Quelques classiques d'algèbre générale

On portera une attention particulière à **la rédaction** et à **la propreté** de la copie.
En particulier tout **graphe ou schéma** pertinent et correctement annoté sera **valorisé**.
Les résultats devront être mis en valeur dès que possible.

Indiquez sur votre copie le temps approximatif pris pour le devoir.

Contexte

Ce devoir est une introduction à plusieurs notions classiques d'algèbre générale, essentielles pour pouvoir comprendre les structures algébriques qui seront étudiées cette année et l'année prochaine.
À l'exception de la partie 1, les parties sont indépendantes entre elles.

- La partie 1 montre que tout sous-groupe additif de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$ pour un unique $d \in \mathbb{N}$. Ce résultat (qui fera partie du cours d'arithmétique) pourra être utilisé dans les autres parties.
- La partie 2 introduit la notion d'**ordre** d'un élément d'un groupe et étudie quelques propriétés de l'ordre dans les groupes abéliens finis.
- La partie 3 introduit la notion d'élément **nilpotent** dans un anneau et étudie quelques propriétés de ces éléments.
- La partie 4 introduit la notion de **caractéristique**.
- Enfin la partie 5 démontre le théorème de Lagrange, affirmant que le cardinal d'un sous-groupe divise toujours le cardinal du groupe (dans le cas où le groupe est fini).

$$x^n = e_G$$
$$x^n = 0_A$$
$$n1_{\mathbb{K}} = 0_{\mathbb{K}}$$

Rappel des notations

- Étant donnés $a, b \in \mathbb{Z}$, $a \wedge b$ désigne le Plus Grand Diviseur Commun de a et b et $a \vee b$ désigne le Plus Petit Commun Multiple de a et b.
- Étant donné un élément x d'un groupe $(G, \cdot)$ et $n \in \mathbb{Z}$, l'expression x^n est définie par la récurrence
  ▷ $x^0 = e_G$,
  ▷ $\forall n \in \mathbb{N}, x^{n+1} = x \cdot x^n$,
  et par
  ▷ $\forall n \in \mathbb{Z}\backslash\mathbb{N}, x^n = (x^{-n})^{-1}$.
  Par exemple on a $x^4 = \underbrace{x \cdot x \cdot x \cdot x}_{4 \text{ fois}}$ et $x^{-3} = \underbrace{(x \cdot x \cdot x)}_{3 \text{ fois}}^{-1}$.
  Les règles usuelles des puissances sont connues et il n'est pas demandé de les redémontrer.
  Dans le cas d'un groupe $(G, +)$ noté *additivement*, on note nx pour x^n.
  Par exemple on a $4x = \underbrace{x + x + x + x}_{4 \text{ fois}}$ et $-3x = -\underbrace{(x + x + x)}_{3 \text{ fois}}$.

---

1. ♣ Sous-groupes additifs de $\mathbb{Z}$

1.1. Soit $d \in \mathbb{N}$. Montrer que $d\mathbb{Z}$ est un sous-groupe additif de $(\mathbb{Z}, +)$.
1.2. Soit H un sous-groupe additif de $(\mathbb{Z}, +)$. Montrer qu'il existe un et unique $d \in \mathbb{N}$ tel que $H = d\mathbb{Z}$.
1.3. Quels sont les idéaux de l'anneau $(\mathbb{Z}, +, \times)$?

---

2. Ordre d'un élément dans un groupe

Dans toute cette partie $(G, \cdot)$ est un groupe.

2.I. Ordre d'un élément

Soit $x \in G$.
2.1. Montrer que

$$\Phi : \begin{array}{c} \mathbb{Z} \to G \\ n \mapsto x^n \end{array}$$

est un morphisme de groupes.

2.2. Montrer que

$$\langle x\rangle = \{x^n, n \in \mathbb{Z}\}$$

est un sous-groupe de G contenant x.
Montrer que pour tout sous-groupe H de G contenant x, on a $\langle x\rangle \subset H$.
Le sous-groupe $\langle x\rangle$ est appelé sous-groupe engendré par x.

2.3. Montrer qu'il existe un et unique $d \in \mathbb{N}$ tel que

$$\mathrm{Ker}(\Phi) = d\mathbb{Z}.$$

Montrer que pour tout $n \in \mathbb{Z}$ on a

$$x^n = e_G \ \Leftrightarrow\ d|n.$$

2.4. Soit $d \in \mathbb{N}$ défini à la question **2.3.**.
Montrer que si $d = 0$ alors $\langle x\rangle$ est isomorphe à $\mathbb{Z}$.
On en déduit en particulier que $\langle x\rangle$ est infini.

2.5. Soit $d \in \mathbb{N}$ défini à la question **2.3.**.
Montrer que si $d \neq 0$ alors $\langle x\rangle$ est isomorphe à $\mathbb{U}_d$.
On en déduit en particulier que $\langle x\rangle$ a exactement d éléments.

Dans la suite, si $d \neq 0$ on dit que x est d'ordre d (et on appelle d l'ordre de x). Si $d = 0$, on dit que x est d'ordre infini.

2.II. Cas des groupes abéliens finis

On suppose désormais que G est **finie**.

2.6. Montrer que pour tout $x \in G$, x est d'ordre fini.

On note dans la suite, pour tout $x \in G$, $\mathrm{ord}(x) \in \mathbb{N}$ l'ordre de x.

2.7. En utilisant le résultat de la partie 5, montrer que pour tout $x \in G$, $\mathrm{ord}(x)|\,\mathrm{card}(G)$.

On suppose de plus dans la suite que G est **abélien**.

On cherche tout d'abord à retrouver le résultat de la question **2.7.** sans utiliser la partie 5.

2.8. Soit $x \in G$.
Montrer que

$$\tau_x : \begin{array}{c} G \to G \\ g \mapsto gx \end{array}$$

est bijective.

2.9. À l'aide de la question précédente, montrer que

$$\prod_{g\in G} g = \prod_{g\in G} (gx)$$

2.10. En déduire que

$$\mathrm{ord}(x)|\,\mathrm{card}(G).$$

On s'intéresse désormais au lien entre ordre et produit.

2.11. Soient $x, y \in G$.
Montrer que

$$\mathrm{ord}(x) \wedge \mathrm{ord}(y) = 1 \Rightarrow \mathrm{ord}(xy) = \mathrm{ord}(x)\,\mathrm{ord}(y).$$

2.12. Donner un exemple de groupe abélien fini G, et d'éléments $x, y \in G$ tels que $\mathrm{ord}(xy) \neq \mathrm{ord}(x) \times \mathrm{ord}(y)$ et tels que $\mathrm{ord}(xy) \neq \mathrm{ord}(x) \vee \mathrm{ord}(y)$.

2.13. Soient $a, b \in \mathbb{Z}$.
Montrer qu'il existe $\widetilde{a}$ et $\widetilde{b}$ tels que

$$\begin{cases} \widetilde{a}|a \\ \widetilde{b}|b \\ \widetilde{a} \wedge \widetilde{b} = 1 \\ \widetilde{a} \times \widetilde{b} = a \vee b \end{cases}$$

2.14. En déduire que pour tous $a, b \in \mathbb{N}^*$,

$$\big(\exists (x,y)\in G^2, \mathrm{ord}(x)=a \text{ et } \mathrm{ord}(y)=b\big) \Rightarrow (\exists z\in G, \mathrm{ord}(z)=a\vee b)\,.$$

3. Un peu d'éléments nilpotents

Dans cette partie $(A,+,\cdot)$ est un anneau.
On dit que $x\in A$ est *nilpotent* s'il existe un entier $n\in\mathbb{N}$ tel que $x^n=0_A$.

3.I. Premiers exemples

3.1. Un élément nilpotent peut-il être régulier ?
3.2. On considère dans cette question $A=\mathcal{M}_2(\mathbb{R})$.
On note $E_{12}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ et $E_{21}=\begin{pmatrix}0&0\\1&0\end{pmatrix}$.
Montrer que
- E_{12} et E_{21} sont nilpotents.
- $E_{12}E_{21}$ n'est pas nilpotent.
- $E_{12}+E_{21}$ n'est pas nilpotent.

3.II. Ordre de nilpotence

3.3. Soit $x\in A$ nilpotent.
Montrer qu'il existe $n_0\in\mathbb{N}$ tel que

$$\forall n\in\mathbb{N}, x^n=0_A \Leftrightarrow n\geq n_0.$$

On dit alors que x est nilpotent d'ordre n_0 (et on appelle n_0 l'ordre de nilpotence de x ou encore nilindice de x).

3.III. Exemples de calculs

3.4. Soit $x\in A$ nilpotent et $y\in A$ quelconque qui **commute** avec x.
Montrer que xy est nilpotent.
3.5. Soient $x,y\in A$ tels que xy est nilpotent.
Montrer que yx est nilpotent.
3.6. Soient $x,y\in A$ nilpotents qui **commutent**.
Montrer que $x+y$ est nilpotent.
3.7. Soit $x\in A$ nilpotent.
Montrer que $1-x$ est inversible et expliciter son inverse.
3.8. Soit $u\in A$ inversible et $n\in A$ nilpotent qui **commutent**.
Montrer que $u+n$ est inversible et expliciter son inverse.

4. Caractéristique d'un corps

Dans toute cette partie $(\mathbb{K},+,\cdot)$ est un corps.
4.1. Montrer que

$$\Phi:\begin{array}{l}\mathbb{Z}\to\mathbb{K}\\ n\mapsto n1_{\mathbb{K}}\end{array}$$

est un morphisme d'anneau.
4.2. Montrer qu'il existe un unique $p\in\mathbb{N}$ tel que

$$\mathrm{Ker}(\Phi)=p\mathbb{Z}.$$

4.3. Montrer que $p=0$ ou p est premier.
On dit alors que $\mathbb{K}$ est de caractéristique p.

---

5. Théorème de Lagrange

Soit $(G,\cdot)$ un groupe **fini**.
On souhaite démontrer le résultat suivant (théorème de Lagrange):
Pour tout sous-groupe H de G, on a

$$\text{card}(H) | \text{card}(G).$$

5.I. Classes d'équivalences à gauche

Soit H un sous-groupe de G.
On définit une relation $\mathcal{R}_H$ sur G par

$$\forall (x_1, x_2) \in G^2,\ x_1 \mathcal{R}_H x_2 \Leftrightarrow x_1 {x_2}^{-1} \in H.$$

5.1. Montrer que $\mathcal{R}_H$ est une relation d'équivalence.
5.2. Soit $x \in G$. Montrer que la classe d'équivalence de x est

$$Hx = \{hx, h \in H\}.$$

5.3. Soient $x_1, x_2 \in H$. Expliciter une bijection de Hx_1 vers Hx_2.

5.II. Théorème de Lagrange

Soit H un sous-groupe de G.
5.4. À l'aide de la sous-partie 5.I montrer que

$$\text{card}(H) | \text{card}(G).$$

5.III. Applications

5.5. Faire la question **2.7.** de la partie 2.
5.6. Soit G un groupe fini.
On suppose que $p = \text{card}(G)$ est un nombre premier.
Montrer que G est isomorphe à $\mathbb{U}_p$.
5.7. Soit $n \in \mathbb{N}^*$ un entier.
On note

$$\varphi(n) = \text{card}\left(\{k \in [\![0, n-1]\!] \mid k \wedge n = 1\}\right)$$

le nombre de nombres entre 0 et $n-1$ et premiers avec n.
Montrer que pour tout $a \in \mathbb{Z}$ tel que $a \wedge n = 1$ on a

$$a^{\varphi(n)} \equiv 1[n].$$