

# GROUPES

B. Landelle

## Table des matières

|            |                                                        |           |
|------------|--------------------------------------------------------|-----------|
| <b>I</b>   | <b>Structure de groupe</b>                             | <b>2</b>  |
| 1          | Définition, propriétés . . . . .                       | 2         |
| 2          | Sous-groupe . . . . .                                  | 4         |
| <b>II</b>  | <b>Morphismes de groupes</b>                           | <b>5</b>  |
| 1          | Définition, propriétés . . . . .                       | 5         |
| 2          | Noyau et image . . . . .                               | 6         |
| 3          | Isomorphisme . . . . .                                 | 7         |
| <b>III</b> | <b>Groupe <math>(\mathbb{Z}/n\mathbb{Z}, +)</math></b> | <b>7</b>  |
| 1          | Définition . . . . .                                   | 7         |
| 2          | Opération d'addition . . . . .                         | 8         |
| 3          | Structure . . . . .                                    | 8         |
| <b>IV</b>  | <b>Groupes monogènes et cycliques</b>                  | <b>9</b>  |
| 1          | Groupe monogène . . . . .                              | 9         |
| 2          | Groupe cyclique . . . . .                              | 9         |
| 3          | Description des groupes monogènes . . . . .            | 10        |
| <b>V</b>   | <b>Ordre d'un élément</b>                              | <b>10</b> |
| 1          | Définition . . . . .                                   | 10        |
| 2          | Cas d'un groupe fini . . . . .                         | 11        |
| <b>VI</b>  | <b>Groupe symétrique</b>                               | <b>11</b> |
| 1          | Définitions . . . . .                                  | 11        |
| 2          | Cycles et transpositions . . . . .                     | 12        |
| 3          | Signature . . . . .                                    | 14        |

Les démonstrations qui ne sont pas détaillées ont été vues dans le chapitre **Structures**. On rappelle les différentes versions de la division euclidienne :

**Théorème 1 (Théorème de la division euclidienne).** Soit  $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{N} \times \llbracket 0; b - 1 \rrbracket$  tel que

$$a = bq + r$$

Soit  $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{Z} \times \llbracket 0; |b| - 1 \rrbracket$  tel que

$$a = bq + r$$

## I Structure de groupe

### 1 Définition, propriétés

**Définition 1.** On appelle groupe un couple  $(G, \star)$  avec  $G$  un ensemble (non vide) et  $\star$  une loi de composition interne sur  $G$  vérifiant :

1. la loi  $\star$  est associative, i.e.

$$\forall (a, b, c) \in G^3 \quad (a \star b) \star c = a \star (b \star c)$$

2. la loi  $\star$  admet un élément neutre (souvent noté  $e$ ), i.e.

$$\exists e \in G : \forall x \in G \quad e \star x = x = x \star e$$

3. tout élément de  $G$  admet un symétrique, i.e.

$$\forall x \in G \quad \exists y \in G : x \star y = e = y \star x$$

Si la loi  $\star$  est commutative, la groupe est dit abélien ou commutatif.

**Proposition 1.** Soit  $(G, \star)$  un groupe. On a :

1. l'élément neutre est unique et est son propre symétrique ;
2. tout élément  $x$  de  $G$  admet un unique symétrique noté  $x^{-1}$  et  $(x^{-1})^{-1} = x$  ;
3.  $\forall (x, y) \in G^2 \quad x \star y = e \quad \text{ou} \quad y \star x = e \implies y = x^{-1}$  ;
4.  $\forall (x, y) \in G^2 \quad (x \star y)^{-1} = y^{-1} \star x^{-1}$ .

**Notations :** En général, on note  $(G, +)$  un groupe abélien,  $0$  pour l'élément neutre et  $-x$  le symétrique de  $x$ . On note  $(G, \times)$  un groupe non abélien,  $1$  l'élément neutre et  $x^{-1}$  le symétrique de  $x$ .

**Définition 2.** Soit  $(G, \star)$  un groupe,  $x \in G$ . On pose  $x^0 = e$ ,  $x^{k+1} = x^k \star x$  et  $x^{-(k+1)} = x^{-k} \star x^{-1}$  pour  $k$  entier.

**Proposition 2.** Soit  $(G, \star)$  un groupe,  $x \in G$  et  $k \in \mathbb{Z}$ . On a

$$(x^{-1})^k = x^{-k}$$

*Démonstration.* Le cas  $k = 0$  est vrai. Supposons  $(x^{-1})^k = x^{-k}$  pour  $k$  entier. On a

$$(x^{-1})^{k+1} = (x^{-1})^k \star x^{-1} = x^{-k} \star x^{-1} = x^{-(k+1)}$$

ce qui prouve l'hérédité. Puis supposons  $(x^{-1})^{-k} = x^k$  pour  $k$  entier. On a

$$(x^{-1})^{-(k+1)} = (x^{-1})^{-k} \star (x^{-1})^{-1} = x^k \star x = x^{k+1}$$

Ce qui prouve l'hérédité. □

**Proposition 3.** Soit  $(G, \star)$  un groupe,  $x \in G$  et  $(k, \ell) \in \mathbb{Z}^2$ . On a

$$x^k \star x^\ell = x^{k+\ell} = x^\ell \star x^k \quad \text{et} \quad (x^k)^\ell = x^{k\ell} = (x^\ell)^k$$

*Démonstration.* On procède par de multiples raisonnements par récurrence. On montre  $x^k \star x = x^{k+1}$  pour tout  $k \in \mathbb{Z}$ . C'est vrai pour  $k$  entier. Ensuite, si  $x^{-k} \star x = x^{-k+1}$  pour  $k$  entier fixé, il vient

$$x^{-(k+1)} \star x = x^{-k} \star (x^{-1} \star x) = x^{-k} = x^{-(k+1)+1}$$

Puis, pour  $k \in \mathbb{Z}$ , on montre  $x^k \star x^\ell = x^{k+\ell}$  pour  $\ell$  entier. C'est vrai pour  $\ell = 0$  et si l'égalité a lieu pour  $\ell$  entier fixé, on a

$$x^k \star x^{\ell+1} = (x^k \star x^\ell) \star x = x^{k+\ell} \star x = x^{k+\ell+1}$$

d'après la propriété ci-avant. On applique alors la relation avec  $x^{-1}$  et  $-k$  et on trouve pour  $\ell$  entier

$$x^k \star x^{-\ell} = (x^{-1})^{-k} \star (x^{-1})^\ell = (x^{-1})^{-k+\ell} = x^{k-\ell}$$

ce qui prouve complètement la première propriété. En particulier, on a  $e = x^{k-k} = x^k \star x^{-k}$  d'où  $(x^k)^{-1} = x^{-k}$  pour tout  $k \in \mathbb{Z}$ . Puis, pour  $k \in \mathbb{Z}$ , on montre  $(x^k)^\ell = x^{k\ell}$  pour  $\ell$  entier. C'est vrai pour  $\ell = 0$  et si c'est vrai pour  $\ell$  entier, il vient

$$(x^k)^{\ell+1} = (x^k)^\ell \star x^k = x^{k\ell} \star x^k = x^{k\ell+k} = x^{k(\ell+1)}$$

d'après la première propriété. Ensuite, pour  $\ell$  entier, on trouve en utilisant un résultat auxiliaire mentionné précédemment et la proposition 2

$$(x^k)^{-\ell} = ((x^k)^{-1})^\ell = (x^{-k})^\ell = x^{-k\ell} = x^{k(-\ell)}$$

ce qui complète la deuxième propriété. □

**Remarque :** Soit  $(x, y) \in G^2$  et  $k \in \mathbb{Z}$ . On peut avoir  $(x \star y)^k \neq x^k \star y^k$ . Mais si  $x$  et  $y$  commutent, alors  $(x \star y)^k = x^k \star y^k$  et aussi  $x^k \star y^\ell = y^\ell \star x^k$  avec  $\ell \in \mathbb{Z}$ .

**Définition 3.** Soient  $(G_1, \star_1), \dots, (G_n, \star_n)$  des groupes. On définit la loi produit  $\star$  sur  $\prod_{i=1}^n G_i$  par

$$(x_1, \dots, x_n) \star (y_1, \dots, y_n) = (x_1 \star_1 y_1, \dots, x_n \star_n y_n)$$

pour  $(x_1, \dots, x_n)$  et  $(y_1, \dots, y_n)$  dans  $\prod_{i=1}^n G_i$ .

**Proposition 4.** Soient  $(G_1, \star_1), \dots, (G_n, \star_n)$  des groupes de neutres respectifs  $e_1, \dots, e_n$ . Alors  $G = \prod_{i=1}^n G_i$  muni de la loi produit  $\star$  est un groupe dont l'élément neutre est  $e = (e_1, \dots, e_n)$ . Le symétrique de  $(x_1, \dots, x_n) \in G$  est  $(x_1^{-1}, \dots, x_n^{-1})$ . Si les groupes  $(G_i, \star_i)$  sont commutatifs, alors  $(G, \star)$  l'est aussi.

*Démonstration.* On vérifie les propriétés d'un groupe : ensemble muni d'une loi interne, associative, avec un élément neutre et tout élément admet un symétrique (aucune difficulté, juste l'écrire). □

## 2 Sous-groupe

**Définition 4.** On appelle sous-groupe d'un groupe  $(G, \star)$  une partie  $H$  de  $G$  vérifiant

1.  $e \in H$ ,
2.  $\forall (x, y) \in H^2 \quad x \star y^{-1} \in H$ .

**Remarque :** Les ensembles  $\{e\}$  et  $G$  sont des sous-groupes (triviaux) de  $(G, \star)$ .

**Proposition 5.** Soit  $H$  un sous-groupe de  $(G, \star)$ . Alors  $(H, \star)$  possède une structure de groupe.

**Théorème 2.** Une intersection (quelconque) de sous-groupes de  $(G, \star)$  est un sous-groupe.

*Démonstration.* Soit  $(H_i)_{i \in I}$  une famille de sous-groupes de  $G$  avec  $I$  non vide. Notons  $H = \bigcap_{i \in I} H_i$ . On a  $e \in H_i$  pour tout  $i \in I$  d'où  $e \in H$ . Soit  $(x, y) \in H^2$ . On a  $x \star y^{-1} \in H_i$  pour tout  $i \in I$  d'où  $x \star y^{-1} \in H$ . □

**Remarque :** En général, une union de deux sous-groupes n'est pas un sous-groupe. Par exemple, dans  $(\mathbb{R}^2, +)$ , les ensembles  $\mathbb{R} \times \{0\}$  et  $\{0\} \times \mathbb{R}$  sont des sous-groupes mais pas leur union. On peut démontrer que l'union de deux sous-groupes est un sous-groupe si et seulement si l'un est inclus dans l'autre.

**Définition 5.** Soit  $(G, \star)$  un groupe et  $A \subset G$ . On appelle sous-groupe engendré par  $A$  noté  $\langle A \rangle$  l'intersection de tous les sous-groupes de  $(G, \star)$  contenant  $A$  :

$$\langle A \rangle = \bigcap_{H \in \mathcal{S}} H \quad \text{avec} \quad \mathcal{S} = \{H \text{ sous-groupe de } G \mid A \subset H\}$$

**Remarque :** L'intersection porte sur un ensemble non vide puisque  $G \in \mathcal{S}$ .

**Théorème 3.** Soit  $(G, \star)$  un groupe et  $A \subset G$ . L'ensemble  $\langle A \rangle$  est le plus petit sous-groupe de  $G$  contenant  $A$ .

*Démonstration.* On a clairement  $A \subset \langle A \rangle$  et  $\langle A \rangle$  sous-groupe de  $G$  comme intersection de sous-groupes de  $G$ . Soit  $H \in \mathcal{S}$ . Alors  $\langle A \rangle = \bigcap_{K \in \mathcal{S}} K \subset H$ . □

**Notation :** Pour  $a \in G$ , on note  $\langle \{a\} \rangle = \langle a \rangle$ .

**Théorème 4.** Soit  $(G, \star)$  un groupe et  $a \in G$ . Alors, le sous-groupe  $\langle a \rangle$  est abélien et on a

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

*Démonstration.* Notons  $H = \{a^k, k \in \mathbb{Z}\}$ . Vérifions qu'il s'agit du plus petit sous-groupe de  $G$  contenant  $a$ . On a  $a^0 = e \in H$ . Puis, pour  $(x, y) \in H^2$ , il existe  $(k, \ell) \in \mathbb{Z}^2$  tel que  $x = a^k$  et  $y = a^\ell$ . Ainsi, on a  $x \star y^{-1} = a^{k-\ell} \in H$  et  $a^1 = a \in H$ . Si  $K$  est sous-groupe de  $G$  contenant  $a$ , alors pour  $k \in \mathbb{N}$ , on a  $a^k \in K$  par récurrence et  $a^{-k} = (a^k)^{-1} \in K$  par symétrie. Ainsi, on a  $H \subset K$  ce qui signifie que  $H$  est le plus petit sous-groupe contenant  $a$ , autrement dit  $H = \langle a \rangle$ . Enfin, on a

$$\forall (k, \ell) \in \mathbb{Z}^2 \quad a^k \star a^\ell = a^{k+\ell} = a^\ell \star a^k$$

ce qui prouve le caractère abélien. □

**Remarque :** Pour un groupe  $(G, +)$  abélien, on a

$$\forall a \in G \quad \langle a \rangle = \{ka, k \in \mathbb{Z}\}$$

**Théorème 5.** Les sous-groupes de  $(\mathbb{Z}, +)$  sont les  $n\mathbb{Z}$  avec  $n \in \mathbb{N}$ .

*Démonstration.* Pour  $n \in \mathbb{N}$ , on a  $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\} = \langle n \rangle$  sous-groupe de  $(\mathbb{Z}, +)$ . Montrons que les  $n\mathbb{Z}$  avec  $n \in \mathbb{N}$  sont les seuls sous-groupes de  $(\mathbb{Z}, +)$ . Soit  $H$  sous-groupe de  $(\mathbb{Z}, +)$  différent de  $\{0\}$ . On a  $H \cap \mathbb{N}^* \neq \emptyset$ . En effet, il existe  $p \in H \setminus \{0\}$ . Si  $p > 0$ , c'est fini et sinon, son symétrique  $-p$  est dans  $H \cap \mathbb{N}^*$ . Ainsi, la partie  $H \cap \mathbb{N}^*$  est une partie de  $\mathbb{N}^*$  non vide qui admet donc un plus petit élément. On pose  $n = \min H \cap \mathbb{N}^*$ . Comme  $n \in H$ , il s'ensuit que  $\langle n \rangle \subset H$ . Soit  $\ell \in H$ . D'après le théorème de la division euclidienne, il existe  $(q, r) \in \mathbb{Z} \times \llbracket 0; n-1 \rrbracket$  tel que  $\ell = nq + r$ . Par suite, on a  $r = \ell - nq \in H$  mais comme  $r < n$  et  $n = \min H \cap \mathbb{N}^*$ , il s'ensuit que  $r = 0$  d'où  $\ell = nq \in \langle n \rangle$  ce qui prouve  $H \subset \langle n \rangle$  d'où  $H = \langle n \rangle$ .  $\square$

## II Morphismes de groupes

### 1 Définition, propriétés

**Définition 6.** Soient  $(G_1, \star_1)$  et  $(G_2, \star_2)$  des groupes. On appelle morphisme du groupe  $(G_1, \star_1)$  vers le groupe  $(G_2, \star_2)$  une application  $\varphi : G_1 \rightarrow G_2$  vérifiant

$$\forall (x, y) \in G_1^2 \quad \varphi(x \star_1 y) = \varphi(x) \star_2 \varphi(y)$$

Si  $(G_1, \star_1) = (G_2, \star_2)$ , le morphisme est dit endomorphisme de groupes.

**Exemples :**  $\exp : (\mathbb{C}, +) \rightarrow (\mathbb{C}^*, \times)$ ,  $\varphi : (\mathbb{R}, +) \rightarrow (\mathbb{C}^*, \times)$ ,  $\theta \mapsto e^{i\theta}$ ,  $\varphi : (\mathcal{O}_n(\mathbb{R}), \times) \rightarrow (\{1, -1\}, \times)$ ,  $A \mapsto \det(A)$ ,  $R : (\mathbb{R}, +) \rightarrow (\mathcal{SO}_2(\mathbb{R}), \times)$ ,  $\theta \mapsto R(\theta)$ , etc.

 **Un exemple important et très utile :** Soit  $(G, \star)$  un groupe. Pour  $a \in G$ ,  $\varphi : \mathbb{Z} \rightarrow G$ ,  $k \mapsto a^k$ .

**Proposition 6.** Une composée de morphismes de groupes est un morphisme de groupes.

*Démonstration.* Immédiate.  $\square$

**Proposition 7.** Soit  $\varphi$  morphisme du groupe  $(G_1, \star_1)$  vers le groupe  $(G_2, \star_2)$ . On a

$$\varphi(e_1) = e_2 \quad \forall (x, k) \in G_1 \times \mathbb{Z} \quad \varphi(x^k) = \varphi(x)^k$$

*Démonstration.* On a  $\varphi(e_1) = \varphi(e_1 \star_1 e_1) = \varphi(e_1) \star_2 \varphi(e_1)$  et en composant par  $\varphi(e_1)^{-1}$ , on trouve  $\varphi(e_1) = e_2$ . Soit  $x \in G$ . Par récurrence, on a  $\varphi(x^k) = \varphi(x)^k$  pour  $k$  entier. Puis, avec  $\varphi(x) \star_2 \varphi(x^{-1}) = \varphi(x \star_1 x^{-1}) = \varphi(e_1) = e_2$ , on trouve  $\varphi(x^{-1}) = \varphi(x)^{-1}$  et pour  $k$  entier

$$\varphi(x^{-k}) = \varphi((x^{-1})^k) = \varphi(x^{-1})^k = (\varphi(x)^{-1})^k = \varphi(x)^{-k}$$

$\square$

## 2 Noyau et image

**Théorème 6.** *L'image d'un sous-groupe par un morphisme de groupes est un sous-groupe.*

*Démonstration.* Soit  $\varphi$  morphisme du groupe  $(G_1, \star_1)$  vers le groupe  $(G_2, \star_2)$  et  $H_1$  sous-groupe de  $G_1$ . On a  $e_2 = \varphi(e_1) \in \varphi(H_1)$ . Soit  $(u, v) \in \varphi(H_1)^2$ . Il existe  $(x, y) \in H_1^2$  tel que  $u = \varphi(x)$  et  $v = \varphi(y)$  et on a

$$u \star_2 v^{-1} = \varphi(x) \star_2 \varphi(y)^{-1} = \varphi(x) \star_2 \varphi(y^{-1}) = \varphi(x \star_1 y^{-1}) \in \varphi(H_1)$$

Ainsi, l'ensemble  $\varphi(H_1)$  est un sous-groupe de  $G_2$ .  $\square$

**Théorème 7.** *L'image réciproque d'un sous-groupe par un morphisme de groupes est un sous-groupe.*

*Démonstration.* Soit  $\varphi$  morphisme du groupe  $(G_1, \star_1)$  vers le groupe  $(G_2, \star_2)$  et  $H_2$  sous-groupe de  $G_2$ . On a  $\varphi(e_1) = e_2 \in H_2$  d'où  $e_1 \in \varphi^{-1}(H_2)$ . Soit  $(x, y) \in \varphi^{-1}(H_2)^2$ . On a

$$\varphi(x \star_1 y^{-1}) = \varphi(x) \star_2 \varphi(y)^{-1} \in H_2$$

d'où  $x \star_1 y^{-1} \in \varphi^{-1}(H_2)$  ce qui prouve que  $\varphi^{-1}(H_2)$  est un sous-groupe de  $G_1$ .  $\square$

**Définition 7.** Soit  $\varphi$  morphisme du groupe  $(G_1, \star_1)$  vers le groupe  $(G_2, \star_2)$ . On appelle image du morphisme  $\varphi$  noté  $\text{Im } \varphi$  l'ensemble défini par  $\text{Im } \varphi = \varphi(G_1)$  et noyau du morphisme  $\varphi$  noté  $\text{Ker } \varphi$  l'ensemble défini par  $\text{Ker } \varphi = \varphi^{-1}(\{e_2\})$ .

**Corollaire 1.** *L'image et le noyau d'un morphisme de groupes sont des sous-groupes.*

*Démonstration.* Conséquence immédiate des théorèmes 6 et 7.  $\square$

**Exemples :**  $\mathcal{SO}_n(\mathbb{R})$  est le noyau du morphisme  $\varphi : (\mathcal{O}_n(\mathbb{R}), \times) \rightarrow (\{-1, 1\}, \times), A \mapsto \det(A)$ .  $\mathbb{U}$  est l'image du morphisme  $\varphi : (\mathbb{R}, +) \rightarrow (\mathbb{C}^*, \times), \theta \mapsto e^{i\theta}$ .

**Proposition 8.** Soit  $\varphi$  morphisme du groupe  $(G_1, \star_1)$  vers le groupe  $(G_2, \star_2)$ . On a

$$\varphi \text{ injectif} \iff \text{Ker } \varphi = \{e_1\}$$

*Démonstration.* Le sens direct est immédiat car

$$x \in \text{Ker } \varphi \iff \varphi(x) = e_2 = \varphi(e_1) \implies x = e_1$$

Réciproquement, supposons  $\text{Ker } \varphi = \{e_1\}$ . Soit  $(x, y) \in G_1^2$ . On a

$$\varphi(x) = \varphi(y) \implies \varphi(x \star_1 y^{-1}) = \varphi(x) \star_2 \varphi(y)^{-1} = e_2 \implies x \star_1 y^{-1} \in \text{Ker } \varphi = \{e_1\}$$

autrement dit  $\varphi(x) = \varphi(y) \implies x \star_1 y^{-1} = e_1 \implies x = y$

$\square$

### 3 Isomorphisme

**Définition 8.** On appelle isomorphisme de groupes un morphisme de groupes bijectif.

**Définition 9.** Deux groupes sont dits isomorphes s'il existe un isomorphisme entre eux.

**Notation :** On note  $(G_1, \star_1) \simeq (G_2, \star_2)$  ou plus simplement  $G_1 \simeq G_2$  s'il n'y a aucune confusion possible sur la loi interne.

**Exemples :**  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$  est un isomorphisme de groupes.

**Proposition 9.** Une composée d'isomorphisme de groupes est un isomorphisme de groupes.

*Démonstration.* Immédiate. □

**Proposition 10.** L'application réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.

*Démonstration.* Soit  $\varphi$  isomorphisme du groupe  $(G_1, \star_1)$  vers le groupe  $(G_2, \star_2)$ . L'application  $\varphi^{-1}$  est bijective en tant que réciproque d'une application bijective. Soit  $(u, v) \in G_2^2$  et  $(x, y) \in G_1^2$  tel que  $u = \varphi(x)$  et  $v = \varphi(y)$ . On a

$$\varphi^{-1}(u \star_2 v) = \varphi^{-1}(\varphi(x) \star_2 \varphi(y)) = \varphi^{-1}(\varphi(x \star_1 y)) = x \star_1 y = \varphi^{-1}(u) \star_1 \varphi^{-1}(v)$$

□

**Définition 10.** On appelle automorphisme d'un groupe  $(G, \star)$  un isomorphisme de  $(G, \star)$  dans lui-même.

**Exemple :** Soit  $(G, \star)$  un groupe et  $a \in G$ . L'application  $\varphi_a : G \rightarrow G, x \mapsto a \star x \star a^{-1}$  est un automorphisme de  $G$  (appelé *automorphisme intérieur*).

## III Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

**Rappels :** Soit  $E$  un ensemble. Une relation d'équivalence  $\mathcal{R}$  sur  $E$  est une relation binaire réflexive, symétrique et transitive. On appelle classe d'équivalence d'un élément  $x \in E$  l'ensemble noté  $\bar{x}$  ou  $\dot{x}$  des éléments qui sont en relation avec  $x$ , à savoir

$$\bar{x} = \{y \in E \mid y \mathcal{R} x\}$$

L'ensemble des classes d'équivalence forme une partition de  $E$ . Pour  $(x, y) \in E^2$ , on a

$$x \mathcal{R} y \iff \bar{x} = \bar{y} \quad \text{et} \quad x \not\mathcal{R} y \iff \bar{x} \cap \bar{y} = \emptyset$$

### 1 Définition

**Définition 11.** Soit  $n$  entier non nul et  $(a, b) \in \mathbb{Z}^2$ . On dit que  $a$  et  $b$  sont congrus modulo  $n$  si  $a - b \in n\mathbb{Z}$  ou encore  $n \mid a - b$ , autrement dit s'il existe  $k \in \mathbb{Z}$  tel que  $a - b = kn$ . On note  $a \equiv b [n]$ .

**Proposition 11.** Soit  $n$  entier non nul. La relation de congruence modulo  $n$  est une relation d'équivalence.

*Démonstration.* Soit  $(a, b, c) \in \mathbb{Z}^3$ . On a  $a = a + 0 \times n$  d'où  $a \equiv a [n]$ . Si  $a \equiv b [n]$ , alors  $a = b + kn$  avec  $k \in \mathbb{Z}$  d'où  $b = a - kn$  et  $-k \in \mathbb{Z}$  donc  $b \equiv a [n]$  et si de plus  $b \equiv c [n]$ , alors  $b = c + \ell n$  avec  $\ell \in \mathbb{Z}$  d'où  $a = c + (k + \ell)n$  avec  $k + \ell \in \mathbb{Z}$  d'où  $a \equiv c [n]$ .  $\square$

**Notation :** Pour  $k \in \mathbb{Z}$ , on note  $\bar{k}$  ou  $\dot{k}$  la classe d'équivalence de  $k \in \mathbb{Z}$ , à savoir

$$\bar{k} = \{\ell \in \mathbb{Z} \mid \ell \equiv k [n]\}$$

**Définition 12.** Soit  $n$  entier non nul. On note  $\mathbb{Z}/n\mathbb{Z}$  l'ensemble des classes d'équivalence de la relation de congruence modulo  $n$ , i.e.  $\mathbb{Z}/n\mathbb{Z} = \{\bar{k}, k \in \mathbb{Z}\}$ .

**Proposition 12.** Soit  $n$  entier non nul. On a  $\text{Card } \mathbb{Z}/n\mathbb{Z} = n$  et

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{k}, k \in \llbracket 0; n-1 \rrbracket\}$$

*Démonstration.* Soit  $\ell \in \mathbb{Z}$ . D'après le théorème de la division euclidienne, il existe un unique couple  $(q, r) \in \mathbb{Z} \times \llbracket 0; n-1 \rrbracket$  tel que  $\ell = nq + r$  d'où  $\bar{\ell} = \bar{r}$  ce qui prouve  $\mathbb{Z}/n\mathbb{Z} = \{\bar{k}, k \in \llbracket 0; n-1 \rrbracket\}$ . Montrons que les classes  $\bar{k}$  pour  $k \in \llbracket 0; n-1 \rrbracket$  sont deux à deux distinctes. Soit  $(k, \ell) \in \llbracket 0; n-1 \rrbracket^2$ . Si  $\bar{k} = \bar{\ell}$ , alors  $k - \ell \in n\mathbb{Z}$ . Or, on a  $k - \ell \in \llbracket -(n-1); n-1 \rrbracket$  d'où  $k = \ell$ . Par contraposée, si  $k \neq \ell$ , alors on a  $\bar{k} \neq \bar{\ell}$ . Ainsi, les classes  $\bar{k}$  pour  $k \in \llbracket 0; n-1 \rrbracket$  sont deux à deux distinctes ce qui prouve  $\text{Card } \mathbb{Z}/n\mathbb{Z} = n$ .  $\square$

## 2 Opération d'addition

**Proposition 13.** Soit  $n$  entier non nul. La relation de congruence modulo  $n$  est compatible avec l'addition, i.e.

$$\forall (x, y, u, v) \in \mathbb{Z}^4 \quad \begin{cases} x \equiv u [n] \\ y \equiv v [n] \end{cases} \implies x + y \equiv u + v [n]$$

*Démonstration.* Soit  $(k, \ell) \in \mathbb{Z}^2$  tel que  $x = u + kn$  et  $y = v + \ell n$ . Par suite

$$x + y = u + v + n(k + \ell)$$

d'où le résultat.  $\square$

**Définition 13.** Soit  $n$  entier non nul. On munit  $\mathbb{Z}/n\mathbb{Z}$  de l'opération  $+$  définie par

$$\forall (x, y) \in \mathbb{Z}^2 \quad \bar{x} + \bar{y} = \overline{x + y}$$

**Remarque :** D'après la proposition précédente, cette opération est bien définie puisque le résultat de l'addition ne dépend pas des représentants choisis pour chaque classe : pour  $(x, y) \in \mathbb{Z}^2$ , on a  $\overline{x + y} = \bar{u} + \bar{v}$  pour tout  $(u, v) \in \bar{x} \times \bar{y}$ .

## 3 Structure

**Théorème 8.** Soit  $n$  entier non nul. Le couple  $(\mathbb{Z}/n\mathbb{Z}, +)$  est un groupe abélien de neutre  $\bar{0}$ .

*Démonstration.* L'addition définie sur  $\mathbb{Z}/n\mathbb{Z}$  est bien une loi interne. Soient  $(x, y, z) \in \mathbb{Z}^3$ . On a

$$\bar{x} + \bar{y} = \overline{x + y} = \overline{y + x} = \bar{y} + \bar{x}$$

ce qui prouve que la loi est commutative. Puis

$$(\bar{x} + \bar{y}) + \bar{z} = \overline{x + y} + \bar{z} = \overline{x + y + z} = \bar{x} + \overline{y + z} = \bar{x} + (\bar{y} + \bar{z})$$

et 
$$\bar{x} + \bar{0} = \overline{x + 0} = \bar{x}$$

et 
$$\bar{x} + \overline{-x} = \overline{x - x} = \bar{0}$$

d'où la structure de groupe abélien. □

**Remarque :** On a établi que pour tout  $x \in \mathbb{Z}$ , on a  $-\bar{x} = \overline{-x}$ .

**Proposition 14.** Soit  $n$  entier non nul. L'application  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, x \mapsto \bar{x}$  est un morphisme de groupes avec  $\text{Im } \varphi = \mathbb{Z}/n\mathbb{Z}$  et  $\text{Ker } \varphi = n\mathbb{Z}$ .

*Démonstration.* Par définition de l'addition dans  $\mathbb{Z}/n\mathbb{Z}$ , l'application  $\varphi$  est un morphisme. On a clairement  $\varphi$  surjective et  $\varphi(x) = \bar{0} \iff x \in n\mathbb{Z}$ . □

**Proposition 15.** Soit  $n$  entier non nul,  $x \in \mathbb{Z}$  et  $k \in \mathbb{Z}$ . On a  $k\bar{x} = \overline{kx}$ .

*Démonstration.* Considérant le morphisme  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, x \mapsto \bar{x}$ , pour  $x \in \mathbb{Z}$ , on a

$$\forall k \in \mathbb{Z} \quad k\bar{x} = k\varphi(x) = \varphi(kx) = \overline{kx}$$

□

## IV Groupes monogènes et cycliques

### 1 Groupe monogène

**Définition 14.** Un groupe  $(G, \star)$  est dit monogène s'il est engendré par un élément, i.e. il existe  $a \in G$  tel que  $G = \langle a \rangle$ . On dit que  $a$  est un générateur de  $G$ .

**Exemples :**  $\mathbb{Z} = \langle 1 \rangle$ ,  $\mathbb{U}_n = \langle \omega \rangle$  avec  $\omega = e^{\frac{2i\pi}{n}}$  et  $n$  entier non nul.

**Théorème 9.** Un groupe monogène est abélien.

*Démonstration.* Conséquence immédiate du théorème 4. □

### 2 Groupe cyclique

**Définition 15.** Un groupe est dit cyclique s'il est monogène fini (de cardinal fini).

**Exemple :**  $\mathbb{U}_n = \langle \omega \rangle$  avec  $\omega = e^{\frac{2i\pi}{n}}$  et  $n$  entier non nul.

**Théorème 10.** Soit  $n$  entier non nul. Le groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$  est cyclique et ses générateurs sont les  $\bar{k}$  avec  $k \in \mathbb{Z}$  tel que  $k \wedge n = 1$ .

*Démonstration.* On a  $\langle \bar{1} \rangle = \{k\bar{1}, k \in \mathbb{Z}\} = \{\bar{k}, k \in \mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$

d'où  $\mathbb{Z}/n\mathbb{Z}$  monogène et donc cyclique puisque fini. Soit  $k \in \mathbb{Z}$ . On a

$$\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z} \iff \bar{1} \in \langle \bar{k} \rangle$$

L'implication directe est immédiate et la réciproque résulte de  $\langle \bar{1} \rangle \subset \langle \bar{k} \rangle$ . Puis

$$\bar{1} \in \langle \bar{k} \rangle \iff \exists u \in \mathbb{Z} \mid \bar{1} = u\bar{k} = \overline{uk} \iff \exists (u, v) \in \mathbb{Z}^2 \mid 1 = uk + vn \iff k \wedge n = 1$$

la dernière équivalence provenant du théorème de Bezout. □

### 3 Description des groupes monogènes

**Théorème 11.** Soit  $(G, \star)$  un groupe monogène.

- Si  $\text{Card } G = +\infty$ , alors  $(G, \star) \simeq (\mathbb{Z}, +)$  ;
- Si  $\text{Card } G = n$  avec  $n$  entier non nul, alors  $(G, \star) \simeq (\mathbb{Z}/n\mathbb{Z}, +)$ .

*Démonstration.* Soit  $a$  générateur de  $G$ . L'application  $\varphi : \mathbb{Z} \rightarrow G, k \mapsto a^k$  est un morphisme de groupes surjectif puisque  $G = \langle a \rangle = \text{Im } \varphi$ . Le noyau  $\text{Ker } \varphi$  est un sous-groupe de  $\mathbb{Z}$  d'où  $\text{Ker } \varphi = n\mathbb{Z}$  avec  $n$  entier. Si  $n = 0$ , alors  $\varphi$  est un isomorphisme de groupe entre  $(\mathbb{Z}, +)$  et  $(G, \star)$  d'où  $G$  infini. Si  $n \neq 0$ , on a  $\varphi(k) = \varphi(\ell) \iff k \equiv \ell [n]$  ce qui signifie que  $\varphi$  est constante sur une classe d'équivalence pour la relation de congruence modulo  $n$ . On pose alors  $\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \rightarrow G, \bar{k} \mapsto \varphi(k) = a^k$  avec  $k \in \llbracket 0; n-1 \rrbracket$ . Cette application est bien définie puisque  $\varphi(\ell) = \varphi(k)$  pour tout  $\ell \in \bar{k}$  ce qui signifie que  $\varphi(k)$  ne dépend que du choix de la classe  $\bar{k}$  et non du choix d'un représentant dans  $\bar{k}$ . Pour  $(k, \ell) \in \mathbb{Z}^2$ , on a

$$\bar{\varphi}(\bar{k}) \star \bar{\varphi}(\bar{\ell}) = \varphi(k) \star \varphi(\ell) = \varphi(k + \ell) = \bar{\varphi}(\overline{k + \ell}) = \bar{\varphi}(\bar{k} + \bar{\ell})$$

donc l'application  $\bar{\varphi}$  est un morphisme. Pour  $k \in \mathbb{Z}$ , on a  $a^k = \bar{\varphi}(\bar{k})$  puisque  $k \in \bar{k}$  d'où la surjectivité de  $\bar{\varphi}$ . Puis, on a

$$\bar{k} \in \text{Ker } \bar{\varphi} \iff \varphi(k) = e \iff k \in \text{Ker } \varphi = n\mathbb{Z} \iff \bar{k} = \bar{0}$$

d'où l'injectivité et donc la bijectivité de  $\bar{\varphi}$ . En particulier, on a

$$n = 0 \implies \text{Card } G = \infty \quad \text{et} \quad n > 0 \implies \text{Card } G < \infty$$

Par contraposition et l'étude qui précède, on a le résultat attendu.  $\square$

## V Ordre d'un élément

### 1 Définition

**Définition 16.** Soit  $(G, \star)$  un groupe. Un élément  $x \in G$  est dit d'ordre fini s'il existe  $n$  entier non nul tel que  $x^n = e$ . On appelle ordre de  $x$  le plus petit entier  $n$  non nul tel que  $x^n = e$ .

**Notation :** Si  $x$  est d'ordre fini, on note  $o(x)$  son ordre (notation non conventionnelle, à rappeler). Si  $G$  est un ensemble fini, on appelle ordre de  $G$  le cardinal de  $G$ .

**Proposition 16.** Soit  $(G, \star)$  un groupe et  $x \in G$  avec  $x$  d'ordre fini. Pour  $m \in \mathbb{Z}$ , on a

$$x^m = e \iff o(x) \mid m$$

*Démonstration.* Soit  $\varphi : \mathbb{Z} \rightarrow \langle x \rangle, k \mapsto x^k$ . C'est un morphisme et on a  $o(x) = \min \text{Ker } \varphi \cap \mathbb{N}^*$  d'où  $\text{Ker } \varphi = o(x)\mathbb{Z}$  d'après la preuve décrivant les sous-groupes de  $\mathbb{Z}$ . Le résultat suit.  $\square$

**Théorème 12.** Soit  $(G, \star)$  un groupe et  $x \in G$  avec  $x$  d'ordre fini. On a

$$o(x) = \text{Card } \langle x \rangle \quad \text{et} \quad \langle x \rangle \simeq \mathbb{Z}/o(x)\mathbb{Z}$$

*Démonstration.* Soit  $\varphi : \mathbb{Z} \rightarrow \langle x \rangle, k \mapsto x^k$ . C'est un morphisme et on a  $\text{Ker } \varphi = o(x)\mathbb{Z}$ . En procédant comme dans la preuve du théorème 11, on définit  $\bar{\varphi} : \mathbb{Z}/o(x)\mathbb{Z} \rightarrow \langle x \rangle, \bar{k} \mapsto x^\ell$  avec  $\ell \in \bar{k}$ . Cette application est alors un isomorphisme d'où le résultat.  $\square$

## 2 Cas d'un groupe fini

**Théorème 13.** Soit  $(G, \star)$  un groupe fini de cardinal  $n$ . Alors, on a  $x^n = e$  pour tout  $x \in G$ .

*Démonstration.* On suppose  $G$  commutatif (cas général hors-programme). Pour  $x \in G$ , l'application  $a \mapsto a \star x$  est bijective d'où

$$\prod_{a \in G} a = \prod_{a \in G} (a \star x) = x^n \star \prod_{a \in G} a \implies x^n = e$$

Le cas d'un groupe quelconque est prouvé en annexe. □

**Remarque :** On en déduit notamment que tout élément d'un groupe fini est d'ordre fini.

**Corollaire 2.** Soit  $(G, \star)$  un groupe fini de cardinal  $n$ . Alors, on a  $o(x) | n$  pour tout  $x \in G$ .

*Démonstration.* D'après le théorème précédent, on a  $x^n = e$  et d'après la proposition 16, il vient  $o(x) | n$ . □

## VI Groupe symétrique

Dans cette partie,  $n$  désigne un entier non nul.

### 1 Définitions

**Proposition 17.** Soit  $E$  un ensemble non vide. L'ensemble des permutations de  $E$  (ou bijections de  $E$  dans  $E$ ) noté  $S(E)$  muni de la loi de composition a une structure de groupe.

*Démonstration.* La loi  $\circ$  est interne puisqu'une composée de bijections est une bijection, elle est associative d'élément neutre  $\text{id}$  et tout élément  $\sigma \in S(E)$  admet un symétrique  $\sigma^{-1}$  à droite et à gauche. □

**Définition 17.** Soit  $E$  un ensemble non vide. Le groupe  $(S(E), \circ)$  est appelé groupe symétrique de  $E$ . Pour  $n$  entier non nul, on note  $(S_n, \circ)$  le groupe  $(S(\llbracket 1; n \rrbracket), \circ)$  appelé groupe symétrique d'ordre  $n$ .

**Proposition 18.** Soit  $E$  un ensemble fini non vide de cardinal  $n$ . Les groupes  $(S(E), \circ)$  et  $(S_n, \circ)$  sont isomorphes.

*Démonstration.* On note  $E = \{x_k, k \in \llbracket 1; n \rrbracket\}$ . Considérons la bijection  $\varphi : \llbracket 1; n \rrbracket \rightarrow E, k \mapsto x_k$ . On pose  $\Phi : S_n \rightarrow S(E), \sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ . L'application  $\Phi$  est un isomorphisme de groupes. Pour  $(\sigma, \tau) \in S_n^2$ , on a

$$\Phi(\sigma \circ \tau) = \varphi \circ \sigma \circ \tau \circ \varphi^{-1} = \varphi \circ \sigma \circ \varphi^{-1} \circ \varphi \circ \tau \circ \varphi^{-1} = \Phi(\sigma) \circ \Phi(\tau)$$

Et, pour  $(\sigma, \gamma) \in S_n \times S(E)$ , on a

$$\gamma = \Phi(\sigma) \iff \gamma = \varphi \circ \sigma \circ \varphi^{-1} \iff \sigma = \varphi^{-1} \circ \gamma \circ \varphi$$

d'où le caractère bijectif. □

**Remarque :** Il suffit donc d'étudier  $(S_n, \circ)$  pour connaître les propriétés de n'importe quel groupe symétrique d'un ensemble fini.

**Notation :** On note  $\sigma$  un élément de  $S_n$  par

$$\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$$

**Définition 18.** Soit  $\sigma \in S_n$ . On appelle support de la permutation  $\sigma$  l'ensemble noté  $\text{supp } \sigma$  défini par

$$\text{supp } \sigma = \{k \in \llbracket 1; n \rrbracket \mid \sigma(k) \neq k\}$$

Les éléments de  $\llbracket 1; n \rrbracket \setminus \text{supp } \sigma$  sont les points fixes de  $\sigma$ .

**Proposition 19.** Soit  $\sigma \in S_n$ . On a  $\sigma(\text{supp } \sigma) \subset \text{supp } \sigma$ .

*Démonstration.* Soit  $k \in \text{supp } \sigma$ . On a  $\sigma(k) \neq k$  d'où  $\sigma(\sigma(k)) \neq \sigma(k)$  par injectivité de  $\sigma$  ce qui prouve  $\sigma(k) \in \text{supp } \sigma$ .  $\square$

**Proposition 20.** Deux permutations à supports disjoints commutent.

*Démonstration.* Soient  $\sigma, \gamma$  deux permutations à supports disjoints et  $x \in \llbracket 1; n \rrbracket$ . Si  $x \notin \text{supp } \sigma \sqcup \text{supp } \gamma$ , alors  $\sigma(\gamma(x)) = x = \gamma(\sigma(x))$ . Si  $x \in \text{supp } \sigma$ , alors on a  $\sigma(x) \in \text{supp } \sigma$  et  $\sigma(\gamma(x)) = \sigma(x) = \gamma(\sigma(x))$  et de même pour  $x \in \text{supp } \gamma$  par symétrie des rôles.  $\square$

**Théorème 14.** On a  $\text{Card } S_n = n!$

*Démonstration.* On procède par récurrence. L'initialisation est immédiate. On écrit

$$S_n = \bigsqcup_{k=1}^n \{\sigma \in S_n \mid \sigma(n) = k\}$$

Soit  $k \in \llbracket 1; n \rrbracket$ . L'application  $\sigma \mapsto \sigma|_{\llbracket 1; n-1 \rrbracket}$  réalise une bijection de  $\{\sigma \in S_n \mid \sigma(n) = k\}$  vers  $B_{n,k}$ , ensemble des bijections de  $\llbracket 1; n-1 \rrbracket$  dans  $\llbracket 1; n \rrbracket \setminus \{k\}$ . Les ensembles  $\llbracket 1; n-1 \rrbracket$  et  $\llbracket 1; n \rrbracket \setminus \{k\}$  sont de même cardinal fini donc il existe  $\varphi : \llbracket 1; n \rrbracket \setminus \{k\} \rightarrow \llbracket 1; n-1 \rrbracket$  bijective. L'application  $\Phi : \tau \mapsto \varphi \circ \tau$  réalise une bijection de l'ensemble  $B_{n,k}$  vers  $S_{n-1}$ . Ainsi

$$\text{Card } \{\sigma \in S_n \mid \sigma(n) = k\} = \text{Card } B_{n,k} = \text{Card } S_{n-1}$$

$$\text{et} \quad \text{Card } S_n = \sum_{k=1}^n \text{Card } \{\sigma \in S_n \mid \sigma(n) = k\} = n \text{ Card } S_{n-1}$$

Le résultat suit.  $\square$

**Remarque :** Le résultat vaut aussi pour  $n = 0$  puisque l'application vide entre  $\emptyset$  et  $\emptyset$  est une permutation de  $\emptyset$ .

## 2 Cycles et transpositions

**Définition 19.** Soit  $p \in \llbracket 2; n \rrbracket$ . Une permutation  $c \in S_n$  est appelée cycle de longueur  $p$  ou  $p$ -cycle s'il existe  $i_1, \dots, i_p$  dans  $\llbracket 1; n \rrbracket$  deux à deux distincts tels que

$$c(i_1) = i_2, \dots, c(i_{p-1}) = i_p, c(i_p) = i_1 \quad \text{et} \quad \forall k \in \llbracket 1; n \rrbracket \setminus \{i_1, \dots, i_p\} \quad c(k) = k$$

On note 
$$c = (i_1 \ \dots \ i_p)$$

**Notations :** Il est d'usage de noter la composée des cycles  $c_1 = (i_1 \ \dots \ i_p)$  et  $c_2 = (j_1 \ \dots \ j_q)$  comme produit

$$c_1 \circ c_2 = c_1 c_2 = (i_1 \ \dots \ i_p) (j_1 \ \dots \ j_q)$$

**Définition 20.** Une transposition est un 2-cycle.

**Remarque :** Une transposition  $(i \ j)$  a pour simple effet d'échanger  $i$  et  $j$ . Elle est son propre inverse.

Le théorème et son corollaire qui suivent sont à redémontrer en cas de besoin.

**Théorème 15.** Pour  $n \geq 3$ , le groupe  $(S_n, \circ)$  n'est pas commutatif.

*Démonstration.* On a  $(1 \ 2)(2 \ 3) = (1 \ 2 \ 3) \neq (1 \ 3 \ 2) = (2 \ 3)(1 \ 2)$

□

**Corollaire 3.** Pour  $n \geq 3$ , le groupe  $(S_n, \circ)$  n'est pas monogène

*Démonstration.* S'il l'était, il serait abélien.

□

**Proposition 21.** Soit  $c = (i_1 \ \dots \ i_p)$  un  $p$ -cycle. On a  
 $\text{supp } c = \{i_1, \dots, i_p\}$

*Démonstration.* Immédiate.

□

**Proposition 22.** L'ordre d'un  $p$ -cycle est  $p$ .

*Démonstration.* Par récurrence, on a  $c^k(i_1) = i_{k+1}$  pour  $k \in \llbracket 0; p-1 \rrbracket$  et  $c^p(i_1) = c(i_p) = i_1$ . Par suite, pour  $k \in \llbracket 1; p \rrbracket$

$$c^p(i_k) = c^p(c^{k-1}(i_1)) = c^{k-1}(c^p(i_1)) = c^{k-1}(i_1) = i_k$$

et  $c^k(i_1) \neq i_1$  pour  $k \in \llbracket 1; p-1 \rrbracket$  d'où le résultat.

□

Les deux propositions qui suivent ne figurent pas officiellement au programme et sont à redémontrer si nécessaire.

**Proposition 23.** Soit  $c = (i_1 \ \dots \ i_p)$  un  $p$ -cycle de  $S_n$ . On a

$$\forall \sigma \in S_n \quad \sigma \circ c \circ \sigma^{-1} = (\sigma(i_1) \ \dots \ \sigma(i_p))$$

*Démonstration.* Soit  $\sigma \in S_n$  et  $\gamma = \sigma \circ c \circ \sigma^{-1}$ . On vérifie que  $\gamma(\sigma(i_k)) = \sigma(i_{k+1})$  pour tout  $k \in \llbracket 1; p-1 \rrbracket$  et  $\gamma(\sigma(i_p)) = \sigma(i_1)$ . Par ailleurs, on a  $\gamma(i) = i$  pour tout  $i \notin \sigma(\text{supp } c)$ .

□

**Vocabulaire :** Soit  $\sigma \in S_n$ . On dit  $\sigma \circ c \circ \sigma^{-1}$  est un *conjugué* de  $c$ .

**Proposition 24.** Les  $p$ -cycles de  $S_n$  sont conjugués.

*Démonstration.* Soit  $c = (i_1 \ \dots \ i_p)$  et  $\gamma = (j_1 \ \dots \ j_p)$  deux  $p$ -cycles. On choisit  $\sigma \in S_n$  telle que  $\sigma(i_k) = j_k$  pour  $k \in \llbracket 1; p \rrbracket$  (choix possible puisque  $\{i_1, \dots, i_p\}$  et  $\{j_1, \dots, j_p\}$  sont en bijection et leurs complémentaires également). D'après le résultat de la proposition précédente, on a  $\gamma = \sigma \circ c \circ \sigma^{-1}$ .

□

**Remarque :** En particulier, les transpositions qui sont des 2-cycles sont conjuguées.

**Théorème 16.** Tout  $p$ -cycle peut se décomposer en produit de  $p-1$  transpositions.

*Démonstration.* On a  $(i_1 \dots i_p) = (i_1 \ i_2) (i_2 \ i_3) \dots (i_{p-1} \ i_p)$

On le prouve par récurrence sur  $p \geq 2$  avec l'égalité

$$(i_1 \dots i_{p+1}) = (i_1 \dots i_p) (i_p \ i_{p+1})$$

□

**Théorème 17.** *Toute permutation de  $S_n$  peut se décomposer en produit d'au plus  $n - 1$  transpositions.*

*Démonstration.* On procède par récurrence. L'initialisation est triviale. Supposons la propriété vraie au rang  $n \geq 1$ . Soit  $\sigma \in S_{n+1}$ . Si  $\sigma(n+1) = n+1$ , alors  $\sigma$  induit une permutation sur  $S_n$  et on lui applique l'hypothèse de récurrence en plongeant les transpositions de  $S_n$  dans  $S_{n+1}$  (en fixant  $n+1$ ). Ainsi, la permutation  $\sigma$  s'écrit comme produit d'au plus  $n - 1$  transpositions. Sinon, on considère  $\gamma = (n+1 \ \sigma(n+1)) \sigma$  qui vérifie l'hypothèse précédente. On conclut avec  $\sigma = (n+1 \ \sigma(n+1)) \gamma$  qui s'écrit comme produit d'au plus  $n - 1 + 1$  transpositions. □

**Théorème 18.** *Toute permutation de  $S_n$  autre que  $\text{id}$  peut se décomposer en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près.*

*Démonstration.* Voir en annexe. □

**Exemple :** Décomposer en produit de cycles la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 6 & 1 & 2 & 3 \end{pmatrix}$$

On trouve

$$\sigma = (1 \ 5) (2 \ 4 \ 6) (3 \ 7)$$

### 3 Signature

**Théorème 19.** *Soit  $n$  entier supérieur ou égal à 2. Il existe un unique morphisme de groupes surjectif  $\varepsilon : (S_n, \circ) \rightarrow (\{1, -1\}, \times)$ .*

*Démonstration.* On note  $\mathcal{P}_{[2]} = \{\{i, j\}, (i, j) \in \llbracket 1; n \rrbracket^2 \text{ et } i \neq j\}$

On pose

$$\forall \sigma \in S_n \quad \forall \{i, j\} \in \mathcal{P}_{[2]} \quad T_\sigma(\{i, j\}) = \frac{\sigma(i) - \sigma(j)}{i - j} \quad \text{et} \quad \varepsilon(\sigma) = \prod_{\{i, j\} \in \mathcal{P}_{[2]}} T_\sigma(\{i, j\})$$

Pour  $\{i, j\} \in \mathcal{P}_{[2]}$ , on a 
$$\frac{\sigma(i) - \sigma(j)}{i - j} = \frac{\sigma(j) - \sigma(i)}{j - i}$$

ce qui justifie que le choix de  $i$  et  $j$  dans  $\{i, j\}$  n'intervient pas. Soit  $(\sigma, \gamma) \in S_n^2$ . On a

$$\begin{aligned} \varepsilon(\sigma \circ \gamma) &= \prod_{\{i, j\} \in \mathcal{P}_{[2]}} T_{\sigma \circ \gamma}(\{i, j\}) = \prod_{\{i, j\} \in \mathcal{P}_{[2]}} [T_\sigma(\{\gamma(i), \gamma(j)\}) T_\gamma(\{i, j\})] \\ &= \left( \prod_{\{i, j\} \in \mathcal{P}_{[2]}} T_\sigma(\{\gamma(i), \gamma(j)\}) \right) \varepsilon(\gamma) \end{aligned}$$

Enfin, l'application  $\mathcal{P}_{[2]} \rightarrow \mathcal{P}_{[2]}, \{i, j\} \mapsto \{\gamma(i), \gamma(j)\}$  est bien définie et clairement bijective.

Ainsi 
$$\prod_{\{i, j\} \in \mathcal{P}_{[2]}} T_\sigma(\{\gamma(i), \gamma(j)\}) = \prod_{\{i, j\} \in \mathcal{P}_{[2]}} T_\sigma(\{i, j\}) = \varepsilon(\sigma)$$

et par conséquent

$$\varepsilon(\sigma \circ \gamma) = \varepsilon(\sigma)\varepsilon(\gamma)$$

Soit  $\{a, b\} \in \mathcal{P}_{[2]}$ . On partitionne  $\mathcal{P}_{[2]}$  en

$$\mathcal{P}_{[2]} = \{a, b\} \sqcup \{\{i, j\} \in \mathcal{P}_{[2]} : \{i, j\} \cap \{a, b\} = \emptyset\} \sqcup \bigsqcup_{j \in \{a, b\}} \{\{i, j\}, i \in \llbracket 1; n \rrbracket \setminus \{a, b\}\}$$

Soit  $\tau = (a \ b)$ . Pour  $\{i, j\} \in \mathcal{P}_{[2]}$  tel que  $\{i, j\} \cap \{a, b\} = \emptyset$ , on a

$$T_\tau(\{i, j\}) = \frac{i-j}{i-j} = 1$$

Il vient alors

$$\varepsilon(\tau) = T_\tau(\{a, b\}) \prod_{i \in \llbracket 1; n \rrbracket \setminus \{a, b\}} [T_\tau(\{i, a\})T_\tau(\{i, b\})] = \frac{b-a}{a-b} \prod_{i \in \llbracket 1; n \rrbracket \setminus \{a, b\}} \left( \frac{i-b}{i-a} \frac{i-a}{i-b} \right) = -1$$

Comme toute permutation s'écrit comme produit de transpositions, il s'ensuit  $\text{Im } \varepsilon \subset \{-1, 1\}$  et l'autre inclusion a lieu puisque  $-1 \in \text{Im } \varepsilon$  et  $1 = \varepsilon(\text{id})$ . Ainsi, l'application  $\varepsilon$  est un morphisme surjectif de  $(S_n, \circ)$  sur  $(\{-1, 1\}, \times)$ . Supposons que  $\varphi$  vérifie les mêmes caractéristiques. Pour  $\tau$  une transposition, on a nécessairement  $\varphi(\tau) = -1$ . Sinon, comme toutes les transpositions sont conjuguées, on aurait  $\varphi(\gamma) = 1$  pour toute transposition  $\gamma$  et comme une permutation s'écrit comme produit de transpositions, on n'aurait pas la surjectivité de  $\varphi$ . Ainsi, pour  $\sigma = \prod_{i=1}^p \tau_i$  avec les  $\tau_i$  des transpositions, on a

$$\varepsilon(\sigma) = \varepsilon\left(\prod_{i=1}^p \tau_i\right) = (-1)^p = \varphi\left(\prod_{i=1}^p \tau_i\right) = \varphi(\sigma)$$

ce qui prouve l'unicité.  $\square$

**Remarque :** Pour établir  $\text{Im } \varepsilon \subset \{-1, 1\}$ , on peut utiliser un résultat moins fort que la décomposition d'une permutation en produit de transpositions en observant simplement que  $|\varepsilon(\sigma)| = 1$  pour tout  $\sigma \in S_n$ .

**Proposition 25.** Soit  $n$  entier supérieur ou égal à 2. On a

$$\forall \sigma \in S_n \quad \varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

*Démonstration.* On note  $\Delta = \{(i, j) \in \llbracket 1; n \rrbracket^2 : i < j\}$ . L'application  $\varphi : \Delta \rightarrow \mathcal{P}_{[2]}, (i, j) \mapsto \{i, j\}$  réalise une bijection. En effet, c'est une application bien définie et pour  $(i, j) \in \Delta$  et  $L \in \mathcal{P}_{[2]}$ , on a

$$\varphi(i, j) = L \iff (i, j) = (\min L, \max L)$$

Pour  $\sigma \in S_n$ , il vient

$$\varepsilon(\sigma) = \prod_{L \in \mathcal{P}_{[2]}} T_\sigma(L) \stackrel{=}{=} \prod_{\substack{L = \varphi(i, j) \\ (i, j) \in \Delta}} T_\sigma(\varphi(i, j)) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

$\square$

**Remarque :** On en déduit la relation

$$\forall \sigma \in S_n \quad \prod_{1 \leq i < j \leq n} (\sigma(i) - \sigma(j)) = \varepsilon(\sigma) \prod_{1 \leq i < j \leq n} (i - j)$$

**Définition 21.** Soit  $n$  entier supérieur ou égal à 2. L'unique morphisme de groupes surjectif  $\varepsilon : (S_n, \circ) \rightarrow (\{1, -1\}, \times)$  est appelé signature sur  $S_n$ .

**Définition 22.** Soit  $n$  entier supérieur ou égal à 2. Le sous-groupe  $A_n = \text{Ker } \varepsilon$  de  $(S_n, \circ)$  est appelé groupe alterné d'ordre  $n$ .

**Remarque :** Soit  $\tau$  une transposition. L'application  $\sigma \mapsto \sigma \circ \tau$  réalise une bijection de  $A_n$  sur  $S_n \setminus A_n$ . On en déduit

$$\text{Card } A_n = \frac{n!}{2}$$

**Proposition 26.** Un  $p$ -cycle a pour signature  $(-1)^{p-1}$ .

*Démonstration.* On a  $c = (i_1 \ \dots \ i_p) = (i_1 \ i_2) (i_2 \ i_3) \dots (i_{p-1} \ i_p)$

d'où  $\varepsilon(c) = \prod_{k=1}^{p-1} \varepsilon((i_k \ i_{k+1})) = (-1)^{p-1}$

□

**Exemple :** On a  $A_3 = \langle (1 \ 2 \ 3) \rangle$ .

## Annexe

**Théorème 1 (Théorème de la division euclidienne).** Soit  $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{N} \times \llbracket 0; b-1 \rrbracket$  tel que

$$a = bq + r$$

Soit  $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{Z} \times \llbracket 0; |b| - 1 \rrbracket$  tel que

$$a = bq + r$$

*Démonstration.* Soit  $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ . On pose  $q' = \left\lfloor \frac{a}{|b|} \right\rfloor$  et  $r = a - |b|q'$ . On a

$$q' \leq \frac{a}{|b|} < q' + 1$$

et en multipliant par  $|b| > 0$ , il vient  $0 \leq a - q'|b| < |b|$

Si  $b > 0$ , on choisit  $q = q'$  et si  $b < 0$ , on choisit  $q = -q'$  et ceci prouve l'existence puisque  $r = a - bq$ . Si  $(q', r') \in \mathbb{Z} \times \llbracket 0; |b| - 1 \rrbracket$  vérifie  $a = b'q + r'$ , alors

$$b(q - q') = r' - r \in \llbracket -( |b| - 1 ); |b| - 1 \rrbracket$$

et comme  $b(q - q')$  est un multiple de  $|b|$ , il s'ensuit  $q = q'$  puis  $r = r'$ .  $\square$

**Remarque :** Sans recours à la partie entière, on considère  $A = \{a - |b|k, k \in \mathbb{Z}\} \cap \mathbb{N}$  qui est une partie non vide de  $\mathbb{N}$  puisque  $\{a - |b|k, k \in \mathbb{Z}\}$  contient  $a$  et  $a - |b|a = -a(|b| - 1)$  et que l'un des deux est un entier naturel. On choisit  $r$  le minimum de  $A$ ,  $q'$  entier relatif tel que  $r = a - |b|q'$  et  $q = \text{sgn}(b)q'$ .

On présente le théorème de Lagrange dont un corollaire permet d'établir le théorème 13 sans l'hypothèse restrictive de commutativité du groupe.

**Théorème 2 (Théorème de Lagrange).** Soit  $G$  un groupe fini et  $H$  un sous groupe de  $G$ . Alors, on a

$$\text{Card } H \mid \text{Card } G$$

*Démonstration.* On définit une relation binaire pour  $(x, y) \in G^2$  par

$$x\mathcal{R}y \iff y \in xH = \{x \star h, h \in H\}$$

Soit  $(x, y, z) \in G^3$ . On a  $x = x \star e \in xH$  puis si  $x\mathcal{R}y$  alors il existe  $h \in H$  tel que  $y = x \star h$  d'où  $x = y \star h^{-1}$ , i.e.  $y\mathcal{R}x$  et si  $y\mathcal{R}z$ , il existe  $k \in H$  tel que  $z = y \star k$  d'où  $z = (x \star h) \star k = x \star (h \star k)$  donc  $x\mathcal{R}z$ . Ainsi, la relation  $\mathcal{R}$  est une relation d'équivalence. Les classes d'équivalence pour cette relation forment une partition de  $G$ . Considérons des représentants de ces classes qu'on

note  $x_1, \dots, x_p$ . On a donc l'union disjointe  $G = \bigsqcup_{i=1}^p x_iH$ . Enfin, pour  $x \in G$ , l'application  $h \mapsto x \star h$  est une bijection de  $H$  vers  $xH$ . Ainsi

$$\text{Card } G = \sum_{i=1}^p \text{Card } x_iH = \sum_{i=1}^p \text{Card } H = p \text{Card } H$$

$\square$

**Remarque :** Notant  $G/H$  l'ensemble des classes d'équivalence de la relation  $\mathcal{R}$ , on a appliqué le lemme des bergers à l'application  $\pi : G \rightarrow G/H, x \mapsto xH$ .

**Corollaire 4.** Soit  $G$  un groupe fini de cardinal  $n$ . Alors, on a  $o(x)|n$  pour tout  $x \in G$ .

*Démonstration.* Soit  $x \in G$ . D'après le théorème de Lagrange, on a

$$o(x) = \text{Card } \langle x \rangle \mid \text{Card } G = n$$

□

Enfin, on se propose de montrer par récurrence le théorème 18. On utilisera sans réserve le lemme suivant :

**Lemme 1.** Soit  $\sigma \in S_n$  et  $\sigma = \prod_{k=1}^r c_k$  une décomposition en produit de cycles à supports disjoints. Alors les permutations  $\sigma$  et  $c_k$  coïncident sur  $\text{supp } c_k$  pour tout  $k \in \llbracket 1; r \rrbracket$ .

*Démonstration.* Immédiate.

□

**Proposition 27.** Soit  $c \in S_n$  un cycle et  $x \in \text{supp } c$ . On note  $p = \min \{k \in \mathbb{N}^* \mid c^k(x) = x\}$ . On a

$$c = (x \ c(x) \ \dots \ c^{p-1}(x))$$

*Démonstration.* Par définition, on dispose de  $i_1, \dots, i_q$  avec  $q \geq 2$  dans  $\llbracket 1; n \rrbracket$  deux à deux distincts tels que  $c = (i_1 \ \dots \ i_q)$ . On note  $a = i_1$  et une récurrence immédiate donne  $i_k = c^k(a)$  pour tout  $k \in \llbracket 0; q-1 \rrbracket$ . Ainsi, on a

$$c = (a \ c(a) \ \dots \ c^{q-1}(a)) \quad \text{et} \quad \text{supp } c = \{a, c(a), \dots, c^{q-1}(a)\}$$

On dispose alors de  $\ell \in \llbracket 0; q-1 \rrbracket$  tel que  $x = c^\ell(a)$ . On note

$$\Lambda = \{c^k(x), k \in \mathbb{N}\}$$

Le support d'une permutation est stable par celle-ci d'où  $\Lambda \subset \text{supp } c$ . Par ailleurs, on a

$$c^{q-\ell}(x) = c^{q-\ell+\ell}(a) = c^q(a) = a \in \Lambda$$

et comme  $c(\Lambda) \subset \Lambda$ , il s'ensuit  $\text{supp } c \subset \Lambda$  d'où  $\Lambda = \text{supp } c$ . Pour  $k \in \mathbb{N}$ , on dispose de  $(q, r) \in \mathbb{N} \times \llbracket 0; p-1 \rrbracket$  tel que  $k = pq + r$  par division euclidienne d'où

$$c^k(x) = c^r(c^{pq}(x)) = c^r(x)$$

ce qui prouve

$$\Lambda \subset \{c^k(x), k \in \llbracket 0; p-1 \rrbracket\}$$

et l'autre inclusion est immédiate. S'il existe  $0 \leq k < k' \leq p-1$  tel que  $c^k(x) = c^{k'}(x)$ , alors on a  $c^{k'-k}(x) = x$  avec  $k' - k \in \llbracket 0; p-1 \rrbracket$  ce qui contredit la minimalité de  $p$ . On en déduit  $\text{Card } \Lambda = p$  et par conséquent  $p = q$ . Notant  $\gamma = (x \ c(x) \ \dots \ c^{q-1}(x))$ , on a

$$\forall k \in \llbracket 0; q-1 \rrbracket \quad c(\gamma^k(x)) = c(c^k(x)) = c^{k+1}(x) = \gamma(\gamma^k(x))$$

ce qui prouve que  $c$  et  $\gamma$  coïncident sur  $\text{supp } \gamma = \Lambda = \text{supp } c$  d'où le résultat.

□

**Proposition 28.** Soit  $\sigma \in S_n$  et  $x \in \llbracket 1; n \rrbracket$ . On a

$$x \in \text{supp } \sigma \iff \sigma(x) \in \text{supp } \sigma$$

*Démonstration.* Le sens direct découle de l'injectivité de  $\sigma$  et le sens indirect de l'injectivité de  $\sigma^{-1}$ .

□

**Théorème 18.** Toute permutation de  $S_n$  autre que  $\text{id}$  peut se décomposer en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près.

*Démonstration.* On procède par récurrence sur  $n$ . Le cas  $n = 1$  est trivial. On suppose l'existence vraie au rang  $n \geq 1$ . Soit  $\sigma \in S_{n+1}$ . Si  $\sigma(n+1) = n+1$ , alors  $\sigma$  induit une permutation de  $S_n$  qui admet une décomposition en produit de cycles à supports disjoints par hypothèse de récurrence. On suppose ensuite  $\sigma(n+1) \neq n+1$ . La permutation  $(n+1 \ \sigma(n+1)) \sigma$  fixe  $n+1$  et admet donc une décomposition en produit de cycles à supports disjoints  $\prod_{k=1}^r c_k$ . Si  $n+1 \notin \bigcup_{k=1}^r \text{supp } c_k$ , alors  $\sigma(n+1) \notin \bigcup_{k=1}^r \text{supp } c_k$  d'après la proposition 28 et la décomposition

$$\sigma = (n+1 \ \sigma(n+1)) \prod_{k=1}^r c_k$$

est une décomposition en produit de cycles à supports disjoints. Si  $n+1 \in \bigcup_{k=1}^r \text{supp } c_k$ , alors il existe un unique  $k_0 \in \llbracket 1; r \rrbracket$  tel que  $c_{k_0} = (n+1 \ \dots \ \sigma^{p-1}(n+1))$  d'après la proposition 27. On en déduit

$$(n+1 \ \sigma(n+1)) (n+1 \ \dots \ \sigma^{p-1}(n+1)) = (\sigma(n+1) \ \dots \ \sigma^{p-1}(n+1))$$

d'où

$$\sigma = (\sigma(n+1) \ \dots \ \sigma^{p-1}(n+1)) \prod_{k \in \llbracket 1; r \rrbracket \setminus \{k_0\}} c_k$$

qui est une décomposition de  $\sigma$  en produit de cycles à supports disjoints. On suppose l'unicité à l'ordre près vraie jusqu'au rang  $n \geq 1$  (récurrence forte). Soit  $\sigma \in S_{n+1}$ . Si  $\sigma(n+1) = n+1$ , alors  $\sigma$  induit une permutation de  $S_n$  et se décompose de manière unique à l'ordre près par hypothèse de récurrence. Sinon, on considère deux décompositions en produit de cycles à supports disjoints :

$$\sigma = \prod_{i=1}^s \gamma_i = \prod_{k=1}^r c_k$$

On dispose d'un unique  $i_0 \in \llbracket 1; s \rrbracket$  et  $k_0 \in \llbracket 1; r \rrbracket$  tels que  $n+1 \in \text{supp } \gamma_{i_0}$  et  $n+1 \in \text{supp } c_{k_0}$ . Ainsi, d'après la proposition 27, on a

$$\gamma_{i_0} = (n+1 \ \dots \ \sigma^{p-1}(n+1)) \quad \text{et} \quad c_{k_0} = (n+1 \ \dots \ \sigma^{q-1}(n+1))$$

avec  $p$  et  $q \geq 2$ . On a

$$p = \min \{k \in \mathbb{N}^* \mid \gamma_{i_0}^k(n+1) = n+1\} = \min \{k \in \mathbb{N}^* \mid \sigma^k(n+1) = n+1\}$$

puisque  $\sigma$  et  $\gamma_{i_0}$  coïncident sur  $\text{supp } \gamma_{i_0}$  et de même avec  $c_{k_0}$  d'où  $p = q$ . Ainsi, on trouve après simplification

$$\prod_{i \in \llbracket 1; s \rrbracket \setminus \{i_0\}} \gamma_i = \prod_{k \in \llbracket 1; r \rrbracket \setminus \{k_0\}} c_k$$

et on conclut par hypothèse de récurrence. □

**Remarque :** La plupart des preuves qu'on trouve dans la littérature sont constructives : on construit les cycles concernés à partir d'une permutation en considérant les *orbites*. La preuve qui précède permet de varier un peu ...