

# Groupes cycliques

|                                                                                   |          |
|-----------------------------------------------------------------------------------|----------|
| <b>Cours</b>                                                                      | <b>2</b> |
| 1 Sous-groupe engendré par une partie . . . . .                                   | 2        |
| 2 Interlude : le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ . . . . .                   | 2        |
| 3 Groupes monogènes et groupes cycliques . . . . .                                | 3        |
| 4 Ordre d'un élément dans un groupe . . . . .                                     | 4        |
| 5 Annexes . . . . .                                                               | 5        |
| 5.1 Annexe : pourquoi l'ordre d'un élément divise le cardinal du groupe . . . . . | 5        |
| 5.2 Annexe : théorème de Lagrange . . . . .                                       | 5        |
| <b>Exercices</b>                                                                  | <b>5</b> |
| Exercices et résultats classiques à connaître . . . . .                           | 5        |
| Un sous-groupe d'un groupe cyclique est cyclique . . . . .                        | 5        |
| Exercices . . . . .                                                               | 6        |
| Petits problèmes d'entraînement . . . . .                                         | 6        |

## 1 Sous-groupe engendré par une partie

**Proposition.** Une intersection de sous-groupes est un sous-groupe : si  $(H_i)_{i \in I}$  une famille de sous-groupes de  $(G, *)$ , alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ .

**Définition.** Soit  $(G, *)$  un groupe et  $A$  une partie de  $G$ . On appelle **sous-groupe engendré par  $A$**  le plus petit sous-groupe  $H$  de  $(G, *)$  qui contient  $A$ .

**Remarque.** On note  $\langle A \rangle$  le sous-groupe engendré par  $A$ , mais cette notation n'est pas dans le programme officiel.

**Remarque.** La définition signifie que  $H$  est le sous-groupe de  $(G, *)$  engendré par  $A$  si et seulement si :

- $H$  est un sous-groupe de  $(G, *)$
- $A \subset H$
- Pour tout sous-groupe  $K$  de  $(G, *)$ ,  $A \subset K \implies H \subset K$

**Proposition.** Avec les notations précédentes :

$$\langle A \rangle = \bigcap_{\substack{A \subset H \\ H \text{ sous-groupe de } G}} H$$

**Description du sous-groupe engendré par  $A$ .** Soit  $G$  un groupe noté multiplicativement.  $\langle A \rangle$  est l'ensemble des éléments de  $G$  qui s'écrivent sous la forme :

$$a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$$

où  $n \in \mathbb{N}$ ,  $a_1, \dots, a_n \in A$ ,  $\varepsilon_1, \dots, \varepsilon_n = \pm 1$ .

**Remarque.** Lorsque  $G$  est commutatif et noté additivement, le sous-groupe engendré par  $A$  est l'ensemble des éléments qui s'écrivent sous la forme :

$$k_1 a_1 + \dots + k_p a_p$$

où  $p \in \mathbb{N}$ ,  $a_1, \dots, a_p \in A$  sont distincts, et  $k_1, \dots, k_p \in \mathbb{Z}$ . Ce ne sont pas tout à fait des combinaisons linéaires, puisque les « scalaires » sont ici entiers.

**Proposition.** Les sous-groupes de  $\mathbb{Z}$  sont les  $a\mathbb{Z} = \langle a \rangle$ , où  $a \in \mathbb{N}$ .

**Définition.** La partie  $A$  de  $(G, *)$  est dite **génératrice de  $G$**  lorsque le sous-groupe de  $(G, *)$  engendré par  $A$  est  $G$ .

## 2 Interlude : le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

**Proposition.** Pour  $n \in \mathbb{N}$ , la relation de **congruence modulo  $n$**  sur  $\mathbb{Z}$  est définie par :

$$\begin{aligned} a \equiv b [n] &\iff a - b \in n\mathbb{Z} \\ &\iff n \mid a - b \end{aligned}$$

C'est une relation d'équivalence.

**Remarque.** Si  $n = 0$ , il s'agit simplement de l'égalité. Si  $n = 1$ , tous les entiers sont en relation.

**Proposition.** Pour  $n \geq 2$ , il y a exactement  $n$  classes d'équivalences :

$$\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

**Définition.** On note  $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ , appelé «  $\mathbb{Z}$  sur  $n\mathbb{Z}$  ».

**Remarque.** On a bien  $\text{Card}(\mathbb{Z}/n\mathbb{Z}) = n$ .

**Proposition.** Pour  $n \geq 2$ , il existe une unique loi de groupe sur  $\mathbb{Z}/n\mathbb{Z}$ , encore notée  $+$ , pour laquelle l'application  $\pi : k \mapsto \overline{k}$  soit un morphisme de groupes, i.e. :

$$\forall a, b \in \mathbb{Z}, \overline{a+b} = \overline{a} + \overline{b}$$

De plus,  $\text{Ker } \pi = n\mathbb{Z}$ .

**Remarque.** Ainsi, pour additionner deux classes d'équivalences, on additionne deux représentants de ces classes d'équivalences.

**Proposition.** Muni de cette loi,  $(\mathbb{Z}/n\mathbb{Z}, +)$  est donc bien un groupe commutatif.

**Exemple.** Construire la table de la loi  $+$  dans  $\mathbb{Z}/4\mathbb{Z}$ .

**Corollaire.** Pour  $n \in \mathbb{N}^*$ ,  $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$  et  $k \in \mathbb{Z}$ ,

$$k \cdot \bar{a} = \overline{ka}$$

**Générateurs de  $\mathbb{Z}/n\mathbb{Z}$ .**

Soit  $n$  entier  $\geq 2$ . Sont équivalentes :

- (i)  $\mathbb{Z}/n\mathbb{Z} = \langle \bar{a} \rangle$
- (ii) il existe  $k \in \mathbb{N}$  tel que  $\overline{ka} = \bar{1}$
- (iii)  $a \wedge n = 1$

**Remarque.** Ainsi,  $(\mathbb{Z}/n\mathbb{Z}, +)$  est engendré par chaque  $\bar{k}$ , où  $k \in \{0, \dots, n-1\}$  est premier avec  $n$ .

**Exemple.** Donner la liste des éléments qui engendrent  $(\mathbb{Z}/12\mathbb{Z}, +)$ .

**Comment définir un morphisme  $\mathbb{Z}/n\mathbb{Z} \rightarrow G$ .**

Soit  $n$  entier  $\geq 2$ , et  $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ .

$$k \mapsto \bar{k}$$

Si  $G$  est un groupe et  $f : \mathbb{Z} \rightarrow G$  un morphisme de groupes, alors les propriétés suivantes sont équivalentes :

- (i) il existe un morphisme  $g : \mathbb{Z}/n\mathbb{Z} \rightarrow G$  tel que  $f = g \circ \pi$
- (ii)  $n\mathbb{Z} \subset \text{Ker } f$

**Remarque.** Ainsi, pour définir un morphisme de groupe  $\mathbb{Z}/n\mathbb{Z} \rightarrow G$ , on définit un morphisme de groupe  $\mathbb{Z} \rightarrow G$  dont le noyau contient  $n\mathbb{Z}$ , et on « passe au quotient ».

**Proposition.** Les groupes  $(\mathbb{Z}/n\mathbb{Z}, +)$  et  $(\mathbb{U}_n, \times)$  sont isomorphes.

### 3 Groupes monogènes et groupes cycliques

**Définition.**

- Un groupe  $G$  est **monogène** s'il existe  $x \in G$  tel que  $G = \langle x \rangle$ . On dit que  $x$  est un **générateur** de  $x$ .
- Lorsque  $G$  est un groupe fini et monogène, on dit que c'est un **groupe cyclique**.

**Exemple.**

- $(\mathbb{Z}, +)$  est monogène, engendré par 1 (et par  $-1$ ).
- Tous les sous-groupes de  $\mathbb{Z}$  sont monogènes.
- $(\mathbb{Z}/n\mathbb{Z}, +)$  est monogène. Ses générateurs sont les  $\bar{k}$ , où  $k$  est premier avec  $n$ .
- $(\mathbb{U}_n, \times)$  est monogène. Ses générateurs sont les  $e^{\frac{2ik\pi}{n}}$ , où  $k$  est premier avec  $n$ .

**Proposition.** Soit  $(G, *)$  un groupe et  $x \in G$ . Alors :

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

Ainsi  $\langle x \rangle = \text{Im } \varphi_x$  où  $\varphi_x : \mathbb{Z} \rightarrow G$ .

$$k \mapsto x^k$$

**Théorème.**

Tout groupe monogène  $\langle x \rangle$  est isomorphe :

- soit à  $(\mathbb{Z}, +)$ , lorsque  $\text{Ker } \varphi_x = \{0\}$  ;
- soit à  $(\mathbb{Z}/n\mathbb{Z}, +)$ , lorsque  $\text{Ker } \varphi_x = n\mathbb{Z}$ .

**Remarque.** Dans le second cas,  $n = \text{Min}\{k \in \mathbb{N}^*, x^k = e\}$ .

## 4 Ordre d'un élément dans un groupe

**Définition.** Soit  $(G, *)$  un groupe dont le neutre est noté  $e$ , et  $x \in G$ . Lorsque  $\langle x \rangle$  est fini, on dit que  $x$  est d'ordre fini et on note :

$$\text{ord}(x) = \text{Min}\{n \in \mathbb{N}^*, x^n = e\}$$

l'ordre de  $x$ .

**Remarque.**

- $\text{ord}(x) = n \iff \text{Ker } \varphi_x = n\mathbb{Z}$
- Si  $\langle x \rangle$  est infini, on convient parfois que  $x$  est d'ordre infini.

**Exemple.** Quel est l'ordre de  $\bar{1}$  (resp. de  $\bar{12}$ ) dans  $\mathbb{Z}/42\mathbb{Z}$  ?

**Proposition.** Avec les notations précédentes, lorsque  $x$  est d'ordre fini  $n$ , on a :

$$x^k = e \iff n \mid k$$

**Théorème.**

Avec les notations précédentes,

$$\text{ord}(x) = \text{Card}(\langle x \rangle)$$

**Corollaire.** Si  $G$  est un groupe fini, alors tout  $x \in G$  est d'ordre fini.

**Théorème.**

Soit  $G$  un groupe fini, et  $x \in G$ . Alors :

$$\text{ord}(x) \mid \text{Card}(G)$$

c'est-à-dire que  $x^{\text{Card } G} = e$ .

**Corollaire.** Tout groupe fini dont le cardinal est premier est cyclique, et engendré par chacun de ses éléments différent du neutre.

## 5 Annexes

### 5.1 Annexe : pourquoi l'ordre d'un élément divise le cardinal du groupe

#### Théorème.

Soit  $(G, *)$  un groupe fini et  $a \in G$ . Alors l'ordre de  $a$  divise  $\text{Card}(G)$ .

*Preuve lorsque  $G$  est abélien.*

On note  $n = \text{Card}(G)$  et on énumère les éléments de  $G$  :  $G = \{g_1, \dots, g_n\}$ . On considère  $a \in G$  (c'est l'un des  $g_i$ ) et  $d$  son ordre.

L'application  $\sigma : x \mapsto a * x$  est une permutation de  $G$ , de réciproque  $x \mapsto a^{-1} * x$ , et donc :

$$\begin{aligned} g_1 * \dots * g_n &= \prod_{g \in G} g \\ &= \prod_{g \in G} \sigma(g) \\ &= (a * g_1) * \dots * (a * g_n) \\ &= a^n * (g_1 * \dots * g_n) \end{aligned}$$

en réordonnant les termes, puisque  $*$  est commutative. Ainsi, en multipliant par  $(g_1 * \dots * g_n)^{-1}$ , on en déduit :

$$e = a^n$$

et donc,  $d \mid n$ .  $\square$

*Preuve dans le cas général, non exigible.*

Soit  $a \in G$  et  $d$  son ordre. On considère la relation :

$$x \mathcal{R} y \iff x^{-1}y \in \langle a \rangle$$

C'est une relation d'équivalence (réflexive, symétrique, transitive). Pour  $x \in G$ , la classe d'équivalence de  $x$  est :

$$\begin{aligned} \bar{x} &= \{y \in G, x^{-1}y \in \langle a \rangle\} \\ &= \{y \in G, \exists k \in \mathbb{Z}, y = xa^k\} \\ &= \{x, xa, xa^2, \dots, xa^{d-1}\} \end{aligned}$$

Cette classe contient exactement  $d$  éléments.

En effet, si  $xa^k = xa^\ell$  où  $0 \leq k \leq \ell \leq d-1$ , alors  $a^{\ell-k} = e$  donc  $d \mid \ell - k$  et donc  $\ell = k$  car  $0 \leq \ell - k < d$ .

L'ensemble  $G$  est donc partitionné en ses classes d'équivalences, que l'on note  $\bar{x}_1, \dots, \bar{x}_p$  :

$$G = \bigcup_{\substack{i=1 \\ \text{union} \\ \text{disjointe}}}^p \bar{x}_i$$

donc :

$$\text{Card}(G) = \sum_{i=1}^p \text{Card}(\bar{x}_i) = \sum_{i=1}^p d = pd$$

donc  $d \mid \text{Card}(G)$ .  $\square$

**Remarque.** Cette seconde démonstration, même si elle n'est pas exigible, est intéressante, parce qu'elle nous permet d'accéder à la démonstration du théorème de Lagrange.

### 5.2 Annexe : théorème de Lagrange

#### Théorème de Lagrange, hors programme.

Si  $G$  est un groupe fini de cardinal  $n$ , alors pour tout  $H$  sous-groupe de  $G$ ,  $\text{Card } H \mid \text{Card } G$ .

*Preuve du théorème de Lagrange.*

Soit  $H$  un sous-groupe de  $G$  et  $d$  son cardinal. On considère la relation :

$$x \mathcal{R} y \iff x^{-1}y \in H$$

C'est une relation d'équivalence (réflexive, symétrique, transitive). Pour  $x \in G$ , la classe d'équivalence de  $x$  est :

$$\begin{aligned} \bar{x} &= \{y \in G, x^{-1}y \in H\} \\ &= \{y \in G, \exists h \in H, y = xh\} \\ &= xH \end{aligned}$$

Cette classe contient exactement  $d$  éléments, comme  $H$ .

L'ensemble  $G$  est donc partitionné en ses classes d'équivalences, que l'on note  $\bar{x}_1, \dots, \bar{x}_p$  :

$$G = \bigcup_{\substack{i=1 \\ \text{union} \\ \text{disjointe}}}^p \bar{x}_i$$

donc :

$$\text{Card}(G) = \sum_{i=1}^p \text{Card}(\bar{x}_i) = \sum_{i=1}^p d = pd$$

donc  $d \mid \text{Card}(G)$ .  $\square$

## Exercices et résultats classiques à connaître

### Un sous-groupe d'un groupe cyclique est cyclique

#### 111.1

Soit  $G$  un groupe cyclique de générateur  $a$ , et  $H$  un sous-groupe de  $G$ .

- Montrer qu'il existe un plus petit entier naturel  $n$  non nul tel que  $a^n \in H$ .
- Montrer que  $H = \langle a^n \rangle$ .

On a montré que tout sous-groupe d'un groupe cyclique est cyclique.

## Exercices

**111.2**

Déterminer le sous-groupe de  $(\mathbb{Z}, +)$  engendré par  $\{-27, 12, 18\}$ .

**111.3**

Montrer que le sous-groupe de  $(\mathbb{C}^*, \times)$  engendré par  $\{i = e^{i\frac{\pi}{2}}, j = e^{i\frac{2\pi}{3}}\}$  est  $\mathbb{U}_{12}$ , l'ensemble des racines 12-ièmes de l'unité.

**111.4**

Déterminer le sous-groupe de  $\mathbb{C}^*$  engendré par l'ensemble  $\mathcal{P}$  des nombres premiers.

**111.5**

Soit  $H$  un sous-groupe d'un groupe  $(G, \star)$  distinct de  $G$ . Déterminer le groupe engendré par le complémentaire  $\overline{H}$  de  $H$  dans  $G$ .

**111.6**

Soit  $G$  un groupe cyclique de cardinal  $n$ , et  $x \in G$ . Calculer  $x^n$ .

**111.7**

Soit  $(G, \star)$  un groupe fini commutatif d'ordre  $n$ , et  $a \in G$ .

- (a) Justifier que  $x \mapsto a \star x$  est une permutation de  $G$ .
- (b) En considérant le produit de tous les éléments de  $G$ , montrer que  $a^n = e$ .

**111.8**

Soit  $(G, *)$  un groupe commutatif. On considère  $g_1, g_2$  deux éléments d'ordre  $d_1, d_2$  respectivement. On suppose que  $d_1 \wedge d_2 = 1$ . Montrer que  $g_1 * g_2$  est d'ordre fini, et calculer cet ordre.

**111.9**

Démontrer que la matrice :

$$\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

est d'ordre fini dans  $\text{GL}_2(\mathbb{R})$ .

**111.10**

Dans  $\mathfrak{S}_{10}$ , déterminer l'ordre de :

$$(1 \ 4 \ 3 \ 7 \ 8)(2 \ 5 \ 7)$$

**111.11**

Voici la liste des éléments de  $\mathfrak{S}_3$  :

$$\{\text{Id}, (1 \ 2), (1 \ 3), (2 \ 3), (1 \ 2 \ 3), (1 \ 3 \ 2)\}$$

Indiquer pour chaque élément son ordre.

**111.12**

Justifier que les éléments inversibles de l'anneau  $\mathbb{Z}/11\mathbb{Z}$  forment un groupe cyclique.

## Petits problèmes d'entraînement

**111.13** 

(a) Soit  $(G, *)$  un groupe. Pour tout  $g \in G$ , on note :

$$\begin{aligned} \phi_g : G &\rightarrow G \\ x &\mapsto g * x \end{aligned}$$

Montrer que  $g \mapsto \phi_g$  est un morphisme de groupes de  $(G, *)$  dans  $(\mathfrak{S}_G, \circ)$ , et qu'il est injectif.

- (b) En déduire que tout groupe fini ayant  $n$  éléments se plonge dans  $\mathfrak{S}_n$ , c'est-à-dire est isomorphe à un sous-groupe de  $\mathfrak{S}_n$ .
- (c) Dans le cas où  $n = 4$ , identifier dans  $\mathfrak{S}_4$  un sous-groupe isomorphe à  $\mathbb{Z}/4\mathbb{Z}$  et un autre isomorphe à  $(\mathbb{Z}/2\mathbb{Z})^2$ .

**111.14**

Soit  $(G, \star)$  un groupe cyclique de cardinal  $n$ , engendré par  $a$ . Pour  $r \in \mathbb{N}^*$ , on introduit  $f : G \rightarrow G$  définie par :

$$f(x) = x^r \quad \forall x \in G$$

et on pose  $d = n \wedge r$ .

- (a) Vérifier que  $f$  est un morphisme du groupe  $(G, \star)$  vers lui-même.
- (b) Déterminer le noyau de  $f$ .
- (c) Montrer que  $\text{Im } f$  est  $\langle a^d \rangle$ , le sous-groupe de  $G$  engendré par  $a^d$ .
- (d) Pour  $y \in G$ , combien y a-t-il de solutions à l'équation  $x^r = y$ ?

### 111.15

Soit  $H$  et  $K$  deux groupes notés multiplicativement.

- (a) Montrer que si  $h$  est un élément d'ordre  $p$  de  $H$  et que  $k$  est un élément d'ordre  $k$  de  $K$ , alors  $(h, k)$  est un élément d'ordre  $\text{ppcm}(p, q)$  du groupe produit  $H \times K$ .
- (b) On suppose  $H$  et  $K$  cycliques. Montrer que  $H \times K$  est cyclique si et seulement si les ordres de  $H$  et  $K$  sont premiers entre eux.

### 111.16

On note  $\text{GL}_2(\mathbb{Z})$  l'ensemble des matrices carrées d'ordre 2 à coefficients dans  $\mathbb{Z}$  dont le déterminant vaut 1 ou  $-1$ .

- (a) Soit  $M$  une matrice carrée d'ordre 2 à coefficients entiers. Montrer que si  $M$  est inversible et que  $M^{-1}$  est à coefficients entiers, alors  $\det(M) = \pm 1$ .
- (b) Montrer que  $(\text{GL}_2(\mathbb{Z}), \times)$  est un groupe.
- (c) On considère  $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  et  $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ . Calculer l'ordre de  $A$ , de  $B$  et de  $AB$ . Que peut-on en conclure?

### 111.17

- (a) Soit  $H$  et  $K$  deux sous-groupes d'un même groupe  $G$ . On suppose  $\text{Card}(H) = \alpha$  et  $\text{Card}(K) = \beta$  avec  $\alpha \wedge \beta = 1$ . Montrer que  $H \cap K = \{e\}$ .
- (b) Soit  $H$  et  $K$  deux sous-groupes de  $G$  de même cardinal  $p$  premier. Montrer que  $H = K$  ou  $H \cap K = \{e\}$ .

### 111.18

Soit  $G$  un groupe abélien noté multiplicativement,  $H$  et  $K$  deux sous-groupes de  $G$ .

- (a) Montrer que  $HK = \{hk, h \in H, k \in K\}$  est un sous-groupe de  $G$ .
- (b) Montrer que  $HK = \langle H \cup K \rangle$ .
- (c) Montrer que, si  $H \cap K = \{e\}$ , alors  $HK$  est isomorphe au produit cartésien  $H \times K$ .
- (d) On suppose que  $G$  est de cardinal  $p^2$ , où  $p$  est premier. Montrer que tout sous-groupe de  $G$  est de cardinal 1,  $p$  ou  $p^2$ .

### 111.19

Soit  $G$  un groupe non réduit à  $\{e\}$ . Montrer que  $G$  n'admet aucun sous-groupe propre si et seulement si il est cyclique de cardinal  $p$  premier.

### 111.20

Soit  $f : G \rightarrow H$  un morphisme de groupes, où  $G$  est un groupe fini. Montrer que :

$$\text{Card}(G) = \text{Card}(\text{Im } f) \times \text{Card}(\text{Ker } f)$$

### 111.21

Soit  $(G, \star)$  un groupe commutatif de cardinal  $ab$ , où  $a, b \in \mathbb{N}^*$  sont premiers entre eux. On pose :

$$A = \{x \in G, x^a = e\} \text{ et } B = \{x \in G, x^b = e\}$$

- (a) Montrer que  $A$  et  $B$  sont des sous-groupes de  $G$ .
- (b) Montrer que  $A \cap B = \{e\}$  et  $G = \{x \star y, x \in A, y \in B\}$ .

### 111.22

Quel est le plus petit entier naturel  $n$  tel qu'il existe un groupe non commutatif à  $n$  éléments?

### 111.23

Soit  $(G, \cdot)$  un groupe et  $a, b \in G$ .

- (a) On suppose  $ab$  d'ordre fini  $n$ . Que dire de  $ba$  ?
- (b) On suppose  $a$  d'ordre fini  $n$ . Pour  $k \in \mathbb{Z}$ , quel est l'ordre de  $a^k$  ?

**111.24**

Pour  $(a, b) \in \mathbb{C}^* \times \mathbb{C}$ , on définit  $f_{a,b} : \mathbb{C} \rightarrow \mathbb{C}$  par :

$$f_{a,b}(z) = az + b$$

- (a) Montrer que  $F = \{f_{a,b}, a \in \mathbb{C}^*, b \in \mathbb{C}\}$ , muni de la loi  $\circ$ , est un groupe.
- (b) Déterminer les éléments d'ordre fini de ce groupe.

**111.25**

On s'intéresse à l'équation :

$$(E); x^2 - 2y^2 = 1$$

d'inconnue  $(x, y) \in \mathbb{Z}^2$ . On considère l'ensemble :

$$G = \{(x, y) \in \mathbb{N}^* \times \mathbb{Z}, x^2 - 2y^2 = 1\}$$

Pour  $(x, y), (x', y') \in G$  on pose :

$$(x, y) \star (x', y') = (xx' + 2yy', xy' + x'y) \text{ et } \varphi(x, y) = \ln(x + \sqrt{2}y)$$

- (a) Montrer que  $(G, \star)$  est un groupe, dont on précisera le neutre  $e$ .
- (b) On pose  $a = (3, 2) \in G$ . Montrer que :

$$\forall (x, y) \in G, 0 \leq \varphi(x, y) < \varphi(a) \implies (x, y) = e$$

- (c) Vérifier que, pour tout  $(x, y), (x', y') \in G$  :

$$\varphi((x, y) \star (x', y')) = \varphi(x, y) + \varphi(x', y')$$

- (d) En déduire que les éléments de  $G$  sont les  $a^n$ , pour  $n \in \mathbb{Z}$ .

**111.26**

Montrer qu'un groupe fini  $G$  de cardinal  $n \geq 2$  possède une partie génératrice constituée d'au plus  $\log_2(n)$  éléments.

**111.27**

Soit  $n \in \mathbb{N}^*$  et  $(e_1, \dots, e_n)$  la base canonique de  $\mathbb{R}^n$ . On note  $t_i = (1 \ i) \in \mathfrak{S}_n$  la transposition et, pour  $s \in \mathfrak{S}_n$ , on définit  $u_s \in \mathcal{L}(\mathbb{R}^n)$  en posant :

$$u_s(e_i) = u_{s(e_i)}$$

- (a) Montrer que  $(t_2, t_3, \dots, t_n)$  engendre  $\mathfrak{S}_n$ .
- (b) Interpréter géométriquement  $u_s$  lorsque  $s$  est une transposition.
- (c) Soit  $s = (1 \ 2 \ \dots \ n-1 \ n)$ . On suppose que  $s$  est la composée de  $p$  transpositions. Montrer que  $p \geq n-1$ .
- (d) Quel est le cardinal minimal d'une famille de transpositions engendrant  $\mathfrak{S}_n$  ?

**111.28**

On souhaite discuter les ordres possibles des éléments  $A \in \text{GL}_2(\mathbb{Z})$ . On note :

$$\chi_A(X) = X^2 - tX + d$$

Préciser les valeurs possibles pour  $t$  et  $d$ , et discuter ensuite des ordres possibles.

Fournir pour chacun des ordres proposés un exemple explicite.

**111.29**

Soit  $G$  un groupe fini de cardinal  $n$ ,  $p$  un nombre premier divisant  $n$ . On souhaite montrer qu'il existe un élément d'ordre  $p$  dans  $G$ .

On définit :

$$E = \{(g_1, g_2, \dots, g_p) \in G^p, g_1 g_2 \dots g_p = 1\}$$

et la relation d'équivalence  $\mathcal{R}$  sur  $E$  définie par :

$$(g_1, \dots, g_p)(h_1, \dots, h_p) \iff \exists k \in \mathbb{Z}, \forall i \in \{1, \dots, p\}, h_i = g_{i+k}$$

avec la convention  $g_{p+1} = g_1, g_{p+2} = g_2$ , etc.

- (a) Déterminer  $\text{Card}(E)$ .
- (b) Montrer qu'une classe d'équivalence pour la relation  $\mathcal{R}$  est de cardinal 1 ou  $p$ .
- (c) En déduire l'existence d'un  $g \in G \setminus \{1\}$  tel que  $g^p = 1$ .