En cas d'erreur de corrigé, n'hésitez pas à me le signaler.

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 $(\mathbb{Z}, +)$.

On a
- $0 = d \times 0 \in d\mathbb{Z}$,
- Soient $a_1, a_2 \in d\mathbb{Z}$.
  Il existe $k_1, k_2 \in \mathbb{Z}$ tels que $a_1 = dk_1$ et $a_2 = dk_2$.
  On a $a_1 + a_2 = dk_1 + dk_2 = d(k_1 + k_2) \in d\mathbb{Z}$.
  D'où la stabilité par somme.
- Soit $a \in d\mathbb{Z}$.
  Il existe $k \in \mathbb{Z}$ tel que $a = dk$.
  On a $-a = -dk = d(-k) \in d\mathbb{Z}$.
  D'où la stabilité par opposé.

Par conséquent $\boxed{d\mathbb{Z} \text{ est un sous-groupe de } (\mathbb{Z}, +)}$.

1.2. Soit H un sous-groupe additif de $(\mathbb{Z}, +)$. Montrer qu'il existe un et unique $d \in \mathbb{N}$ tel que $H = d\mathbb{Z}$.

Si $H = \{0\}$, on a $H = 0\mathbb{Z}$.
Sinon il existe $x \in H\backslash\{0\}$.
Alors comme $x \in H$ et $-x \in H$ et $x > 0$ ou $-x > 0$, on a $H \cap \mathbb{N}^* \neq \emptyset$.
Comme toute partie non vide de $\mathbb{N}$ admet un plus petit élément, on peut définir

$$d = \min\left(H \cap \mathbb{N}^*\right).$$

Montrons par double-inclusion que $H = d\mathbb{Z}$.
- Comme $d \in H$ et H stable par somme et opposé, on a $d\mathbb{Z} \subset H$.
- Soit $a \in H$, on considère la division euclidienne de a par d.
  Il existe $q, r \in \mathbb{Z}$ tels que

$$a = dq + r$$

avec

$$0 \leq r < d.$$

Alors comme $d\mathbb{Z} \subset H$, on a $dq \in H$.
Donc $dq \in H$ et $a \in H$ donc $r = a - dq \in H$.
Comme $r \in \mathbb{N}$ et $r < d = \min(H \cap \mathbb{N}^*)$ on a donc $r = 0$.
Donc $a = dq$ et $a \in d\mathbb{Z}$.

On a donc bien $\boxed{H = d\mathbb{Z}}$.
Enfin pour l'unicité, soient $d_1, d_2 \in \mathbb{N}$ tels que $d_1\mathbb{Z} = d_2\mathbb{Z}$.
Comme $d_1 \in d_2\mathbb{Z}$ on a $d_2 | d_1$.
De même $d_2 \in d_1\mathbb{Z}$ donc $d_1 | d_2$.
Donc $d_1 = \pm d_2$. Comme $d_1, d_2 \in \mathbb{N}$ on a $d_1 = d_2$.
D'où $\boxed{\text{l'unicité}}$.

1.3. Quels sont les idéaux de l'anneau $(\mathbb{Z}, +, \times)$?

Soit I un idéal de $(\mathbb{Z}, +, \times)$.
En particulier I est un sous-groupe additif de $(\mathbb{Z}, +)$.
Donc par la question précédente, il existe $d \in \mathbb{N}$ tel que $I = d\mathbb{Z}$.
De plus soit $d \in \mathbb{N}$.
Soit $a \in d\mathbb{Z}$ et $b \in \mathbb{Z}$.
Il existe $k \in \mathbb{Z}$ tel que $a = dk$.
On a $ab = dkb = d(bk) \in d\mathbb{Z}$.
Donc $d\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.
Par conséquent $\boxed{\text{les idéaux de } (\mathbb{Z}, +, \times) \text{ sont les } d\mathbb{Z} \text{ pour } d \in \mathbb{N}}$.

---

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.

Soient $n_1, n_2 \in \mathbb{Z}$.
On a

$$\Phi(n_1 + n_2) = x^{n_1+n_2} = x^{n_1} \cdot x^{n_2} = \Phi(n_1) \cdot \Phi(n_2).$$

Donc $\boxed{\Phi \text{ est un morphisme de groupes}}$.

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.

On a $x = x^1 \in \langle x \rangle$. Donc $\boxed{x \in \langle x \rangle}$.
Comme $\langle x \rangle = \mathrm{Im}(\Phi)$, c'est en particulier $\boxed{\text{un sous-groupe de } G}$.
Soit H un sous-groupe de G contenant x.
Alors comme H est stable par produit et inverse on a pour tout $n \in \mathbb{Z}$, $x^n \in H$.
D'où $\boxed{\langle x \rangle \subset H}$.

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

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

On a $\mathrm{Ker}(\Phi)$ est un sous-groupe de $\mathbb{Z}$.
Par la partie 1 il existe un et unique $d \in \mathbb{N}$ tel que

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

Par définition du noyau et de $d\mathbb{Z}$, on a pour tout $n \in \mathbb{Z}$, $x^n = e_G$ ssi $n \in \mathrm{Ker}(\Phi)$ ssi $n \in d\mathbb{Z}$ ssi $d|n$.
Et donc $\boxed{x^n = e_G \text{ ssi } d|n}$.

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.

Si $d = 0$, on a $\mathrm{Ker}(\Phi) = 0\mathbb{Z} = \{0\}$.
Donc Φ est injective.
Ainsi $\Phi^{|\mathrm{Im}(\Phi)}$ est un isomorphisme.
Donc $\mathrm{Im}(\Phi) = \langle x \rangle$ est isomorphe à $\mathbb{Z}$.
Donc $\boxed{\langle x \rangle \text{ est isomorphe à } \mathbb{Z}}$.

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.

Par définition du noyau on a pour tous $n_1, n_2 \in \mathbb{Z}$, $x^{n_1} = x^{n_2}$ ssi $x^{n_1 - n_2} = e_G$ ssi $d|n_1 - n_2$ ssi $n_1 \equiv n_2[d]$.
Soit $\omega \in \mathbb{U}_d$.
Il existe $n \in \mathbb{N}$ tel que $\omega = e^{\frac{2i\pi n}{d}}$.
De plus étant donnés $n_1, n_2 \in \mathbb{Z}$, on a $e^{\frac{2i\pi n_1}{d}} = e^{\frac{2i\pi n_2}{d}}$ ssi $\frac{2\pi n_1}{d} \equiv \frac{2\pi n_2}{d}[2\pi]$ ssi $n_1 \equiv n_2[d]$, et dans ce cas $x^{n_1} = x^{n_2}$ d'après ce qui précède.
Ainsi x^n ne dépend pas de n mais seulement de ω.
On peut donc poser $\phi(\omega) = x^n$.
La fonction $\phi : \mathbb{U}_d \to \langle x \rangle$ est $\boxed{\text{bien définie}}$.
Remarque: il y a plusieurs façons de rédiger ce morphisme (par exemple en passant par $\mathbb{Z}/d\mathbb{Z}$), le point essentiel est de vérifier que l'écriture est bien définie, c'est à dire ici qu'elle ne dépend pas du choix de représentant.
Vérifions que ϕ est un isomorphisme.
Soient $\omega_1, \omega_2 \in \mathbb{U}_d$.
Il existe $n_1, n_2 \in \mathbb{N}$ tels que $\omega_1 = e^{\frac{2i\pi n_1}{d}}$ et $\omega_2 = e^{\frac{2i\pi n_2}{d}}$.
Alors

$$\begin{aligned}\phi(\omega_1\omega_2) &= \phi\left(e^{\frac{2i\pi(n_1+n_2)}{d}}\right)\\ &= x^{n_1+n_2}\\ &= x^{n_1}x^{n_2}\\ &= \phi(\omega_1)\phi(\omega_2).\end{aligned}$$

et donc ϕ est un morphisme de groupes.
De plus pour tout $\omega \in \mathbb{U}_d$, avec $n \in \mathbb{N}$ tel que $\omega = e^{\frac{2i\pi n}{d}}$, on a $\phi(\omega) = e_G$ ssi $x^n = e_G$ ssi $d|n$ ssi $\omega = 1$.
Donc ϕ est injective.
Et enfin soit $y \in \langle x \rangle$.
Il existe $n \in \mathbb{Z}$ tel que $y = x^n$.

Alors avec $\omega = e^{\frac{2i\pi n}{d}}$, on a $\phi(\omega) = x^n = y$ et donc ϕ est surjective.
Donc $\boxed{\phi : \mathbb{U}_d \to \langle x \rangle \text{ est un isomorphisme}}$.

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 **fini**.

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

Soit $x \in G$.
Supposons par l'absurde que x n'est pas d'ordre fini. Alors par la question **2.4.**, $\langle x \rangle$ est infini. Et comme $\langle x \rangle \subset G$ on en déduit G est infini. Ce qui est absurde.
D'où $\boxed{x \text{ est d'ordre fini}}$.

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

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

D'après le théorème de Lagrange (partie 5) le cardinal de tout sous-groupe divise le cardinal du groupe.
Comme $\langle x \rangle$ est un sous-groupe de G (comme image d'un morphisme de groupe) on en déduit que $\boxed{\text{ord}(x) | \text{card}(G)}$.

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.

Posons

$$\tau_{x^{-1}} : \begin{array}{c} G \to G \\ g \mapsto gx^{-1}. \end{array}$$

Alors pour tout $g \in G$ on a

$$(\tau_x \circ \tau_{x^{-1}})(g) = (gx^{-1})x = g$$

et de même

$$(\tau_{x^{-1}} \circ \tau_x)(g) = (gx)x^{-1} = g.$$

On a donc

$$\tau_x \circ \tau_{x^{-1}} = \text{Id}_G$$
$$\tau_{x^{-1}} \circ \tau_x = \text{Id}_G$$

et donc en particulier $\boxed{\tau_x \text{ est bijective}}$ (et de bijection réciproque $\tau_{x^{-1}}$).

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

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

Comme $\tau_x : G \to G$ est bijective, on a par changement d'indice ($h = gx$)

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

C'est à dire

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

2.10. En déduire que

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

On a aussi (le groupe est abélien)

$$\prod_{g\in G}(gx) = \left(\prod_{g\in G} g\right) \times \left(\prod_{g\in G} x\right) = x^{\operatorname{card}(G)} \prod_{g\in G} g.$$

Par conséquent on a

$$x^{\operatorname{card}(G)} \prod_{g\in G} g = \prod_{g\in G} g$$

et donc (tout élément d'un groupe est simplifiable car inversible)

$$x^{\operatorname{card}(G)} = 1_G.$$

On conclut alors (définition de l'ordre)

$$\boxed{\operatorname{ord}(x) | \operatorname{card}(G)}.$$

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

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

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

Supposons $\operatorname{ord}(x) \wedge \operatorname{ord}(y) = 1$.
Comme les ordres sont des entiers naturels pour montrer l'égalité on peut procéder par «double divisiblité».

- Comme G est abélien, on a

$$\begin{aligned}(xy)^{\operatorname{ord}(x)\operatorname{ord}(y)} &= x^{\operatorname{ord}(x)\operatorname{ord}(y)} y^{\operatorname{ord}(x)\operatorname{ord}(y)} \\ &= \left(x^{\operatorname{ord}(x)}\right)^{\operatorname{ord}(y)} \left(y^{\operatorname{ord}(y)}\right)^{\operatorname{ord}(x)} \\ &= 1_G^{\operatorname{ord}(y)} 1_G^{\operatorname{ord}(x)} \\ &, = 1_G\end{aligned}$$

  et donc par la définition de l'ordre on en déduit que

$$\boxed{\operatorname{ord}(xy) | \operatorname{ord}(x)\operatorname{ord}(y)}.$$

- On a $(xy)^{\operatorname{ord}(xy)} = 1_G$ et donc en particulier

$$(xy)^{\operatorname{ord}(xy)\operatorname{ord}(x)} = 1_G^{\operatorname{ord}(x)} = 1_G.$$

  Comme G est abélien on a donc

$$\left(x^{\operatorname{ord}(x)}\right)^{\operatorname{ord}(xy)} y^{\operatorname{ord}(x)\operatorname{ord}(xy)} = 1_G$$

  c'est à dire, comme $x^{\operatorname{ord}(x)} = 1_G$,

$$y^{\operatorname{ord}(x)\operatorname{ord}(xy)} = 1_G.$$

  Donc par la définition de l'ordre

$$\operatorname{ord}(y) | \operatorname{ord}(x)\operatorname{ord}(xy)$$

  et comme $\operatorname{ord}(x)$ et $\operatorname{ord}(y)$ sont premiers entre eux par le lemme de Gauss on déduit que

$$\operatorname{ord}(y) | \operatorname{ord}(xy).$$

  De même par symétrie on a

$$\operatorname{ord}(x) | \operatorname{ord}(xy).$$

  Et comme $\operatorname{ord}(x)$ et $\operatorname{ord}(y)$ sont premiers entre eux, on peut donc conclure que

$$\boxed{\operatorname{ord}(x)\operatorname{ord}(y) | \operatorname{ord}(xy)}.$$

On a donc bien montré

$$\boxed{\operatorname{ord}(x) \wedge \operatorname{ord}(y) = 1 \Rightarrow \operatorname{ord}(xy) = \operatorname{ord}(x)\operatorname{ord}(y)}.$$

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

$\text{ord}(xy) \neq \text{ord}(x) \vee \text{ord}(y)$.

Par exemple avec $G = \mathbb{U}_4$ on a $\text{ord}(i) = 4$ et $\text{ord}(i) = 4$.
Mais $\boxed{\text{ord}(i \times i) = 2,\ ord(i) \times \text{ord}(i) = 16,\ \text{ord}(i) \vee \text{ord}(i) = 4}$.

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

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

Pour tout nombre premier p on pose

$$m_p = \begin{cases} \nu_p(a) & \text{si } \nu_p(a) \geq \nu_p(b) \\ 0 & \text{si } \nu_p(a) < \nu_p(b) \end{cases}$$

$$n_p = \begin{cases} 0 & \text{si } \nu_p(a) \geq \nu_p(b) \\ \nu_p(b) & \text{si } \nu_p(a) < \nu_p(b) \end{cases}$$

et

$$\widetilde{a} = \prod_{p \text{ premier}} p^{m_p}$$

$$\widetilde{b} = \prod_{p \text{ premier}} p^{n_p}$$

qui sont bien définis (car m_p et n_p tous nuls sauf un nombre fini).
On a alors pour tout nombre premier p, par disjonction de cas,

$$\begin{aligned} \nu_p(\widetilde{a}) &\leq \nu_p(a) \\ \nu_p(\widetilde{b}) &\leq \nu_p(b) \\ \min\left(\nu_p(\widetilde{a}), \nu_p(\widetilde{b})\right) &= 0 \\ \nu_p(\widetilde{a}) + \nu_p(\widetilde{b}) &= \max(\nu_p(a), \nu_p(b)) \end{aligned}$$

et donc $\widetilde{a}$ et $\widetilde{b}$ conviennent.
Remarque: ce n'est évidemment pas la seule façon de procéder, on peut aussi construire par récurrence un tel élément, facteur premier par facteur premier ou bien tout simplement poser

$$\widetilde{a} = a//(a \wedge b)$$

$$\widetilde{b} = b//(a \wedge b)$$

et utiliser ensuite les règles de calcul du pgcd et du ppcm.

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

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

Supposons qu'il existe x et y des éléments d'ordres respectifs a et b. Fixons les.
Fixons alors $\widetilde{a}$ et $\widetilde{b}$ des éléments comme à la question **2.13.**
Alors avec $a = q_a\widetilde{a}$ on a x^{q_a} est d'ordre $\widetilde{a}$.
En effet pour tout $n \in \mathbb{Z}$ on a les équivalences

$$\begin{aligned} (x^{q_a})^n = 1_G &\Leftrightarrow x^{q_a n} = 1 \\ &\Leftrightarrow a | q_a n \\ &\Leftrightarrow q_a\widetilde{a} | q_a n \\ &\Leftrightarrow \widetilde{a} | n \end{aligned}$$

et donc par la définition de l'ordre on a donc $\text{ord}\left(x^{q_a}\right) | \widetilde{a}$ et $\widetilde{a} | \text{ord}\left(x^{q_a}\right)$ d'où le résultat.
De même avec $b = q_b\widetilde{b}$ on a y^{q_b} est d'ordre $\widetilde{b}$.
Comme $\widetilde{a}$ et $\widetilde{b}$ sont premiers entre eux par la question **2.11.** on en déduit que $x^{q_a}y^{q_b}$ est d'ordre $\widetilde{a}\widetilde{b}$ et donc en particulier $\boxed{\text{il existe un élément d'ordre } a \vee b}$.

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 $x^n = 0_A$.

Dans la suite on suppose $0_A \neq 1_a$.
En particulier on a pour tout $x \in A$, $x^0 = 1_A \neq 0_A$.

3.I. Premiers exemples

3.1. Un élément nilpotent peut-il être régulier ?

Un élément nilpotent est diviseur de zéro et donc ne peut pas être régulier.
Plus précisément supposons par l'absurde que x est régulier.
Avec $n \in \mathbb{N}^*$ tel $x^n = 0_A$ on a $x^{n-1}x = x^{n-1}0_A$ d'où $x = 0_A$ ce qui est absurde.

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.

On a

$$E_{12}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

et donc E_{12} est nilpotent.
De plus on a

$$E_{12}E_{21} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

et pour tout $n \in \mathbb{N}$, on a

$$(E_{12}E_{21})^n = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

et donc $E_{12}E_{21}$ n'est pas nilpotent.
Enfin on a

$$(E_{12} + E_{21}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

qui est inversible (car $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$) et donc $E_{12} + E_{21}$ 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

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

Comme x est nilpotent l'ensemble

$$\{n \in \mathbb{N} \mid x^n = 0_A\}$$

est une partie non vide de $\mathbb{N}$.
Posons

$$n_0 = \min\{n \in \mathbb{N} \mid x^n = 0_A\}.$$

Soit $n \in \mathbb{N}$,
- si $x^n = 0_A$, comme le minimum est un minorant, alors $n_0 \leq n$,
- si $n \geq n_0$ alors $x^n = x^{n-n_0}x^{n_0}$ et comme le minimum est dans l'ensemble, on a $x^{n_0} = 0_A$ et donc $x^n = 0_A$.

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

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.

Soient $n \in \mathbb{N}$ tels que $x^n = 0_A$.
Alors comme x **et** y **commutent**, on a

$$(xy)^n = x^n y^n = 0_A y^n = 0_A$$

Et donc $\boxed{xy \text{ est nilpotent}}$.

3.5. Soient $x, y \in A$ tels que xy est nilpotent.
Montrer que yx est nilpotent.

Soit $n \in \mathbb{N}$ tel que $(xy)^n = 0_A$.
Alors

$$(yx)^{n+1} = y(xy)^n x = y0_A x = 0_A$$

et donc $\boxed{yx \text{ est nilpotent}}$.

3.6. Soient $x, y \in A$ nilpotents qui **commutent**.
Montrer que $x + y$ est nilpotent.

Soient $n_x, n_y \in \mathbb{N}^*$ tels que $x^{n_x} = 0_A$ et $y^{n_y} = 0_A$.
Alors avec $N = n_x + n_y - 1$ on a comme x **et** y **commutent**, par la formule du binôme, en constatant de plus que pour tout $k \in [\![0, n_x - 1]\!]$, $N - k = n_y + (n_x - 1 - k) \geq n_y$, donc $y^{N-k} = 0_A$,

$$\begin{aligned}(x+y)^N &= \sum_{k=0}^{N} \binom{N}{k} x^k y^{N-k} \\ &= \sum_{k=0}^{n_x-1} \binom{N}{k} x^k \underbrace{y^{N-k}}_{=0_A} + \sum_{k=n_x}^{N} \binom{N}{k} \underbrace{x^k}_{=0_A} y^{N-k} \\ &= 0_A\end{aligned}$$

et donc $\boxed{x + y \text{ est nilpotent}}$.

3.7. Soit $x \in A$ nilpotent.
Montrer que $1 - x$ est inversible et expliciter son inverse.

Soit $n \in \mathbb{N}^*$ tel que $x^n = 0_A$.
Par la formule de Bernoulli comme 1_A et x **commutent**, on a

$$\begin{aligned}1_A^n - x^n &= (1_A - x)\left(\sum_{k=0}^{n-1} 1_A^{n-1-k} x^k\right) \\ &= \left(\sum_{k=0}^{n-1} 1_A^{n-1-k} x^k\right)(1_A - x)\end{aligned}$$

et comme $1_A^n - x^n = 1_A - 0_A = 1_A$ on a donc $\boxed{1 - x \text{ est inversible}}$ et son inverse est

$$\boxed{(1_A - x)^{-1} = \sum_{k=0}^{n-1} x^k}.$$

3.8. Soit $u \in A$ inversible et $n \in A$ nilpotent qui **commutent**.
Montrer que $u+n$ est inversible et expliciter son inverse.

Comme u et n **commutent**, et que u est inversible on a

$$u+n = u\left(1_A - (-u^{-1}n)\right).$$

De plus comme u^{-1} et n commutent et n est nilpotent on a $-u^{-1}n$ est nilpotent, d'indice de nilpotence m.
Par la question précédente on a donc $\boxed{u+n \text{ est inversible}}$ et son inverse est

$$\boxed{(u+n)^{-1} = \left(\sum_{k=0}^{m-1}(-u^{-1}n)^k\right)u^{-1}}.$$

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.

On a
- Pour tous $n_1, n_2 \in \mathbb{Z}$, $\Phi(n_1+n_2) = (n_1+n_2)1_{\mathbb{K}} = n_1 1_{\mathbb{K}} + n_2 1_{\mathbb{K}} = \Phi(n_1) + \Phi(n_2)$.
- Pour tous $n_1, n_2 \in \mathbb{Z}$, $\Phi(n_1 n_2) = (n_1 n_2)1_{\mathbb{K}} = (n_1 1_{\mathbb{K}})(n_2 1_{\mathbb{K}}) = \Phi(n_1)\Phi(n_2)$.
- $\Phi(1) = 1 1_{\mathbb{K}} = 1_{\mathbb{K}}$.

Donc $\boxed{\Phi \text{ est un morphisme d'anneau}}$.

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

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

Comme Φ est un morphisme d'anneaux, on a $\mathrm{Ker}(\Phi)$ est un idéal de $(\mathbb{Z}, +)$.
Par la partie 1 $\boxed{\text{il existe un unique } p \in \mathbb{N} \text{ tel que } \mathrm{Ker}(\Phi) = p\mathbb{Z}}$.

4.3. Montrer que $p = 0$ ou p est premier.

Supposons $p \neq 0$.
Soient $a, b \in \mathbb{N}$ tels que $p = ab$.
Alors, comme $p \in \mathrm{Ker}(\Phi)$, on a $0_{\mathbb{K}} = \Phi(p) = \Phi(ab) = \Phi(a)\Phi(b) = (a1_{\mathbb{K}})(b1_{\mathbb{K}})$.
Comme tout corps est intègre on a donc $a1_{\mathbb{K}} = 0_{\mathbb{K}}$ ou $b1_{\mathbb{K}} = 0_{\mathbb{K}}$, c'est à dire par définition du noyau $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$.
On a donc montré que si $p = ab$ alors $p|a$ ou $p|b$ et donc $\boxed{p \text{ est premier}}$.

On dit alors que $\underline{\mathbb{K} \text{ est de caractéristique } p}$.

---

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

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

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.

On observe que chaque item de la définition d'une relation d'équivalence est vérifié par un item de la définition de sous-groupe.
- **Réflexivité**:
  Soit $x \in G$.
  On a par **non vacuité** de H, $e_G \in H$ et de plus $xx^{-1} = e_G H$ donc $x\mathcal{R}_H x$.
- **Transitivité**
  Soient $x_1, x_2, x_3 \in G$ tels que $x_1\mathcal{R}_H x_2$ et $x_2\mathcal{R}_H x_3$.
  C'est à dire $x_1 x_2^{-1} \in H$ et $x_2 x_3^{-1} \in H$.
  Comme H est **stable par produit** on a donc $(x_1 x_2^{-1})(x_2 x_3^{-1}) = x_1 x_3^{-1} \in H$ et donc $x_1\mathcal{R}_H x_3$.
- **Symétrie**
  Soient $x_1, x_2 \in G$ tels que $x_1\mathcal{R}_H x_2$.
  C'est à dire $x_1 x_2^{-1} \in H$.
  Comme H est **stable par inverse** on a donc $(x_1 x_2^{-1})^{-1} = x_2 x_1^{-1} \in H$ et donc $x_2\mathcal{R}_H x_1$.

Donc $\boxed{\mathcal{R}_H \text{ est une relation d'équivalence}}$.

5.2. Soit $x \in G$. Montrer que la classe d'équivalence de x est

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

Soit $y \in G$. On a les équivalences

$$\begin{aligned} y\mathcal{R}_H x &\Leftrightarrow yx^{-1} \in H \\ &\Leftrightarrow \exists h \in H, yx^{-1} = h \\ &\Leftrightarrow \exists h \in H, y = hx \\ &\Leftrightarrow y \in Hx \end{aligned}$$

et donc $\boxed{\text{la classe d'équivalence de } x \text{ est } Hx}$.

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

Soit

$$\tau : \begin{array}{l} Hx_1 \to Hx_2 \\ g \mapsto g{x_1}^{-1}x_2. \end{array}$$

Alors τ est
- **bien définie** car pour tout $g \in Hx_1$ il existe $h \in H$ tel que $g = hx_1$ et donc $g{x_1}^{-1}x_2 = hx_1{x_1}^{-1}x_2 = hx_2 \in Hx_2$.
- **injective** car pour tout $g_1, g_2 \in Hx_1$ si $\tau(g_1) = \tau(g_2)$ alors $g_1{x_1}^{-1}x_2 = g_2{x_1}^{-1}x_2$ et donc $g_1 = g_2$.
- **surjective** car pour tout $g \in Hx_2$ on a $g{x_2}^{-1}x_1 \in Hx_1$ et $g = (g{x_2}^{-1})x_1x_2$.

D'où une $\boxed{\text{bijection de } Hx_1 \text{ vers } Hx_2}$.

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

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

Soit $\mathcal{R}_H$ la relation d'équivalence associée à H.
Comme les classes d'équivalence forment une partition de G on en particulier

$$\operatorname{card}(G) = \sum_{X \in G/\mathcal{R}_H} \operatorname{card}(X).$$

Soit $X \in G/\mathcal{R}_H$.
Alors $X = Hx$ pour un certain $x \in G$ et donc par la question précédente $\operatorname{card}(X) = \operatorname{card}(H)$.
Et donc

$$\operatorname{card}(G) = \operatorname{card}(G/\mathcal{R}_H)\operatorname{card}(H)$$

et en particulier $\boxed{\operatorname{card}(H) | \operatorname{card}(G)}$.

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 $\mathbb{U}_p$.

Soit $x \in G$ tel que $x \neq e_G$.
Alors $\langle x \rangle$ est un sous-groupe de G.
Par le théorème de Lagrange on a donc $\text{card}(\langle x \rangle) | p$ et donc $\text{card}(\langle x \rangle) = 1$ ou $\text{card}(\langle x \rangle) = p$.
Or $e_G, x \in \langle x \rangle$ et sont distincts et donc $\text{card}(\langle x \rangle) \geq 2$.
On a donc $\text{card}(\langle x \rangle) = p$ et donc $\langle x \rangle = G$.
Par la partie 2 on a donc $\boxed{G \text{ est isomorphe à } \mathbb{U}_p}$.
Remarque:
Ce résultat est essentiel pour comprendre les "petits groupes": en particulier il n'y a (à isomorphisme) près qu'un seul groupe d'ordre 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

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

On travaille tout d'abord dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ que l'on identifie à $[\![0, n-1]\!]$ par choix du représentant correspondant au reste de la division euclidienne.
Soit $a \in \mathbb{Z}$ Par le théorème de Bézout, il existe $u \in \mathbb{Z}$ tel que $au \equiv 1[n]$ ssi $a \wedge n = 1$.
Par conséquent

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{\overline{k}, k \in [\![0, n-1]\!] \text{ t.q } k \wedge n = 1\right\}$$

En particulier

$$\boxed{\varphi(n) = \text{card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right)}.$$

Soit $a \in \mathbb{Z}$ tel que $a \wedge n = 1$.
Alors $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et donc en particulier (cf partie 2),

$$\overline{a}^{\text{card}((\mathbb{Z}/n\mathbb{Z})^\times)} = \overline{1}.$$

C'es à dire

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