HAX501X – Groupes et anneaux 1

CM8 05/10/2023

Clément Dupont

Retour sur les exercices du cours

Exercice 35

Soit G un groupe et $H \subset G$ un sous-ensemble de G. Montrer que H est un sous-groupe de G si et seulement s'il vérifie les conditions suivantes :

1') $H \neq \varnothing$;

2') $\forall x, y \in H,\ xy^{-1} \in H$.

- Si H est un sous-groupe de G, montrons que H vérifie 1') et 2').

1') $H \neq \varnothing$ car $e \in H$.

2') Pour $x, y \in H$, $y^{-1} \in H$ car H est stable par passage à l'inverse, et donc $xy^{-1} \in H$ car H est stable par produit.

- Si H vérifie 1') et 2'), montrons que c'est un sous-groupe de G.

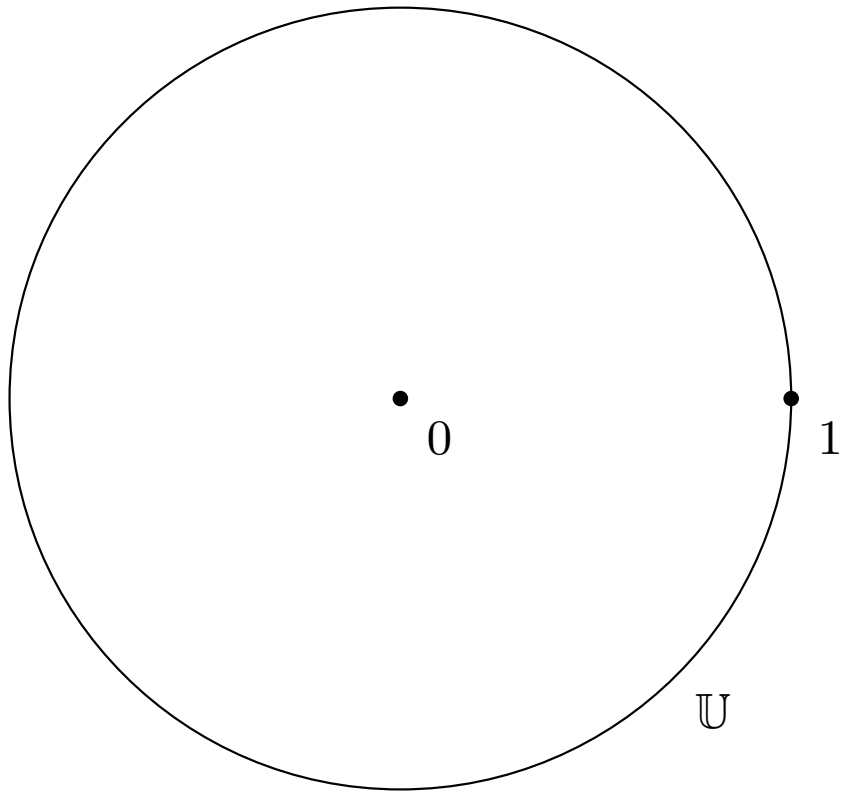
1) Comme $H \neq \varnothing$ par 1'), il existe un élément $x \in H$. D'après 2'), $xx^{-1} \in H$, et donc $e \in H$.

3) Si on applique 2') à $x = e$, on obtient alors : $\forall y \in H$, $y^{-1} \in H$. Donc H est stable par passage à l'inverse.

2) Soient $x, y \in H$. Alors par ce qu'on vient de voir $y^{-1} \in H$, et donc en appliquant 2') à x et y^{-1} on obtient $x(y^{-1})^{-1} \in H$ et donc $xy \in H$. Donc H est stable par produit.

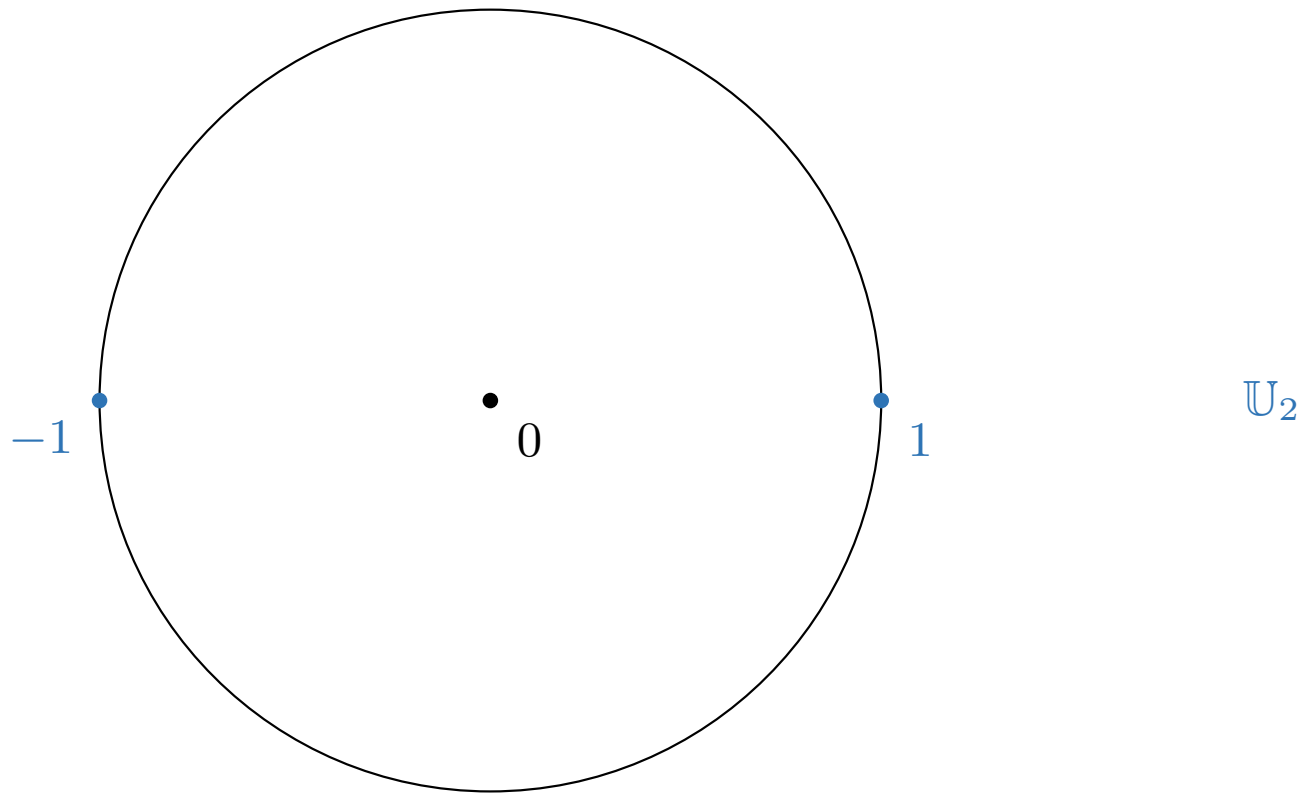
Exercice 36

Représenter dans le plan complexe les groupes $\mathbb{U}$, puis $\mathbb{U}_2$, $\mathbb{U}_3$, $\mathbb{U}_4$, $\mathbb{U}_5$, $\mathbb{U}_6$.



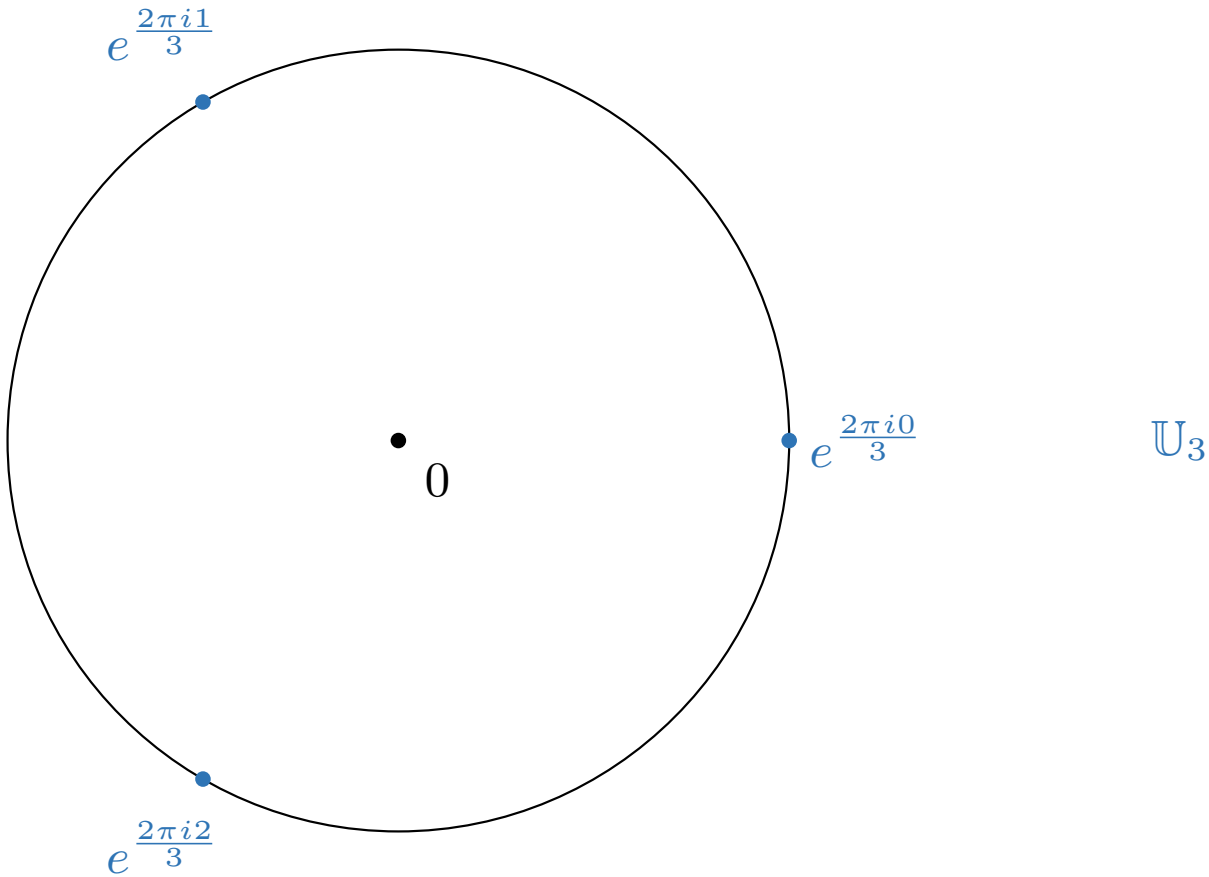
Exercice 36

Représenter dans le plan complexe les groupes $\mathbb{U}$, puis $\mathbb{U}_2$, $\mathbb{U}_3$, $\mathbb{U}_4$, $\mathbb{U}_5$, $\mathbb{U}_6$.



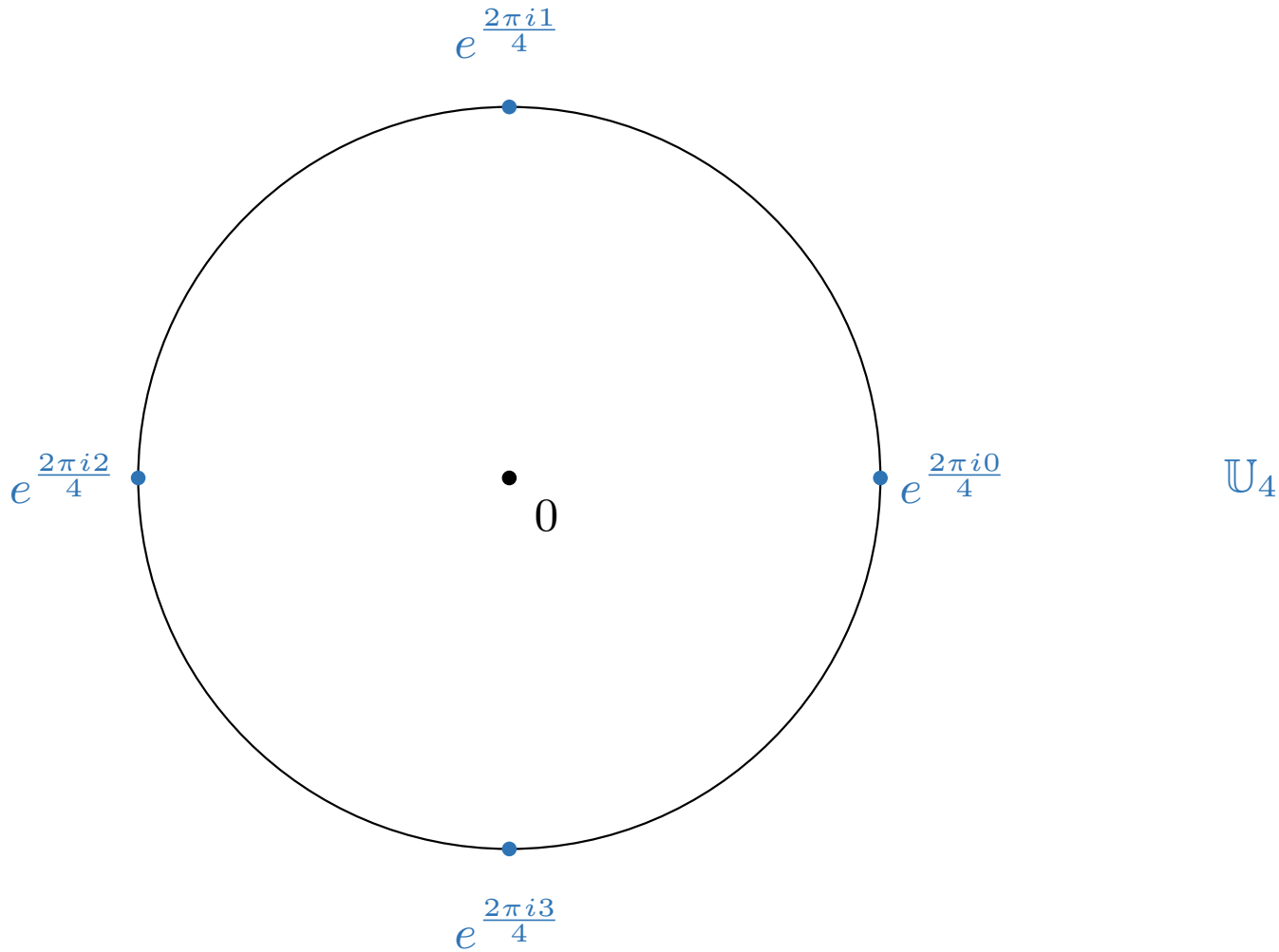
Exercice 36

Représenter dans le plan complexe les groupes $\mathbb{U}$, puis $\mathbb{U}_2$, $\mathbb{U}_3$, $\mathbb{U}_4$, $\mathbb{U}_5$, $\mathbb{U}_6$.



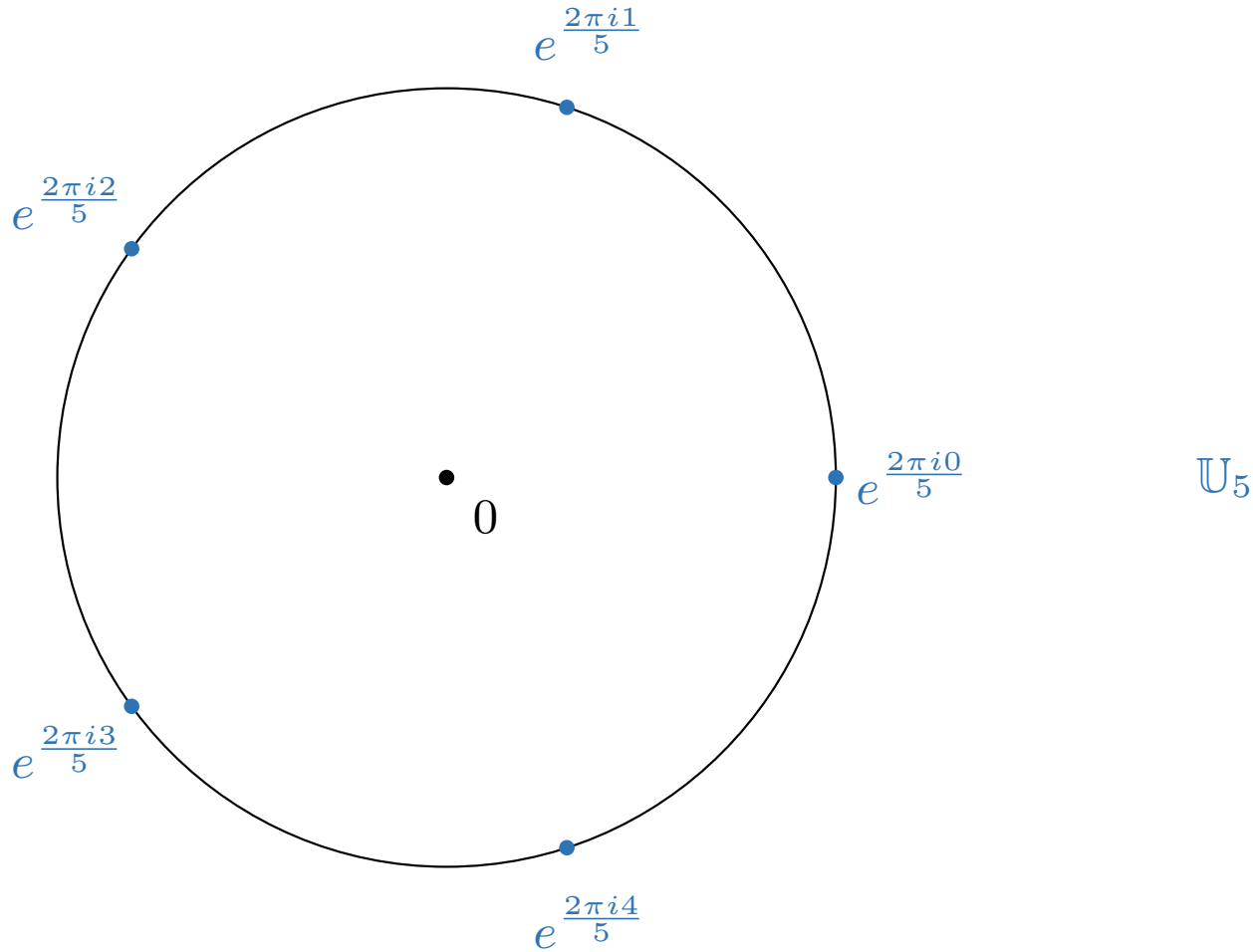
Exercice 36

Représenter dans le plan complexe les groupes $\mathbb{U}$, puis $\mathbb{U}_2$, $\mathbb{U}_3$, $\mathbb{U}_4$, $\mathbb{U}_5$, $\mathbb{U}_6$.



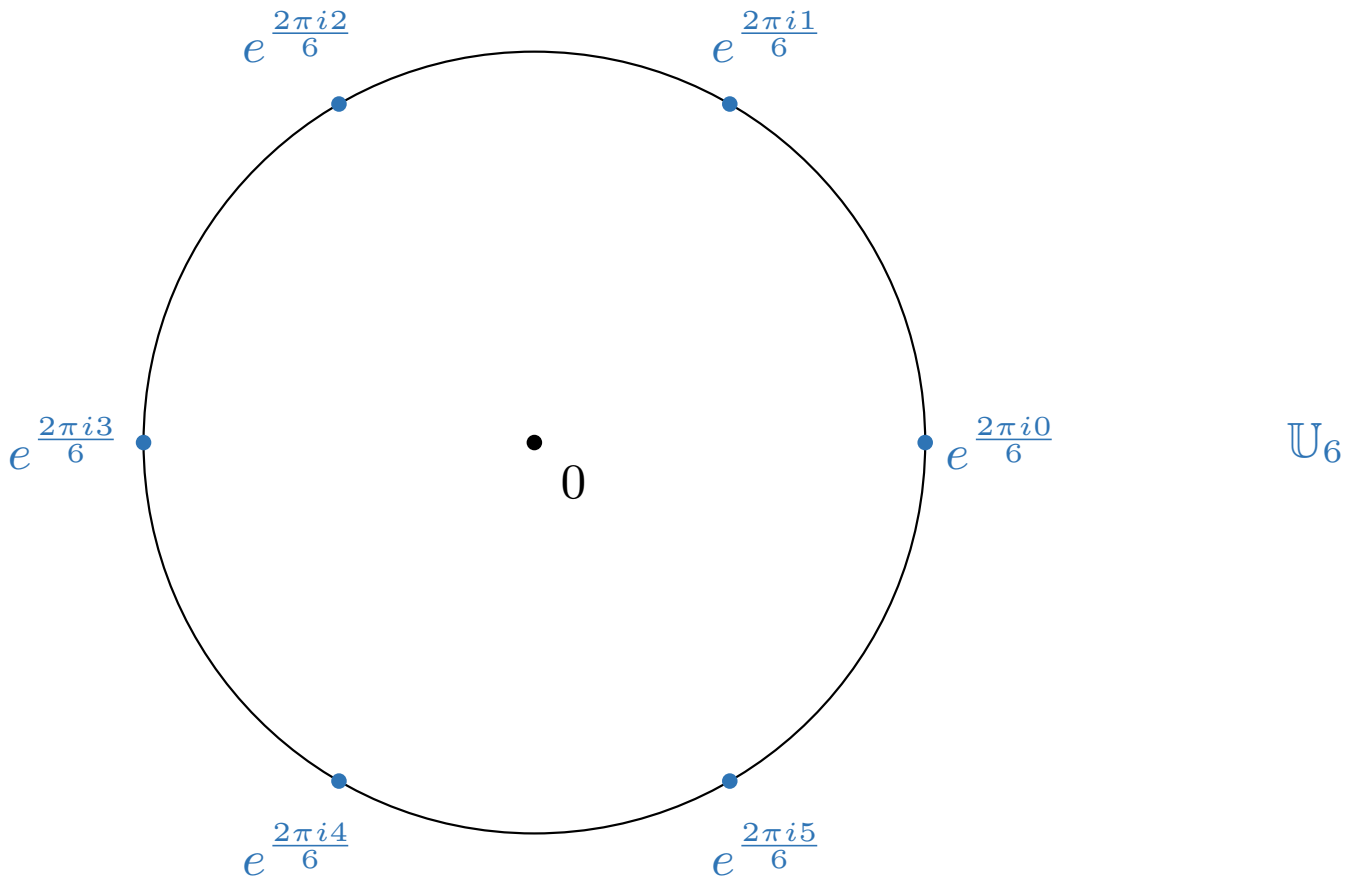
Exercice 36

Représenter dans le plan complexe les groupes $\mathbb{U}$, puis $\mathbb{U}_2$, $\mathbb{U}_3$, $\mathbb{U}_4$, $\mathbb{U}_5$, $\mathbb{U}_6$.



Exercice 36

Représenter dans le plan complexe les groupes $\mathbb{U}$, puis $\mathbb{U}_2$, $\mathbb{U}_3$, $\mathbb{U}_4$, $\mathbb{U}_5$, $\mathbb{U}_6$.



Exercice 37

Montrer que $\mathbb{U}_n$ et $\mathbb{U}$ sont des sous-groupes de $\mathbb{C}^*$. Montrer que $\mathrm{SL}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

Soit $n \in \mathbb{N}^*$. On montre que $\mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$. (On a bien $\mathbb{U}_n \subset \mathbb{C}^*$ car $0^n = 0 \neq 1$.)

1) Comme $1^n = 1$, on a $1 \in \mathbb{U}_n$.
2) Soient $z, w \in \mathbb{U}_n$, on a $z^n = 1$ et $w^n = 1$. Alors $(zw)^n = z^n w^n = 1$ donc $zw \in \mathbb{U}_n$.
3) Soit $z \in \mathbb{U}_n$, on a $z^n = 1$ et donc $(\frac{1}{z})^n = \frac{1}{z^n} = 1$ donc $\frac{1}{z} \in \mathbb{U}_n$.

Remarque

Autre justification : $\mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$ car c'est le noyau du morphisme de groupes

$$f : \mathbb{C}^* \to \mathbb{C}^* \ , \ z \mapsto z^n.$$

(C'est bien un morphisme de groupes : pour $z, w \in \mathbb{C}^*$ on a $(zw)^n = z^n w^n$.)

On montre que $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^*$. (On a bien $\mathbb{U} \subset \mathbb{C}^*$ car $|0| = 0 \neq 1$.)

1) Comme $|1| = 1$, on a $1 \in \mathbb{U}$.
2) Soient $z, w \in \mathbb{U}$, on a $|z| = 1$ et $|w| = 1$. Alors $|zw| = |z| \times |w| = 1$ donc $zw \in \mathbb{U}$.
3) Soit $z \in \mathbb{U}$, on a $|z| = 1$ et donc $|\frac{1}{z}| = \frac{1}{|z|} = 1$ donc $\frac{1}{z} \in \mathbb{U}$.

Remarque

Autre justification : $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^*$ car c'est le noyau du morphisme de groupes

$$f : \mathbb{C}^* \to \mathbb{R}^* \ , \ z \mapsto |z|.$$

(C'est bien un morphisme de groupes : pour $z, w \in \mathbb{C}^*$ on a $|zw| = |z|\,|w|$.)

On montre que $\mathrm{SL}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

1) On a $\det(I_n) = 1$ donc $I_n \in \mathrm{SL}_n(\mathbb{R})$.
2) Soient $A, B \in \mathrm{SL}_n(\mathbb{R})$, alors $\det(A) = 1$ et $\det(B) = 1$ et donc $\det(AB) = \det(A)\det(B) = 1$. Donc $AB \in \mathrm{SL}_n(\mathbb{R})$.
3) Soit $A \in \mathrm{SL}_n(\mathbb{R})$, alors $\det(A) = 1$ et donc $\det(A^{-1}) = \frac{1}{\det(A)} = 1$. Donc $A^{-1} \in \mathrm{SL}_n(\mathbb{R})$.

Remarque

Autre justification : $\mathrm{SL}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$ car c'est le noyau du morphisme de groupes

$$\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^* \ , \ A \mapsto \det(A).$$

(C'est bien un morphisme de groupes : pour $A, B \in \mathrm{GL}_n(\mathbb{R})$ on a $\det(AB) = \det(A)\det(B)$.)

Exercice 38

Montrer que le groupe symétrique $\mathfrak{S}_3$ est engendré par les transpositions $(1\ 2)$ et $(1\ 3)$:

$$\mathfrak{S}_3 = \langle\, (1\ 2), (1\ 3)\,\rangle.$$

On montre que tous les éléments de $\mathfrak{S}_3$ peuvent s'écrire comme produit de $(1\ 2)$, $(1\ 3)$ et de leurs inverses (qui sont respectivement $(1\ 2)$ et $(1\ 3)$...).

- L'identité id est égale au produit de 0 élément par convention.
- $(1\ 2) = (1\ 2)$.
- $(1\ 3) = (1\ 3)$.
- $(2\ 3) = (1\ 2)(1\ 3)(1\ 2)$ (ou aussi $(1\ 3)(1\ 2)(1\ 3)$).
- $(1\ 2\ 3) = (1\ 3)(1\ 2)$.
- $(1\ 3\ 2) = (1\ 2)(1\ 3)$.

Exercice 39

Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est un groupe cyclique.

- Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est engendré par l'élément $(\widetilde{1}, \widehat{1})$ car en ajoutant cet élément avec lui-même on trouve successivement :

$$(\widetilde{0}, \widehat{0}), (\widetilde{1}, \widehat{1}), (\widetilde{0}, \widehat{2}), (\widetilde{1}, \widehat{0}), (\widetilde{0}, \widehat{1}), (\widetilde{1}, \widehat{2}).$$

- Autre justification (en prenant un peu d'avance) : par le théorème chinois des restes, on a un isomorphisme de groupes :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}.$$

  Comme $\mathbb{Z}/6\mathbb{Z}$ est un groupe cyclique (engendré par $\overline{1}$), on en conclut qu'il en est de même pour $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Exercice 40

Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas un groupe cyclique.

Dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ on a :

- $\langle (\overline{0}, \overline{0}) \rangle = \{(\overline{0}, \overline{0})\}$;
- $\langle (\overline{1}, \overline{0}) \rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0})\}$;
- $\langle (\overline{0}, \overline{1}) \rangle = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1})\}$;
- $\langle (\overline{1}, \overline{1}) \rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{1})\}$.

Donc aucun des éléments de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'engendre $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, donc ce groupe n'est pas cyclique.

Exercice 40

Montrer que $\mathfrak{S}_n$ n'est pas un groupe cyclique si $n \geqslant 3$.

- Un groupe cyclique
$$\langle x \rangle = \{x^k,\ k \in \mathbb{Z}\}$$
est nécessairement **abélien** : en effet, pour $k, l \in \mathbb{Z}$ on a
$$x^k x^l = x^{k+l} = x^{l+k} = x^l x^k.$$
- Pour tout $n \geqslant 3$ le groupe $\mathfrak{S}_n$ n'est pas abélien et donc pas cyclique.

Exercice 41

Montrer que $\mathbb{U}_n$ est un groupe cyclique, pour tout $n \in \mathbb{N}^*$.

- On a (re)vu en exercice qu'on a

$$\mathbb{U}_n = \{e^{\frac{2ik\pi}{n}}, k \in \mathbb{Z}\} = \left\{\left(e^{\frac{2i\pi}{n}}\right)^k, k \in \mathbb{Z}\right\}.$$

- Donc $\mathbb{U}_n$ est un groupe cyclique, engendré par $e^{\frac{2i\pi}{n}}$.

Remarque

Cela explique la terminologie "cyclique".

Exercice 42

Lister tous les morphismes de groupes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$. Lister tous les endomorphismes de $\mathbb{Z}/3\mathbb{Z}$.

Soit $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ un morphisme de groupes. On a $f(\overline{0}) = \widetilde{0}$. On s'intéresse à $f(\overline{1})$.

- Si $f(\overline{1}) = \widetilde{0}$ alors $f(\overline{2}) = f(\overline{1}+\overline{1}) = f(\overline{1}) + f(\overline{1}) = \widetilde{0}+\widetilde{0} = \widetilde{0}$, et donc f est le morphisme trivial $\overline{k} \mapsto \widetilde{0}$.
- Si $f(\overline{1}) = \widetilde{1}$ alors $f(\overline{1}+\overline{1}+\overline{1}) = \widetilde{1}+\widetilde{1}+\widetilde{1} = \widetilde{3}$, et donc $f(\overline{0}) = \widetilde{3} \neq \widetilde{0}$, ce qui est impossible.
- Si $f(\overline{1}) = \widetilde{2}$ alors $f(\overline{1}+\overline{1}+\overline{1}) = \widetilde{2}+\widetilde{2}+\widetilde{2} = \widetilde{2}$, et donc $f(\overline{0}) = \widetilde{2} \neq \widetilde{0}$, ce qui est impossible.
- Si $f(\overline{1}) = \widetilde{3}$ alors $f(\overline{1}+\overline{1}+\overline{1}) = \widetilde{3}+\widetilde{3}+\widetilde{3} = \widetilde{1}$, et donc $f(\overline{0}) = \widetilde{1} \neq \widetilde{0}$, ce qui est impossible.

Conclusion : le seul morphisme de groupes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$ est le morphisme trivial $\overline{k} \mapsto \widetilde{0}$.

Soit $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ un morphisme de groupes. On a $f(\overline{0}) = \overline{0}$. On s'intéresse à $f(\overline{1})$.

- Si $f(\overline{1}) = \overline{0}$ alors $f(\overline{2}) = f(\overline{1} + \overline{1}) = f(\overline{1}) + f(\overline{1}) = \overline{0} + \overline{0} = \overline{0}$, et donc f est le morphisme trivial $\overline{k} \mapsto \overline{0}$.
- Si $f(\overline{1}) = \overline{1}$ alors $f(\overline{2}) = f(\overline{1} + \overline{1}) = \overline{1} + \overline{1} = \overline{2}$, et donc f est le morphisme identité $\overline{k} \mapsto \overline{k}$.
- Si $f(\overline{1}) = \overline{2}$ alors $f(\overline{2}) = f(\overline{1} + \overline{1}) = \overline{2} + \overline{2} = \overline{1}$. On vérifie que cela définit un morphisme de groupes. C'est le morphisme $\overline{k} \mapsto \overline{2k} = \overline{2} \times \overline{k}$

Conclusion : il y a trois endomorphismes de groupes de $\mathbb{Z}/3\mathbb{Z}$: le morphisme trivial $\overline{k} \mapsto \overline{0}$, l'identité $\overline{k} \mapsto \overline{k}$, et le morphisme $\overline{k} \mapsto \overline{2k} = \overline{2} \times \overline{k}$.

Exercice 43

Montrer que les endomorphismes de $\mathbb{Z}$ sont les applications $k \mapsto ak$ avec $a \in \mathbb{Z}$.

- On montre que pour tout $a \in \mathbb{Z}$ l'application $f : \mathbb{Z} \to \mathbb{Z}$, $k \mapsto ak$ est un morphisme de groupes : pour $k, k' \in \mathbb{Z}$ on calcule

$$f(k + k') = a(k + k') = ak + ak' = f(k) + f(k').$$

- Soit $f : \mathbb{Z} \to \mathbb{Z}$ un morphisme de groupes. Notons $a = f(1)$. On a

$$f(1) = a = a \times 1;$$
$$f(2) = f(1 + 1) = f(1) + f(1) = a + a = 2a = a \times 2;$$
$$f(3) = f(2 + 1) = f(2) + f(1) = 2a + a = 3a = a \times 3;$$
$$\dots$$

Une récurrence évidente montre que pour tout $k \geqslant 1$ on a $f(k) = ak$. Comme par ailleurs

$$f(-k) = -f(k) = -ak = a(-k)$$

cette formule est aussi valable pour $k \leqslant -1$. Elle est aussi valable pour $k = 0$ car $f(0) = 0$. Donc elle est valable pour tout $k \in \mathbb{Z}$.

Exercice 43

Pour $n \in \mathbb{N}^*$, montrer que les endomorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont les applications $\overline{k} \mapsto \overline{ak} = \overline{a} \times \overline{k}$, avec $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$.

- On montre que pour tout $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ l'application

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\,,\ \overline{k} \mapsto \overline{a} \times \overline{k}$$

est un morphisme de groupes : pour $\overline{k}, \overline{k'} \in \mathbb{Z}/n\mathbb{Z}$ on calcule

$$f(\overline{k} + \overline{k'}) = \overline{a} \times (\overline{k} + \overline{k'}) = \overline{a} \times \overline{k} + \overline{a} \times \overline{k'} = f(\overline{k}) + f(\overline{k'}).$$

- Soit $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ un morphisme de groupes. Notons $\overline{a} = f(\overline{1})$. On a

$$f(\overline{0}) = \overline{0} = \overline{a} \times \overline{0};$$
$$f(\overline{1}) = \overline{a} = \overline{a} \times \overline{1};$$
$$f(\overline{2}) = f(\overline{1} + \overline{1}) = f(\overline{1}) + f(\overline{1}) = \overline{a} + \overline{a} = \overline{2a} = \overline{a} \times \overline{2};$$
$$f(\overline{3}) = f(\overline{2} + \overline{1}) = f(\overline{2}) + f(\overline{1}) = \overline{2a} + \overline{a} = \overline{3a} = \overline{a} \times \overline{3};$$
$$\dots$$

Une récurrence évidente montre que pour tout $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ on a $f(\overline{k}) = \overline{a} \times \overline{k}$.

4. Autour de la notion d'ordre

4.1 Ordre d'un élément dans un groupe

4.2 Retour sur les groupes cycliques

4.3 Le théorème de Lagrange

4.4 Application aux groupes d'ordre premier

Ordre d'un élément dans un groupe

Définition

*Soit G un groupe et soit $x \in G$. L'***ordre** *de x dans G est le plus petit $n \in \mathbb{N}^*$ tel que $x^n = e$, avec la convention que x est d'***ordre infini** *si pour tout $n \in \mathbb{N}^*$, $x^n \neq e$.*

Remarque

En notation additive : l'ordre de x dans G est le plus petit $n \in \mathbb{N}^*$ tel que $nx = 0$, avec la convention que x est d'ordre infini si pour tout $n \in \mathbb{N}^*$, $nx \neq 0$.

Exemple

Le seul élément d'ordre 1 dans un groupe G est l'élément neutre e. Un élément x est d'ordre 2 si et seulement si $x \neq e$ et $x^2 = e$.

Le cas d'un élément d'ordre infini

- Soit $x \in G$ un élément d'ordre infini.
- Alors dans
$$\langle x \rangle = \{x^k,\ k \in \mathbb{Z}\},$$
tous les x^k, pour $k \in \mathbb{Z}$, sont deux à deux distincts.
- La loi de groupe dans $\langle x \rangle$ se calcule comme la somme dans $\mathbb{Z}$:
$$x^k x^{k'} = x^{k+k'}.$$
- Conclusion : le groupe $\langle x \rangle$ se comporte comme le groupe $\mathbb{Z}$.
- Plus formellement, le groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}$.

Le cas d'un élément d'ordre fini

- Soit $x \in G$ un élément d'ordre fini $n \in \mathbb{N}^*$.
- Alors on a
$$\langle x \rangle = \{x^k,\, k \in \mathbb{Z}\} = \{e, x, x^2, \ldots, x^{n-1}\}$$
et les x^k, pour $k \in \{0, \ldots, n-1\}$, sont deux à deux distincts.

- La loi de groupe dans $\langle x \rangle$ se calcule comme la somme dans $\mathbb{Z}/n\mathbb{Z}$:
$$x^k x^{k'} = x^{k+k'} \qquad \text{avec} \quad x^n = e.$$

- Par exemple, si x est d'ordre 6 on a
$$\langle x \rangle = \{e, x, x^2, x^3, x^4, x^5\},$$
qui a 6 éléments et où la loi de groupe se calcule comme :
$$x^5 x^4 = x^9 = x^6 x^3 = e x^3 = x^3.$$
(Ça revient à calculer dans $\mathbb{Z}/6\mathbb{Z}$: $\overline{5} + \overline{4} = \overline{3}$.)

- Conclusion : le groupe $\langle x \rangle$ se comporte comme le groupe $\mathbb{Z}/n\mathbb{Z}$.
- Plus formellement, le groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Une proposition importante

Soit $x \in G$ et considérons l'application

$$\varphi_x : \mathbb{Z} \to G \ , \ k \mapsto x^k.$$

C'est un morphisme de groupes : $\varphi_x(k+k') = x^{k+k'} = x^k x^{k'} = \varphi_x(k)\varphi_x(k')$.

Proposition

Soit G un groupe, soit $x \in G$.

- *Si x est d'ordre infini, φ_x induit un isomorphisme de groupes*

$$\mathbb{Z} \to \langle x \rangle \ , \ k \mapsto x^k.$$

- *Si x est d'ordre fini $n \in \mathbb{N}^*$, φ_x induit un isomorphisme de groupes*

$$\mathbb{Z}/n\mathbb{Z} \to \langle x \rangle \ , \ \overline{k} \mapsto x^k$$

et notamment

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}.$$

En particulier, l'ordre de x est égal à l'ordre du groupe $\langle x \rangle$.

Début de la démonstration

$$\varphi_x : \mathbb{Z} \to G \ , \ k \mapsto x^k.$$

- Par définition :
$$\mathrm{Im}(\varphi_x) = \langle\, x \,\rangle.$$
- Comme φ_x est un morphisme de groupes, le noyau $\ker(\varphi_x)$ est un sous-groupe de $\mathbb{Z}$, et donc de la forme
$$\ker(\varphi_x) = \{k \in \mathbb{Z} \mid x^k = e\} = n\mathbb{Z}$$
pour un unique $n \in \mathbb{N}$.
- Cas $n = 0$. Alors il n'existe aucun $k \in \mathbb{N}^*$ tel que $x^k = e$, donc x est d'ordre infini. De plus, $\ker(\varphi_x) = \{0\}$ donc φ_x est injective. Comme son image est $\langle\, x \,\rangle$, on obtient donc un isomorphisme de groupes
$$\mathbb{Z} \to \langle\, x \,\rangle \ , \ k \mapsto x^k.$$
- Cas $n \geqslant 1$. Alors x est d'ordre n par définition. (À suivre.)

Et en notation additive...

- Si on utilise la **notation additive** pour la loi de groupe, alors on a

$$\langle x \rangle = \{kx,\ k \in \mathbb{Z}\}$$

avec

$$kx = \underbrace{x + x + \cdots + x}_{k \text{ fois}}.$$

- On a alors

$$\varphi_x : \mathbb{Z} \to G\ ,\ k \mapsto kx.$$

- On a alors, si x est d'ordre fini $n \in \mathbb{N}^*$:

$$\langle x \rangle = \{0, x, 2x, 3x, \ldots, (n-1)x\}.$$

Une remarque

- Soit G un groupe fini, alors tout élément $x \in G$ est d'ordre fini.
- En effet, si x était d'ordre infini alors le sous-groupe $\langle x \rangle \subset G$ serait infini (en bijection avec $\mathbb{Z}$), ce qui contredirait la finitude de G.

Un exercice

Exercice 48

Dans chaque cas, donner l'ordre de x dans le groupe G et décrire $\langle x \rangle$.

- $G = \mathbb{Z}$, $x = 1$.
- $G = \mathbb{Z}$, $x = -1$.
- $G = \mathbb{Z}$, $x = 2$.
- $G = \mathbb{R}^*$, $x = 1$.
- $G = \mathbb{R}^*$, $x = -1$.
- $G = \mathbb{R}^*$, $x = 2$.
- $G = \mathfrak{S}_4$, $x = (1\ 2\ 3)(3\ 4)$.
- $G = \mathrm{GL}_2(\mathbb{R})$, $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
- $G = \mathrm{GL}_2(\mathbb{R})$, $x = \begin{pmatrix} 2 & -2 \\ 4 & -7 \end{pmatrix}$.
- $G = \mathbb{Z}/24\mathbb{Z}$, $x = \overline{14}$.

Plus d'exercices

Exercice 49
Dans $\mathbb{Z}/n\mathbb{Z}$, quel est l'ordre d'un élément $\overline{k}$?

Exercice 50
Soit G un groupe, soit $x \in G$ un élément d'ordre fini n. Pour un élément $k \in \mathbb{Z}$, quel est l'ordre de x^k ?

Une proposition importante

Proposition

Soit G un groupe et soit $x \in G$ un élément d'ordre fini n. Alors pour tout $r \in \mathbb{Z}$ on a l'équivalence :

$$x^r = e \quad \Longleftrightarrow \quad n|r.$$

Démonstration. Avec les notations ci-dessus, $x^r = e$ si et seulement si $r \in \ker(\varphi_x)$. Or $\ker(\varphi_x) = n\mathbb{Z}$ et donc c'est équivalent à $n|r$. □

Remarque

On a tendance à faire l'erreur de dire que si $x^r = e$ alors x est d'ordre r, ce qui est évidemment faux.

Classification des groupes cycliques

Proposition

Soit G un groupe. Alors G est cyclique si et seulement s'il est isomorphe à $\mathbb{Z}$ ou à un $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}^*$.

Démonstration. Comme $\mathbb{Z}$ et tous les $\mathbb{Z}/n\mathbb{Z}$ sont des groupes cycliques, tout groupe isomorphe à un de ces groupes est cyclique. Réciproquement, si G est cyclique alors il existe $x \in G$ tel que $G = \langle x \rangle$, et une proposition vue plus haut dit que G est isomorphe à $\mathbb{Z}$ ou à un $\mathbb{Z}/n\mathbb{Z}$. □

Classification des sous-groupes d'un groupe cyclique

Proposition

Soit G un groupe cyclique d'ordre fini $n \in \mathbb{N}^*$, et soit x un générateur de G. Pour chaque diviseur d de n, il existe exactement un sous-groupe de G d'ordre d, qui est le groupe cyclique engendré par $x^{n/d}$. Ce sont tous les sous-groupes de G.

Démonstration. D'après une proposition vue plus haut, on a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \simeq G$ qui envoie $\overline{k}$ sur x^k. Le résultat est alors une conséquence de la classification des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. □

Classification des générateurs d'un groupe cyclique

Proposition

Soit G un groupe cyclique d'ordre fini $n \in \mathbb{N}^*$, et soit x un générateur de G. Les générateurs de G sont les x^a avec $a \wedge n = 1$.

Démonstration. D'après une proposition vue plus haut, on a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \simeq G$ qui envoie $\overline{k}$ sur x^k. Le résultat est alors une conséquence de la classification des générateurs de $\mathbb{Z}/n\mathbb{Z}$. □

Le théorème de Lagrange

Théorème (Théorème de Lagrange)

Soit G un groupe fini et soit H un sous-groupe de G. Alors $|H|$ divise $|G|$.

Définition

*Soit G un groupe fini et soit H un sous-groupe de G. Le quotient $\frac{|G|}{|H|}$ est appelé l'***indice** *de H dans G.*

Le théorème de Lagrange pour l'ordre d'un élément

Théorème
Soit G un groupe fini et soit $x \in G$. Alors l'ordre de x divise $|G|$.

Démonstration. C'est une conséquence du théorème de Lagrange et du fait que l'ordre de x est égal à $|\langle x \rangle|$. □

- Une autre formulation, complètement équivalente :

Théorème
Soit G un groupe fini. Alors pour tout $x \in G$ on a :

$$x^{|G|} = e.$$