbb{N}^*} \mathbb{U}_n</math>.</p> <p>(ii) <math>G = \mathcal{M}_n(\mathbb{C})</math>, <math>H</math> l'ensemble des matrices triangulaires supérieures de <math>G</math>.</p> <p>(iii) <math>G = \text{GL}_2(\mathbb{R})</math>, <math>H</math> l'ensemble des éléments de <math>G</math> dont tous les coefficients</p> | <p>sont dans <math>\mathbb{Z}</math>.</p> <p>(iv) <math>G = \text{GL}_n(\mathbb{R})</math>, <math>H</math> l'ensemble des matrices triangulaires supérieures dont les coefficients diagonaux valent 1.</p> <p>(v) <math>G = \mathfrak{S}_n</math>, <math>H = \{\sigma \in \mathfrak{S}_n \mid \sigma(1) = 2\}</math>.</p> |
|--|---|
- 

#### Exercice 19.4 (★★)

Dans cet exercice, on note  $G$  l'ensemble des similitudes directes du plan, qu'on assimile à l'ensemble des fonctions  $f : \mathbb{C} \rightarrow \mathbb{C}$  telles qu'il existe  $(a, b) \in \mathbb{C}^* \times \mathbb{C}$  tels que pour tout  $z \in \mathbb{C}$ ,  $f(z) = az + b$ .

1. Montrer que  $(G, \circ)$  est un groupe, et qu'il n'est pas abélien.

2. Soit  $z_0 \in \mathbb{C}$ . On pose  $G_{z_0} = \{g \in G \mid g(z_0) = z_0\}$ .

Montrer que  $G_{z_0}$  est un sous-groupe de  $G$ , isomorphe à  $\mathbb{C}^*$ . Est-il abélien ?

3. Soit  $H$  l'ensemble des homothéties et des translations du plan. Montrer que  $H$  est un sous-groupe de  $G$ . Est-il abélien ?

### Exercice 19.5 (★★ - Centre d'un groupe - 📌)

Soit  $(G, *)$  un groupe. On appelle centre de  $G$  l'ensemble :

$$\mathcal{Z}(G) = \{x \in G \mid \forall y \in G, x * y = y * x\}.$$

1. Montrer que  $\mathcal{Z}(G)$  est un sous-groupe de  $G$ . À quelle condition a-t-on  $\mathcal{Z}(G) = G$  ?

2. Déterminer  $\mathcal{Z}(\mathrm{GL}_n(\mathbb{K}))$  lorsque  $n \geq 2$  (avec  $\mathbb{K} = \mathbb{R}$  ou  $\mathbb{C}$ ). Que dire si  $n = 1$  ?

*Indication : montrer que si  $M \in \mathcal{Z}(\mathrm{GL}_n(\mathbb{K}))$ , alors  $M$  commute avec toute matrice élémentaire.*

### Exercice 19.6 (★★★ - Union de sous-groupes)

1. Donner un exemple de deux sous-groupes de  $(\mathbb{R}^*, \times)$  dont l'union n'est pas un sous-groupe.

2. Soit  $G$  un groupe,  $H$  et  $K$  deux sous-groupes de  $G$ . Montrer que  $H \cup K$  est un sous-groupe si, et seulement si,  $H \subset K$  ou  $K \subset H$ .

3. Soit  $(H_n)_{n \in \mathbb{N}}$  une suite croissante (pour l'inclusion) de sous-groupes de  $G$ . Montrer que  $\bigcup_{n \in \mathbb{N}} H_n$  est un sous-groupe de  $G$ .

1. On peut par exemple proposer  $H = \langle 2 \rangle = \{2^k, k \in \mathbb{Z}\}$  et  $K = \langle 3 \rangle = \{3^\ell, \ell \in \mathbb{Z}\}$ . On remarque que 2 et 3 appartiennent à  $H \cup K$ , mais pas leur produit 6. Ainsi,  $H \cup K$  n'est pas stable par produit : ça n'est pas un sous-groupe de  $(\mathbb{R}^*, \times)$ .

**Remarque.** On a vu en cours que si  $(H_i)_{i \in I}$  est une famille de sous-groupes d'un groupe  $G$ , alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ . Ce n'est donc pas vrai pour l'union

: une union de sous-groupes n'est en général pas un sous-groupe. Le but de la suite de cet exercice est de déterminer des conditions nécessaires et/ou suffisantes pour lesquelles c'est le cas.

2. Si  $H \subset K$ ,  $H \cup K = K$  est effectivement un sous groupe de  $G$ . De même si  $K \subset H$ .

Pour la réciproque, supposons que  $H \cup K$  est un sous-groupe de  $G$ . Par l'absurde, si  $H \not\subset K$  et  $K \not\subset H$ , il existe  $h \in H \setminus K$  et  $k \in K \setminus H$ . Puisque  $h, k \in H \cup K$  qui est un sous-groupe de  $G$  par hypothèse,  $h * k$  appartient à  $H \cup K$ . Deux cas se présentent :

- si  $h * k$  appartient à  $H$ , alors :

$$k = \underbrace{h^{-1}}_{\in H} * \underbrace{(h * k)}_{\in H} \in H$$

ce qui est contradictoire par définition de  $k$  ;

- on aboutit de même à une contradiction si  $h * k \in K$ .

Par conséquent,  $H \subset K$  ou  $K \subset H$ .

3. Soit  $(H_n)_{n \in \mathbb{N}}$  une suite croissante de sous-groupes de  $G$ . Montrons que  $K = \bigcup_{n \in \mathbb{N}} H_n$  est un sous-groupe de  $G$  :

- l'élément neutre  $e$  de  $G$  appartient au sous-groupe  $H_0$  (par exemple), donc à  $K$  ;
- soient  $g, h$  dans  $K$  : il existe  $i, j \in \mathbb{N}$  tels que  $g \in H_i$  et  $h \in H_j$ . En notant  $n = \max(i, j)$ , par croissance de la suite de sous-groupes,  $H_i \subset H_n$  et  $H_j \subset H_n$ . Ainsi,  $g$  et  $h$  appartiennent à  $H_n$ , et donc  $g * h^{-1}$  également car  $H_n$  est un sous-groupe de  $G$ . Finalement,  $g * h^{-1}$  appartient bien à  $K$ .

Par la caractérisation des sous-groupes,  $K$  est un sous-groupe de  $G$ .

### Exercice 19.7 (★★★ - Sous-groupes de $\mathbb{Z}$ - )

1. Soit  $n \in \mathbb{Z}$ . Montrer que l'ensemble  $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$  est un sous-groupe de  $\mathbb{Z}$ .
2. Soit  $H$  un sous-groupe de  $\mathbb{Z}$  non réduit à  $\{0\}$ .
  - (a) Justifier l'existence du minimum  $n_0$  de l'ensemble  $E = \{h \in H \mid h > 0\}$ .
  - (b) Montrer que  $n_0\mathbb{Z} \subset H$ .
  - (c) Soit  $h \in H$ . En considérant la division euclidienne de  $h$  par  $n_0$ , montrer que  $h \in n_0\mathbb{Z}$ .
  - (d) Que peut-on en conclure sur les sous-groupes de  $\mathbb{Z}$  ?
3. Soit  $(G, *)$  un groupe fini d'élément neutre  $e$ , et  $a \in G$ .
  - (a) Montrer que l'application  $\varphi_a : p \in \mathbb{Z} \mapsto a^p \in G$  est un morphisme de groupes.
  - (b) En déduire l'existence et l'unicité d'un entier  $n \in \mathbb{N}^*$  tel que : 
$$\begin{cases} a^n = e, \\ \forall p \in \mathbb{Z}, a^p = e \Leftrightarrow n \mid p \end{cases}$$

### Exercice 19.8 (★★★ - Un cas particulier du théorème de Lagrange - )

Soit  $G$  un groupe commutatif fini, de cardinal  $n$ .

1. Soit  $g \in G$ . Montrer que  $x \mapsto gx$  est une bijection de  $G$  sur lui-même.
2. Soit  $g \in G$ . En calculant de deux manières le produit  $\prod_{x \in G} (gx)$ , montrer que  $g^n = 1_G$ .
3. Déterminer tous les sous-groupes finis de  $(\mathbb{C}^*, \times)$ .

1. Soit  $g \in G$ . On vérifie que l'application  $\varphi_g : x \mapsto gx$  est une bijection de  $G$  dans  $G$ , de bijection réciproque  $\varphi_{g^{-1}}$ . Pour cela, on vérifiera aisément que  $\varphi_g \circ \varphi_{g^{-1}} = \varphi_{g^{-1}} \circ \varphi_g = \text{id}_G$ .
2. Soit toujours  $g \in G$ . Notons  $P = \prod_{x \in G} (gx)$  et calculons  $P$  de deux manières comme suggéré :
  - en utilisant que  $G$  est commutatif, on peut « sortir »  $g$  du produit, en notant

bien qu'il sort alors  $n = \text{Card}(G)$  fois :

$$P = \prod_{x \in G} (gx) = g^n \prod_{x \in G} x.$$

- en utilisant la question 1 :

$$P = \prod_{x \in G} (gx) = \prod_{x \in G} \varphi_g(x).$$

Puisque  $\varphi_g$  est une bijection de  $G$  dans lui-même, lorsque  $x$  parcourt  $G$ ,  $\varphi_g(x)$  parcourt également tout  $G$  (dans un ordre différent a priori). Ainsi, tous les éléments de  $G$  vont apparaître une et une seule fois dans ce produit, et quitte à le réordonner (on utilise pour cela que  $G$  est commutatif), on peut écrire :

$$P = \prod_{x \in G} x.$$

D'où l'égalité suivante :

$$g^n \left( \prod_{x \in G} x \right) = \prod_{x \in G} x.$$

L'élément  $\left( \prod_{x \in G} x \right)$  étant inversible (comme tous les éléments du groupe  $G$ ), on obtient  $g^n = e$  en multipliant à droite par son inverse.

**Remarque.** On vient ici de démontrer le *théorème de Lagrange* dans le cas particulier d'un groupe abélien, à savoir :

Si  $G$  est un groupe d'ordre fini  $n$ , alors pour tout  $g \in G$ ,  $g^n = 1_G$ .

Ce résultat reste valable sans l'hypothèse  $G$  abélien. Une preuve en a été donnée dans le DM11.

3. Soit  $G$  un sous-groupe fini de  $(\mathbb{C}^*, \times)$  d'ordre  $n$ . Par le théorème de Lagrange,  $g^n = 1$  pour tout  $g \in G$  : tous les éléments de  $G$  sont donc des racines  $n$ -èmes de l'unité. Par conséquent,  $G \subset \mathbb{U}_n$ , et puisque ces deux ensembles ont même cardinal,  $G = \mathbb{U}_n$ .

Réciproquement, il est bien connu que pour tout  $n \geq 1$ ,  $\mathbb{U}_n$  est un sous-groupe fini de  $(\mathbb{C}^*, \times)$ . Ainsi, les sous-groupes finis de  $(\mathbb{C}^*, \times)$  sont les  $\mathbb{U}_n$  pour  $n \geq 1$ .

### Exercice 19.9 (★★ - Automorphismes intérieurs - )

Soit  $G$  un groupe multiplicatif. Pour  $a \in G$ , on note  $f_a : x \in G \mapsto a x a^{-1} \in G$ .

1. Montrer que pour tout  $a \in G$ ,  $f_a$  est un automorphisme de  $G$ .
2. Montrer que  $\varphi : a \in G \mapsto f_a \in \text{Aut}(G)$  est un morphisme de groupes.
3. Déterminer le noyau de  $\varphi$ .

### Exercice 19.10 (★★★)

Déterminer tous les morphismes de groupes de  $(\mathbb{Z}, +)$  dans  $(\mathbb{Z}, +)$ , puis de  $(\mathbb{Q}, +)$  dans  $(\mathbb{Z}, +)$ .

**Exercice 19.11 (★★★)**

Les groupes suivants sont-ils isomorphes :

- |  |   |
|--|---|
| (i) $\mathbb{U}_5$ et $\mathbb{U}_2 \times \mathbb{U}_2$ ; | (iii) $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ ;                    |
| (ii) $(\mathbb{Z}, +)$ et $(\mathbb{R}, +)$ ;              | (iv) $\mathfrak{S}_X$ et $\mathfrak{S}_Y$ lorsque $X$ et $Y$ sont en bijection. |

**Exercice 19.12 (★★★)**

Soient  $G$  un groupe,  $H$  et  $K$  deux sous-groupes de  $G$ . On pose  $HK = \{h * k, h \in H, k \in K\}$ .

- Si  $G$  est abélien, montrer que  $HK$  est un sous-groupe de  $G$ .
- Prouver que  $HK$  est un sous-groupe de  $G$  si, et seulement si,  $HK = KH$ .
- Si  $H$  et  $K$  sont finis et si  $H \cap K = \{e\}$  (où  $e$  désigne l'élément neutre de  $G$ ), montrer que  $\text{Card}(HK) = \text{Card}(H) \cdot \text{Card}(K)$ .

1. Supposons  $G$  abélien. Montrons que  $HK$  est un sous-groupe de  $G$ .

- $e_G = \underbrace{e_G}_{\in H} \underbrace{e_G}_{\in K} \in HK$ .

- Soient  $x, y \in HK$ . Il existe  $(h_1, h_2) \in H^2$  et  $(k_1, k_2) \in K^2$  tels que  $x = h_1 k_1$  et  $y = h_2 k_2$ . Alors (comme  $G$  est abélien) :

$$xy = h_1 k_1 h_2 k_2 = \underbrace{h_1 h_2}_{\in H} \underbrace{k_1 k_2}_{\in K} \in HK.$$

- Soit  $x \in HK$ . Il existe  $h \in H$  et  $k \in K$  tels que  $x = hk$ . Alors (comme  $G$  est abélien) :

$$x^{-1} = k^{-1} h^{-1} = \underbrace{h^{-1}}_{\in H} \underbrace{k^{-1}}_{\in K} \in HK.$$

Donc  $HK$  est un sous-groupe de  $G$ .

2. Supposons que  $HK = KH$ . Prouvons qu'alors  $HK$  est un sous-groupe de  $G$ .

- $e_G = \underbrace{e_G}_{\in H} \underbrace{e_G}_{\in K} \in HK$ .

- Soient  $x, y \in HK$ . Il existe  $(h_1, h_2) \in H^2$  et  $(k_1, k_2) \in K^2$  tels que  $x = h_1 k_1$  et  $y = h_2 k_2$ . Comme  $k_1 h_2 \in KH = HK$ , il existe  $h_3 \in H$  et  $k_3 \in K$  tels que  $k_1 h_2 = h_3 k_3$ . Alors :

$$xy = h_1 k_1 h_2 k_2 = \underbrace{h_1 h_3}_{\in H} \underbrace{k_3 k_2}_{\in K} \in HK.$$

- Soit  $x \in HK$ . Il existe  $h \in H$  et  $k \in K$  tels que  $x = hk$ . Alors

$$x^{-1} = k^{-1} h^{-1} \in KH = HK.$$

Ainsi,  $HK$  est un sous-groupe de  $G$ .

Inversement, supposons que  $HK$  soit un sous-groupe de  $G$ . Montrons que  $HK = KH$ .

- Soit  $x \in KH$ . Il existe  $h \in H$  et  $k \in K$  tels que  $x = kh$ . Alors :

$$x = kh = \underbrace{e_G k}_{\in HK} \underbrace{h e_G}_{\in HK} \in HK$$

car  $HK$  est un sous-groupe de  $G$ . Donc  $KH \subset HK$ .

- Inversement, soit  $x \in HK$ . Alors  $x^{-1} \in HK$  (car  $HK$  est un sous-groupe), et il existe  $h \in H$  et  $k \in K$  tels que  $x^{-1} = hk$ , de sorte que  $x = k^{-1}h^{-1} \in KH$ .

Donc  $KH = HK$ .

3. Considérons l'application  $f$  suivante :

$$f : \begin{array}{ccc} H \times K & \rightarrow & HK \\ (h, k) & \mapsto & hk \end{array} .$$

Par définition de l'ensemble  $HK$ ,  $f$  est surjective. Montrons qu'elle est injective.



### Mise en garde.

L'application  $f$  n'étant pas un morphisme de groupes (je vous laisse vous en convaincre si besoin), on ne peut étudier son noyau. On est ici contraint de revenir à la caractérisation générale de l'injectivité vue au chapitre sur les applications.

Soient  $(h_1, k_1), (h_2, k_2)$  dans  $H \times K$ . Alors :

$$f((h_1, k_1)) = f((h_2, k_2)) \Leftrightarrow h_1 k_1 = h_2 k_2 \Leftrightarrow \underbrace{h_2^{-1} h_1}_{\in H} = \underbrace{k_2 k_1^{-1}}_{\in K} .$$

Ainsi,  $h_2^{-1} h_1 \in H \cap K$  et  $k_2 k_1^{-1} \in H \cap K$ . Comme  $H \cap K = \{e\}$ ,  $h_2^{-1} h_1 = e$ , et donc  $h_1 = h_2$  et de même  $k_1 = k_2$ . Ainsi,  $f$  est injective, et donc bijective.

Si  $H$  et  $K$  sont finis, alors  $H \times K$  l'est aussi. Puisque  $f$  est bijective, l'ensemble  $HK$  est fini et :

$$\text{Card}(HK) = \text{Card}(H \times K) = \text{Card}(H) \cdot \text{Card}(K).$$

### Exercice 19.13 (★★★★)

Soit  $G$  un groupe non réduit à un élément tel que pour tout  $g \in G$ ,  $g^2 = e$ .

1. Montrer que  $G$  est abélien.
2. Montrer que  $G$  possède au moins un sous-groupe de cardinal 2.
3. On suppose que  $G$  contient au moins trois éléments. Soit  $H$  un sous-groupe fini de  $G$ , différent de  $\{e\}$  ou de  $G$ , et soit  $g \in G \setminus H$ . On pose alors  $gH = \{gh, h \in H\}$ .
  - (a) Montrer que  $H \cup gH$  est un sous-groupe de cardinal  $2|H|$ .
  - (b) Montrer que si  $G$  est fini, alors son cardinal est une puissance de 2.

1. Pour tout  $g \in G$ ,  $gg = g^2 = e$ , de sorte que  $g^{-1} = g$ .

Si  $g, h \in G$ , on obtient alors  $gh = (gh)^{-1} = h^{-1}g^{-1} = hg$ . Donc  $G$  est abélien.

2. Comme  $G$  n'est pas réduit à un élément, il existe  $g \in G$  tel que  $g \neq e$ . On vérifie alors sans difficulté que  $\{e, g\}$  est un sous-groupe de  $G$  de cardinal 2.

3. (a) Remarquons que, d'après la question précédente, un tel sous-groupe  $H$  existe.

Montrons que  $H \cup gH$  est un sous-groupe de  $G$ .

- Puisque  $e \in H$  (car c'est un sous-groupe),  $e$  appartient à  $H \cup gH$ .
- Soient  $g_1, g_2 \in H \cup gH$ . Montrons que  $g_1g_2^{-1} = g_1g_2$  appartient à  $H \cup gH$ .

On procède par disjonction de cas :

- Si  $g_1, g_2 \in H$ , alors  $g_1g_2 \in H \subset H \cup gH$  car  $H$  est un sous-groupe.
- si  $g_1 \in H$  et  $g_2 = gh_2 \in gH$ , alors :

$$g_1g_2 = g_1gh_2 = g \underbrace{(g_1h_2)}_{\in H} \in gH \subset H \cup gH.$$

- si  $g_1 = gh_1 \in gH$  et  $g_2 \in H$ , alors :

$$g_1g_2 = g \underbrace{(h_1g_2)}_{\in H} \in gH \subset H \cup gH.$$

- si  $g_1 = gh_1 \in gH$  et  $g_2 = gh_2 \in gH$ , alors :

$$g_1g_2 = gh_1gh_2 = g^2h_1h_2 = h_1h_2 \in H \subset H \cup gH.$$

Ainsi,  $H \cup gH$  est un sous-groupe de  $G$ .

On vérifie aisément que  $h \mapsto gh$  définit une bijection de  $H$  sur  $gH$ . Puisque  $H$  est fini, il en est de même de  $gH$ , et ces ensembles ont même cardinal.

Par ailleurs, les ensembles  $H$  et  $gH$  sont disjoints. En effet, supposons par l'absurde qu'il existe  $x \in H \cap gH$ . Alors  $x \in H$  et il existe  $h \in H$  tel que  $x = gh$ . Mais  $g = xh^{-1}$  appartiendrait aussi au sous-groupe  $H$ , ce qui est absurde puisqu'on a supposé  $g \notin H$ .

Finalement,  $\text{Card}(H \cup gH) = \text{Card}(H) + \text{Card}(gH) = 2\text{Card}(H)$ .

(b) On suppose que  $G$  est fini. Montrons que c'est une puissance de 2. Raisonnons par l'absurde pour cela.

Soit  $H_1$  un sous-groupe de  $G$  de cardinal 2 (existe bien par la question 2.). Alors  $H_1 \neq G$  (puisque le cardinal de  $G$  n'est pas une puissance de 2), et il existe  $g_1 \in G \setminus H_1$ . Par ce qui précède,  $H_2 = H_1 \cup g_1H_1$  est un sous-groupe de  $G$  de cardinal 4.

Mais alors  $H_2 \neq G$  puisque  $G$  n'est pas de cardinal 4. Donc il existe  $g_2 \in G \setminus H_2$ , et  $H_3 = H_2 \cup g_2H_2$  est un sous-groupe de  $G$  de cardinal 8.

En poursuivant ce raisonnement, on construit par récurrence une suite de sous-groupes  $(H_k)_{k \geq 1}$  tels que  $H_k$  soit de cardinal  $2^k$ . Mais si  $k$  est suffisamment grand,  $2^k > \text{Card}(G)$ , ce qui est absurde.

Donc  $\text{Card}(G)$  est nécessairement une puissance de 2.

### Exercice 19.14 (★★★★)

1. Soit  $H$  un sous-groupe de  $(\mathbb{R}, +)$  non réduit à  $\{0\}$ .

- (a) Montrer l'existence de  $a = \inf\{h \in H \mid h > 0\}$ .
- (b) Montrer que si  $a > 0$ , alors  $H = a\mathbb{Z}$ .
- (c) Montrer que si  $a = 0$ , alors  $H$  est une partie dense de  $\mathbb{R}$ .

2. **Application.** On admet que  $\pi$  est irrationnel. Prouver que l'ensemble  $\mathbb{Z} + 2\pi\mathbb{Z}$  est dense dans  $\mathbb{R}$ . En déduire que l'ensemble  $A = \{\cos(n), n \in \mathbb{N}\}$  est dense dans  $[-1, 1]$ .

1. (a) Notons  $A = \{h \in H \mid h > 0\}$ . Cette partie de  $\mathbb{R}$  est par définition minorée par 0. Montrons qu'elle est non vide. Puisque  $H \neq \{0\}$ , il existe  $h \in H$  tel que  $h \neq 0$ . Si  $h > 0$ ,  $h$  appartient à  $A$  et  $A \neq \emptyset$ . Si  $h < 0$ , alors son symétrique  $-h$  est strictement positif et appartient à  $H$  (puisque  $H$  est un sous-groupe de  $(\mathbb{R}, +)$ ), et donc à  $A$ .

Ainsi,  $A$  est bien une partie non vide et minorée de  $\mathbb{R}$ , d'où l'existence de  $a = \inf(A)$ .

- (b) Supposons dans cette question  $a > 0$ .

Par l'absurde, supposons que  $a$  n'appartienne pas à  $H$ .  $a$  est par définition le plus grand des minorants de  $A$ . Comme  $2a > a$ ,  $2a$  n'est pas un minorant de  $A$ . D'où l'existence d'un élément  $x \in H$  tel que  $a < x < 2a$ . De même,  $x$  n'est pas un minorant de  $A$ , et il existe  $y \in H$  tel que  $a < y < x < 2a$ .

Puisque  $H$  est un sous-groupe de  $(\mathbb{R}, +)$ ,  $x - y$  appartient à  $H$ , et est par définition strictement compris entre 0 et  $a$ . Or ceci est contradictoire avec la définition de  $a$  comme borne inférieure de  $A = \{h \in H \mid h > 0\}$ .

Ainsi, l'élément  $a$  appartient bien à  $H$ .

Montrons maintenant que  $H = a\mathbb{Z}$ . Puisque  $a$  appartient à  $H$ , le sous-groupe  $a\mathbb{Z} = \langle a \rangle$  qu'il engendre est inclus dans  $H$  (puisque  $H$  est un sous-groupe).

Réciproquement, soit  $b$  un élément de  $H$ . Comme  $a > 0$ , on peut poser  $q = \left\lfloor \frac{b}{a} \right\rfloor$  et  $r = b - aq$ . Puisque  $b$  et  $aq$  sont dans  $H$  (car  $a\mathbb{Z} \subset H$ ),  $r$  appartient également au sous-groupe  $H$ . De plus, par définition de la partie entière :

$$q \leq \frac{b}{a} < q + 1, \quad \text{d'où} \quad 0 \leq b - aq < a.$$

Ainsi,  $r$  appartient à  $H \cap [0, a[$ . Par définition de  $a$ ,  $r$  est donc nul, et  $b = aq$  appartient à  $a\mathbb{Z}$ .

On a ainsi montré que  $H = a\mathbb{Z}$ .

- (c) Supposons dans cette question  $a = 0$ . Montrons que  $G$  est dense dans  $\mathbb{R}$ .

Soit  $I = ]x, y[$  un intervalle ouvert non vide de  $\mathbb{R}$ . Puisque  $y - x > 0$ , il existe (par définition de la borne inférieure) un élément  $h \in H$  tel que  $0 < h < y - x$ . L'ensemble :

$$R = \{k \in \mathbb{Z} \mid kh > x\}$$

est une partie non vide (car  $\mathbb{R}$  est archimédien) et minorée de  $\mathbb{Z}$ . Elle admet donc un plus petit élément  $n \in \mathbb{Z}$ , qui satisfait par définition :

$$(n - 1)h \leq x < nh, \quad \text{d'où} \quad x < nh \leq x + h < x + (y - x) = y.$$

Donc  $nh$  appartient à l'intervalle  $]x, y[$ . Ceci prouve que  $H$  est dense dans  $\mathbb{R}$ .

2.

### Exercice 19.15 (★★★★)

Soit  $(G, *)$  un groupe, et soit  $A$  une partie non vide **finie** de  $G$ , stable par  $*$ . Prouver que  $A$  est un sous-groupe de  $G$ .

### Exercice 19.16 (★★★★)

Soit  $G$  un groupe possédant exactement deux sous-groupes. Montrer qu'il existe  $x \in G$  tel que  $G = \langle x \rangle$ , que  $G$  est fini, et que son cardinal est premier.

Remarquons pour commencer que  $G$  n'est pas le groupe trivial réduit à un élément, étant donné qu'il possède exactement deux sous-groupes. Notons également que puisque  $\{e\}$  et  $G$  sont des sous-groupes distincts de  $G$  (où  $e$  désigne l'élément neutre de  $G$ ), il n'y en a donc pas d'autres par hypothèse.

Prenons alors  $x$  dans  $G$  distinct de l'élément neutre  $e$  de  $G$ , et considérons  $\langle x \rangle$  le sous-groupe de  $G$  engendré par  $x$ . Celui-ci étant non trivial (car  $x \neq e$ ), il est donc égal à  $G$ .

Si  $x^2 = e$ , alors  $G = \{e, x\}$  est bien fini. Sinon, considérons le sous-groupe  $\langle x^2 \rangle$  engendré par  $x^2$ . Ce sous-groupe étant non réduit à  $\{e\}$  (car  $x^2 \neq e$ ), il est par hypothèse égal à  $G$ . Ainsi,  $x$  appartient à  $\langle x^2 \rangle$ , et il existe  $k \in \mathbb{Z}$  tel que  $x = x^{2k}$ , et donc  $x^{2k-1} = e = x^{1-2k}$ .

Considérons  $\{m \in \mathbb{N}^* \mid x^m = e\}$ . Cet ensemble est non vide (il contient  $2k - 1$  ou  $1 - 2k$ ), et admet donc un plus petit élément. Notons le  $n$ .

Montrons alors que  $G = \{x^s, s \in \llbracket 0, n - 1 \rrbracket\}$ . L'inclusion  $\supset$  est immédiate. Réciproquement, soit  $s \in \mathbb{Z}$ , et notons  $q$  et  $r$  les quotient et reste de la division euclidienne de  $s$  par  $n$  :

$$s = nq + r \quad \text{et} \quad 0 \leq r \leq n - 1.$$

Alors :

$$x^s = x^{nq+r} = (x^n)^q * x^r = e^q * x^r = x^r.$$

D'où l'inclusion  $G \subset \{x^s, s \in \llbracket 0, n - 1 \rrbracket\}$ . Ainsi,  $G$  est bien fini de cardinal au plus  $n$ .

Notons que les éléments de  $\{x^s, s \in \llbracket 0, n - 1 \rrbracket\}$  sont deux à deux distincts. En effet, s'il existe  $0 \leq i < j \leq n - 1$  tel que  $x^i = x^j$ , alors  $x^{j-i} = e$  avec  $1 \leq j - i < n$ , ce qui contredit la minimalité de  $n$ . Ainsi,  $G = \{x^s, s \in \llbracket 0, n - 1 \rrbracket\}$  et est de cardinal  $n$ .

Supposons enfin que  $n$  ne soit pas premier, et considérons  $a, b \in \llbracket 2, n - 1 \rrbracket$  tels que  $n = ab$ . Alors  $(x^a)^b = x^{ab} = x^n = e$  et pour tout  $k \in \llbracket 1, b - 1 \rrbracket$ ,  $(x^a)^k = x^{ka} \neq e$  car  $1 \leq ka < n$ .

Ainsi,  $\langle x^a \rangle = \{e, x^a, \dots, (x^a)^{b-1}\}$  est un sous-groupe de  $G$  de cardinal  $b$ , et donc ni égal à  $\{e\}$ , ni à  $G$ . D'où une contradiction. Donc  $n$  est premier.

## Anneaux, corps

### Exercice 19.17 (★)

On note  $A$  l'ensemble des matrices  $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ ,  $a$  et  $b$  décrivant  $\mathbb{Z}$ .

Montrer que  $A$  est un anneau pour les lois d'addition et de multiplication matricielles, puis déterminer  $\mathcal{U}(A)$ .

### Exercice 19.18 (★★)

L'anneau  $(\mathbb{R}^{\mathbb{R}}, +, \times)$  est-il intègre ? Déterminer  $\mathcal{U}(\mathbb{R}^{\mathbb{R}})$ .

### Exercice 19.19 (★★)

Soit  $a \in \mathbb{N}^*$  fixé. On pose  $A_a = \left\{ \frac{p}{a^n} \mid p \in \mathbb{Z}, n \in \mathbb{N} \right\}$ .

1. Montrer que  $A_a$  est un sous-anneau de  $\mathbb{Q}$ .
2. Montrer  $\mathcal{U}(A_2) = \{\pm 2^k, k \in \mathbb{Z}\}$ .
3. Déterminer  $\mathcal{U}(A_{10})$ .

### Exercice 19.20 (★★)

1. On rappelle que  $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$  est un sous-anneau de  $\mathbb{C}$ .

Montrer que pour tout  $z \in \mathbb{Z}[i]$ ,  $|z|^2 \in \mathbb{N}$ , puis en déduire  $\mathcal{U}(\mathbb{Z}[i])$ .

2. Montrer que l'ensemble  $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2}, a, b \in \mathbb{Z}\}$  est un sous-anneau de  $\mathbb{C}$ , puis déterminer  $\mathcal{U}(\mathbb{Z}[i\sqrt{2}])$ .

1. Soit  $z \in \mathbb{Z}[i]$ , qu'on note  $z = a + ib$  avec  $a, b \in \mathbb{Z}$ . Alors  $|z|^2 = a^2 + b^2 \in \mathbb{N}$ .

Supposons que  $z$  soit inversible dans  $\mathbb{Z}[i]$  : il existe  $z' \in \mathbb{Z}[i]$  tel que  $z \times z' = 1$ . En prenant le module au carré, on obtient l'égalité dans  $\mathbb{N}$  :

$$|z|^2 \times |z'|^2 = 1.$$

Puisque  $|z|^2$  et  $|z'|^2$  sont des entiers naturels, cette égalité implique  $|z|^2 = 1$ , et donc  $a^2 + b^2 = 1$ . De nouveau, puisque  $a^2$  et  $b^2$  sont dans  $\mathbb{N}$ , on obtient  $\begin{cases} a^2 = 1 \\ b^2 = 0 \end{cases}$  ou

$$\begin{cases} a^2 = 0 \\ b^2 = 1 \end{cases}, \text{ et donc } z = \pm 1 \text{ ou } z = \pm i.$$

Réciproquement, on vérifie sans difficulté que  $1, -1, i, -i$  sont bien inversibles dans  $\mathbb{Z}[i]$  d'inverses respectivement  $1, -1, -i, i$ . Ainsi,  $\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$ .

2. Laissez en exercice, on procèdera comme précédemment pour montrer que  $\mathcal{U}(\mathbb{Z}[i\sqrt{2}]) = \{1, -1\}$ .

**Exercice 19.21 (★★ - Produit direct d'anneaux - )**

Soient  $(A, +_A, \times_A)$  et  $(B, +_B, \times_B)$  deux anneaux. On munit  $A \times B$  de deux lois de composition  $\oplus$  et  $\otimes$  définies par :

$$(a, b) \oplus (a', b') = (a +_A a', b +_B b') \text{ et } (a, b) \otimes (a', b') = (a \times_A a', b \times_B b')$$

Montrer que  $(A \times B, \oplus, \otimes)$  est un anneau, commutatif si  $A$  et  $B$  le sont. Cet anneau est-il intègre ?

**Exercice 19.22 (★★)**

Parmi les ensembles suivants, lesquels sont des sous-anneaux de  $\mathbb{R}^{\mathbb{N}}$ , l'anneau des suites réelles ?

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>(i) l'ensemble des suites de limite nulle ;</li> <li>(ii) l'ensemble des suites croissantes ;</li> <li>(iii) l'ensemble des suites convergentes ;</li> <li>(iv) l'ensemble des suites divergentes ;</li> <li>(v) l'ensemble des suites bornées ;</li> </ul> | <ul style="list-style-type: none"> <li>(vi) l'ensemble des suites <math>(u_n)</math> telles que <math>\lim_{n \rightarrow +\infty} u_n = +\infty</math> ;</li> <li>(vii) l'ensemble des suites stationnaires ;</li> <li>(viii) l'ensemble des suites nulles à partir d'un certain rang.</li> </ul> |
|--|--|

**Exercice 19.23 (★★ - Anneau de Boole)**

Soit  $A$  un anneau non nul pour lequel  $x^2 = x$  pour tout  $x \in A$ .

1. Montrer que pour tout  $x \in A$ ,  $x = -x$ .
2. Montrer que  $A$  est commutatif.
3. Déterminer  $A$  dans le cas où  $A$  est intègre.
4. On définit une relation binaire  $\preceq$  sur  $A$  en posant pour tous  $x, y \in A$  :  $x \preceq y \Leftrightarrow yx = x$ .  
Montrer que  $\preceq$  est une relation d'ordre.

**Exercice 19.24 (★★★★)**

Montrer qu'un anneau commutatif intègre fini est un corps.

Soit  $(A, +, \times)$  un anneau commutatif intègre fini. Pour prouver que  $A$  est un corps, il suffit de prouver que tout élément non nul de  $A$  admet un inverse.

Prenons pour cela  $x \neq 0_A$ , et considérons l'application :

$$f : \begin{array}{l} A \rightarrow A \\ y \mapsto xy \end{array}$$

L'application  $f$  est injective. En effet, pour tous  $y_1, y_2 \in A$  :

$$f(y_1) = f(y_2) \Leftrightarrow xy_1 = xy_2 \Leftrightarrow xy_1 - xy_2 = 0_A \Leftrightarrow x(y_1 - y_2) = 0_A.$$

Comme  $A$  est intègre et  $x \neq 0_A$ , ceci équivaut à  $y_1 - y_2 = 0_A$ , et donc à  $y_1 = y_2$ .

Comme  $A$  est de cardinal fini et que  $f$  est injective, elle est donc bijective. Tout élément de  $A$  admet donc un unique antécédent par  $f$ . En particulier,  $1_A$  admet un antécédent par  $f$  : il existe  $y \in A$  tel que  $xy = 1_A$ . Comme  $A$  est commutatif,  $yx = xy = 1_A$  et  $x$  est bien inversible (d'inverse  $y$ ).

Par conséquent, tout élément non nul de  $A$  est inversible :  $A$  est bien un corps.

### Exercice 19.25 (★★★★)

Prouver que  $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid (a, b) \in \mathbb{Q}^2\}$  est un corps et déterminer tous ses automorphismes.

Afin de montrer qu'un ensemble est muni d'une structure de corps, il est intéressant de se demander s'il ne pourrait pas s'agir d'un sous-corps d'un ensemble déjà connu. En effet, il y a bien moins de propriétés à prouver pour un sous-corps que pour un corps. Dans le cas qui nous intéresse ici, nous allons montrer que  $\mathbb{Q}(\sqrt{2})$  est un sous-corps de  $(\mathbb{R}, +, \times)$ . Commençons tout d'abord par montrer qu'il s'agit d'un sous-anneau.

- (1)  $\mathbb{Q}(\sqrt{2})$  est bien évidemment une partie de  $\mathbb{R}$ .
- (2) Il est clair que  $1 \in \mathbb{Q}(\sqrt{2})$  puisque  $1 = 1 + 0\sqrt{2}$  avec  $0, 1 \in \mathbb{Q}$ .
- (3) Soit  $(x, y) \in \mathbb{Q}(\sqrt{2})^2$ . Alors il existe  $a, b, c, d \in \mathbb{Q}$  tels que  $x = a + b\sqrt{2}$  et  $y = c + d\sqrt{2}$ .  
Calculons :

$$x - y = \underbrace{(a - c)}_{\in \mathbb{Q}} + \underbrace{(b - d)}_{\in \mathbb{Q}} \sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

- (4) Avec les mêmes notations que celles du point précédent :

$$x \times y = (a + b\sqrt{2}) \times (c + d\sqrt{2}) = \underbrace{(ac + 2bd)}_{\in \mathbb{Q}} + \underbrace{(ad + bc)}_{\in \mathbb{Q}} \sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Pour montrer que  $\mathbb{Q}(\sqrt{2})$  est un sous-corps de  $(\mathbb{R}, +, \times)$ , il nous reste à montrer que tout élément non nul  $x \in \mathbb{Q}(\sqrt{2})$  est inversible dans  $\mathbb{Q}(\sqrt{2})$ . Puisque  $x \in \mathbb{R}^*$ , il est inversible dans  $\mathbb{R}$  et son inverse est  $\frac{1}{x}$ . Il s'agit ici de vérifier que  $\frac{1}{x} \in \mathbb{Q}(\sqrt{2})$ . Puisque  $x \in \mathbb{Q}(\sqrt{2})$ , il existe deux rationnels  $a$  et  $b$  tels que  $x = a + b\sqrt{2}$ . L'inverse de  $x$  dans  $\mathbb{R}$  est :

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2 - 2b^2}}_{\in \mathbb{Q}} \sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Notons que la deuxième égalité est bien valide puisque  $a - b\sqrt{2} \neq 0$ . En effet si  $a = b\sqrt{2}$ , alors nécessairement  $b \neq 0$  (sinon  $b = a = 0$ , et  $x$  aussi, ce qui n'est pas) et on aurait  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$  ce que nous savons faux.

Nous avons montré que  $\mathbb{Q}(\sqrt{2})$  est un sous-corps de  $(\mathbb{R}, +, \times)$ . C'est donc bien un corps.

Pour déterminer les automorphismes de  $(\mathbb{Q}(\sqrt{2}), +, \times)$ , nous allons procéder par analyse-synthèse.

- **Analyse.** Si  $\varphi$  est un automorphisme de  $\mathbb{Q}(\sqrt{2})$ , il satisfait par définition  $\varphi(1) = 1$ . Mais alors  $\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$ . En répétant cet argument, on montre par récurrence que  $\varphi(n) = n$  pour tout  $n \in \mathbb{N}$ .

D'autre part, si  $n \in \mathbb{Z}$  est tel que  $n \leq 0$ , alors  $-n \in \mathbb{N}$ , et par ce qui a été établi précédemment :

$$\varphi(-n) = -n.$$

Mais comme  $\varphi$  est un morphisme de corps :

$$0 = \varphi(0) = \varphi(n - n) = \varphi(n) + \varphi(-n) = \varphi(n) - n.$$

Ainsi,  $\varphi(n) = n$ , égalité vérifiée à présent pour tout  $n \in \mathbb{Z}$ .

Soit à présent  $n \in \mathbb{N}^*$ . En exploitant que  $\varphi$  est un morphisme de corps :

$$1 = \varphi(1) = \varphi\left(n \times \frac{1}{n}\right) = \varphi(n) \times \varphi\left(\frac{1}{n}\right) = n \times \varphi\left(\frac{1}{n}\right)$$

en utilisant que  $\varphi(n) = n$  puisque  $n \in \mathbb{Z}$ . On obtient  $\varphi\left(\frac{1}{n}\right) = \frac{1}{n}$ .

Soit enfin  $r$  un rationnel. Il existe  $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$  tels que  $r = \frac{p}{q}$ . Calculons :

$$\varphi(r) = \varphi\left(\frac{p}{q}\right) = \varphi\left(p \times \frac{1}{q}\right) = \varphi(p) \times \varphi\left(\frac{1}{q}\right) = p \times \frac{1}{q} = r.$$

Ainsi, pour  $x \in \mathbb{Q}(\sqrt{2})$  qu'on écrit  $x = a + b\sqrt{2}$  avec  $a, b \in \mathbb{Q}$ , nous obtenons (en utilisant encore et toujours que  $\varphi$  est un automorphisme de corps) :

$$\varphi(x) = \varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a + b\varphi(\sqrt{2}).$$

Connaitre l'automorphisme  $\varphi$  se ramène alors à déterminer  $\varphi(\sqrt{2})$ . Or :

$$\varphi(\sqrt{2})^2 = \varphi((\sqrt{2})^2) = \varphi(2) = 2.$$

$\varphi(\sqrt{2})$  est donc l'une des racines du polynôme  $X^2 - 2$ , à savoir  $\sqrt{2}$  ou  $-\sqrt{2}$ . Deux cas se présentent :

- si  $\varphi(\sqrt{2}) = \sqrt{2}$ , alors pour tout  $x \in \mathbb{Q}(\sqrt{2})$ , qu'on écrit  $x = a + b\sqrt{2}$  avec  $a, b \in \mathbb{Q}$  :

$$\varphi(x) = \varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a + b\sqrt{2} = x.$$

Dans ce cas,  $\varphi$  est l'application identité.

- si  $\varphi(\sqrt{2}) = -\sqrt{2}$ , alors avec les mêmes notations que précédemment, un calcul identique donne :

$$\varphi(x) = a - b\sqrt{2}.$$

- **Synthèse.** Réciproquement, vérifions que les deux applications ainsi obtenues sont bien des automorphismes du corps  $\mathbb{Q}(\sqrt{2})$ . C'est évident pour l'identité. Pour la

seconde, elle vérifie  $\varphi(1) = 1$  et est bijective puisque  $\varphi \circ \varphi = \text{id}$ . Pour tout  $(x, y) \in \mathbb{Q}(\sqrt{2})^2$ , qu'on écrit  $x = a + b\sqrt{2}$  et  $y = c + d\sqrt{2}$  avec  $a, b, c, d \in \mathbb{Q}$ , calculons :

$$x + y = (a + c) + (b + d)\sqrt{2} \quad \text{et} \quad x \times y = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

D'où :

$$\varphi(x + y) = (a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2}) = \varphi(x) + \varphi(y)$$

et :

$$\varphi(x \times y) = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2}) \times (c - d\sqrt{2}) = \varphi(x) \times \varphi(y).$$

Ainsi,  $\varphi$  est elle aussi un automorphisme du corps  $\mathbb{Q}(\sqrt{2})$ .

En conclusion, le corps  $\mathbb{Q}(\sqrt{2})$  comporte exactement deux automorphismes de corps, à savoir  $\text{id}_{\mathbb{Q}(\sqrt{2})}$  et l'application « conjugaison »  $\varphi$  :

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \rightarrow & \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} & \mapsto & a - b\sqrt{2} \end{array}.$$

### Exercice 19.26 (★★★★★ - Idéaux premiers (d'après oral ENS))

Soit  $A$  un anneau commutatif non nul. On appelle idéal de  $A$  tout sous-groupe  $I$  de  $(A, +)$  tel que  $\forall(a, x) \in A \times I, ax \in I$ .

1. Montrer que pour tout  $x \in A, xA = \{ax, a \in A\}$  est un idéal de  $A$ .
2. Un idéal  $I$  est dit *maximal* si tout idéal de  $A$ , différent de  $A$ , et qui contient  $I$  est égal à  $I$  lui-même.

Un idéal  $I$  différent de  $A$  est dit *premier* si :  $\forall(a, b) \in A^2, ab \in I \Rightarrow a \in I$  ou  $b \in I$ .

- (a) Montrer qu'un idéal  $I$  est maximal si, et seulement si, pour tout  $x \in A \setminus I, I + xA = A$  (où  $I + aA$  est l'ensemble des éléments qui s'écrivent comme somme d'un élément de  $I$  et d'un élément de  $aA$ ).
  - (b) Prouver qu'un idéal maximal est premier.
3. Montrer que  $A$  est un corps si, et seulement si, tout idéal de  $A$  autre que  $A$  est premier.

1. Soit  $x \in A$ . Vérifions en premier lieu que  $xA$  est un sous-groupe de  $(A, +)$  :

- (i)  $0_A = 0_A \times x$  appartient bien à  $xA$  ;
- (ii) Soient  $b_1, b_2 \in xA$ . Par définition, il existe  $a_1, a_2 \in A$  tels que  $b_i = a_i x$  pour  $i = 1, 2$ . Alors :

$$b_1 - b_2 = a_1 x - a_2 x = \underbrace{(a_1 - a_2)}_{\in A} \times x \in xA.$$

Donc  $xA$  est un sous-groupe de  $(A, +)$ . Pour montrer que c'est un idéal de  $(A, +)$ , on étudie le dernier point suivant :

- (iii) Soit  $b \in xA$  et  $c \in A$ . Par définition, il existe  $a \in A$  tel que  $b = ax$ . Alors :

$$c \times b = \underbrace{(c \times a)}_{\in A} \times x \in xA.$$

On dit alors que  $xA$  est *absorbant*.

Donc  $xA$  est bien un idéal de  $A$ .

**Remarque.** Donnons  $\{0_A\}$  et  $A$  comme autre exemple trivial d'idéaux de  $A$ .

2. (a) Supposons  $I$  maximal, et soit  $x \in A \setminus I$ . On vérifie (laissé en exercice) que  $I + xA$  est un idéal de  $A$  qui contient  $x$  et  $I$ . Il contient donc strictement  $I$  qui est maximal. Donc  $I + xA = A$ .

Réciproquement, supposons que  $I$  est un idéal de  $A$  satisfaisant, pour tout  $x \in A \setminus I$ ,  $I + xA = A$ . Montrons que  $I$  est maximal. Soit pour cela  $J$  un idéal de  $A$ , différent de  $A$ , et tel que  $I \subset J$ . Montrons que  $I = J$ . Par l'absurde, supposons que  $I \subsetneq J$ , et donc qu'il existe  $x \in J \setminus I$ . Puisque  $J$  est un idéal, on vérifie (laissé en exercice – on utilise que  $J$  est un idéal), que  $J$  contient  $I + xA = A$ . Ce qui contredit  $J \neq A$ . Ainsi,  $J = I$  et  $I$  est un idéal maximal.

- (b) Soit  $I$  un idéal maximal différent de  $A$ . Montrons que  $I$  est premier. Soient pour cela  $a, b \in A$  tels que  $ab \in I$ . Supposons que  $a \notin I$  et montrons que  $b \in I$ .

Par la question précédente,  $I + aA = A$ . En particulier,  $1_A$  appartient à  $I + aA$ , et il existe  $x \in I$ ,  $y \in A$  tels que :

$$1_A = x + ay.$$

D'où en multipliant cette égalité par  $b$  :

$$b = b \underbrace{x}_{\in I} + \underbrace{ab}_{\in I} y \in I$$

car  $I$  est un idéal.

Ainsi,  $I$  est bien un idéal premier de  $A$ .

3. Supposons que  $A$  soit un corps, et soit  $I$  un idéal de  $A$ . Si  $I = \{0_A\}$ , alors  $I$  est premier car  $A$  est non nul et intègre. Supposons  $I \neq \{0_A\}$ . Alors  $I$  contient un élément non nul  $x$ . Mais alors  $1_A = x \times x^{-1} \in I$ , et pour tout  $a \in A$ ,  $a = a \times 1_A \in I$ . Ainsi,  $I = A$  et donc tout idéal de  $A$ , différent de  $A$ , est bien premier.

Réciproquement, supposons que tout idéal de  $A$  autre que  $A$  est premier. En particulier,  $I = \{0_A\}$  est un idéal premier, de sorte que  $A$  est intègre.

Soit  $a \in A$  non nul. Montrons que  $a$  est inversible. Considérons pour cela l'idéal  $a^2A$ . Deux cas se présentent :

- si  $a^2A = A$ , alors en particulier  $1_A \in a^2A$ , et il existe  $b \in A$  tel que :

$$1_A = a^2b = a(ab).$$

Dans ce cas,  $a$  est bien inversible (d'inverse  $ab$ ).

- si  $a^2A$  est différent de  $A$ , alors c'est un idéal premier par hypothèse. Puisque  $a \times a = a^2 \times 1_A \in a^2A$ ,  $a^2A$  contient  $a$ , et il existe  $b \in A$  tel que :

$$a = a^2b, \quad \text{d'où} \quad a(1_A - ab) = 0_A.$$

Et  $A$  étant intègre et  $a$  non nul, on obtient  $1_A = ab$ , et donc  $a$  est inversible.

Dans tous les cas,  $a$  est bien inversible. Donc  $A$  est un corps.

---