الكلية متعددة التخصصات الناظور
Faculté Pluridisciplinaire de Nador

Cours d'algèbre 1 (M.I.P)

Chapitre 5 : Groupes

(Ce document ne peut en aucun cas remplacer les séances de cours en présentiel)

Pr. EL MEHDI BOUBA

Année universitaire :2023–2024

5. **Groupes**

5.1. **Groupe.**

5.1.1. *Définition.*

Définition 5.1. Un **groupe** $(G,\star)$ est un ensemble G auquel est associé une opération $\star$ (la **loi de composition**) vérifiant les quatre propriétés suivantes :

(1) pour tout $x,y \in G$, $\quad x \star y \in G \quad$ ($\star$ est une **loi de composition interne**)
(2) pour tout $x,y,z \in G$, $\quad (x \star y) \star z = x \star (y \star z) \quad$ (la loi est **associative**)
(3) il existe $e \in G$ tel que $\quad \forall x \in G,\ x \star e = x$ et $e \star x = x \quad$ (e est l'**élément neutre**)
(4) pour tout $x \in G$ il existe $x' \in G$ tel que $\quad x \star x' = x' \star x = e \quad$ (x' est l'**inverse** de x et est noté x^{-1})

Si de plus l'opération vérifie

$$\text{pour tout } x,y \in G, \qquad x \star y = y \star x,$$

on dit que G est un groupe **commutatif** (ou **abélien**).

Remarque 5.2.

- L'élément neutre e est unique. En effet si e' vérifie aussi le point (3), alors on a $e' \star e = e$ (car e est élément neutre) et $e' \star e = e'$ (car e' aussi). Donc $e = e'$. Remarquez aussi que l'inverse de l'élément neutre est lui-même. S'il y a plusieurs groupes, on pourra noter e_G pour l'élément neutre du groupe G.
- Un élément $x \in G$ ne possède qu'un seul inverse. En effet si x' et x'' vérifient tous les deux le point (4) alors on a $x \star x'' = e$ donc $x' \star (x \star x'') = x' \star e$. Par l'associativité (2) et la propriété de l'élément neutre (3) alors $(x' \star x) \star x'' = x'$. Mais $x' \star x = e$ donc $e \star x'' = x'$ et ainsi $x'' = x'$.

Exemples 24. Voici des ensembles bien connus pour lesquels l'opération donnée définit une structure de groupe.

- $(\mathbb{R}^*,\times)$ est un groupe commutatif, $\times$ est la multiplication habituelle. Vérifions chacune des propriétés :
  (1) Si $x,y \in \mathbb{R}^*$ alors $x \times y \in \mathbb{R}^*$.
  (2) Pour tout $x,y,z \in \mathbb{R}^*$ alors $x \times (y \times z) = (x \times y) \times z$, c'est l'associativité de la multiplication des nombres réels.
  (3) 1 est l'élément neutre pour la multiplication, en effet $1 \times x = x$ et $x \times 1 = x$, ceci quelque soit $x \in \mathbb{R}^*$.
  (4) L'inverse d'un élément $x \in \mathbb{R}^*$ est $x' = \frac{1}{x}$ (car $x \times \frac{1}{x}$ est bien égal à l'élément neutre 1). L'inverse de x est donc $x^{-1} = \frac{1}{x}$. Notons au passage que nous avions exclu 0 de notre groupe, car il n'a pas d'inverse.
  Ces propriétés font de $(\mathbb{R}^*,\times)$ un groupe.
  (5) Enfin $x \times y = y \times x$, c'est la commutativité de la multiplication des réels.
- $(\mathbb{Q}^*,\times)$, $(\mathbb{C}^*,\times)$ sont des groupes commutatifs.
- $(\mathbb{Z},+)$ est un groupe commutatif. Ici $+$ est l'addition habituelle.

(1) Si $x,y \in \mathbb{Z}$ alors $x+y \in \mathbb{Z}$.
(2) Pour tout $x,y,z \in \mathbb{Z}$ alors $x+(y+z) = (x+y)+z$.
(3) 0 est l'élément neutre pour l'addition, en effet $0+x = x$ et $x+0 = x$, ceci quelque soit $x \in \mathbb{Z}$.
(4) L'inverse d'un élément $x \in \mathbb{Z}$ est $x' = -x$ car $x+(-x) = 0$ est bien l'élément neutre 0. Quand la loi de groupe est $+$ l'inverse s'appelle plus couramment l'**opposé**.
(5) Enfin $x+y = y+x$, et donc $(\mathbb{Z},+)$ est un groupe commutatif.

- $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ sont des groupes commutatifs.
- L'ensemble $\mathcal{S}(E)$ des bijections d'un ensemble E non vide muni de la composition des applications : $f \circ g : E \to E$, $x \to f \circ g(x) = f(g(x))$. est un groupe d'élement neutre $\mathrm{id}_E : E \to E$, $x \to x$. Ce groupe n'est pas commutatif dès que $\mathrm{card}(E) \geq 3$.

Voici deux exemples qui **ne sont pas** des groupes :

- $(\mathbb{Z}^*,\times)$ n'est pas un groupe. Car si 2 avait un inverse (pour la multiplication $\times$) ce serait $\frac{1}{2}$ qui n'est pas un entier.
- $(\mathbb{N},+)$ n'est pas un groupe. En effet l'inverse de 3 (pour l'addition $+$) devrait être -3 mais $-3 \notin \mathbb{N}$.

5.1.2. *Puissance.*
Revenons à un groupe $(G,\star)$. Pour $x \in G$ nous noterons $x \star x$ par x^2 et $x \star x \star x$ par x^3.

Plus généralement nous noterons :

- $x^n = \underbrace{x \star x \star \cdots \star x}_{n \text{ fois}}$,
- $x^0 = e$,
- $x^{-n} = \underbrace{x^{-1} \star \cdots \star x^{-1}}_{n \text{ fois}}$.

Rappelez-vous que x^{-1} désigne l'inverse de x dans le groupe.

Les règles de calcul sont les mêmes que pour les puissances des nombres réels. Pour $x,y \in G$ et $m,n \in \mathbb{Z}$ nous avons :

- $x^m \star x^n = x^{m+n}$,
- $(x^m)^n = x^{mn}$,
- $(x \star y)^{-1} = y^{-1} \star x^{-1}$, attention à l'ordre !
- **Si** $(G,\star)$ est **commutatif** alors $(x \star y)^n = x^n \star y^n$.

5.2. **Sous-groupes.**
Montrer qu'un ensemble est un groupe à partir de la définition peut être assez long. Il existe une autre technique, c'est de montrer qu'un sous-ensemble d'un groupe est lui-même un groupe : c'est la notion de sous-groupe.

5.2.1. *Définition.*
Soit $(G,\star)$ un groupe.

Définition 5.3. Une partie $H \subset G$ est un **sous-groupe** de G si :

- $e \in H$,
- pour tout $x, y \in H$, on a $x \star y \in H$,
- pour tout $x \in H$, on a $x^{-1} \in H$.

Notez qu'un sous-groupe H est aussi un groupe $(H,\star)$ avec la loi induite par celle de G.

Par exemple si $x \in H$ alors, pour tout $n \in \mathbb{Z}$, nous avons $x^n \in H$.

Remarque 5.4. Un critère pratique et plus rapide pour prouver que H est un sous-groupe de G est :

- H contient au moins un élément
- pour tout $x,y \in H$, $x \star y^{-1} \in H$.

Exemples 25.

- $(\mathbb{R}_+^*,\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$. En effet :
  - $1 \in \mathbb{R}_+^*$,
  - si $x,y \in \mathbb{R}_+^*$ alors $x \times y \in \mathbb{R}_+^*$,
  - si $x \in \mathbb{R}_+^*$ alors $x^{-1} = \frac{1}{x} \in \mathbb{R}_+^*$.
- $(\mathbb{U},\times)$ est un sous-groupe de $(\mathbb{C}^*,\times)$, où $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.
- $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{R},+)$.
- $\{e\}$ et G sont les **sous-groupes triviaux** du groupe G.
- Si H et K sont des sous groupes de G, alors $H \cap K$ est un sous-groupe de G.
- Si H et K sont deux sous-groupes de G, alors, en général, $H \cup K$ n'est pas un sous-groupe de G. Soient, par exemple, $H = \{(x, y) \in \mathbb{R}^2/x = 0\}$ et $K = \{(x, y) \in \mathbb{R}^2/y = 0\}$. Il est évident que H et K sont deux sous-groupes du groupe additif de $\mathbb{R}^2$. Cependant, $H \cup K$ n'est pas un sous-groupe de $\mathbb{R}^2$ car on a par exemple $(1,0) + (0,1) = (1,1) \notin H \cup K$.

Exercice 5.5. Soient H et K deux sous-groupes d'un groupe G. Montrer que $H \cup K$ est un sous-groupe de G si, et seulement si, $H \subset K$ ou $K \subset H$.

5.2.2. *Sous-groupes de* $\mathbb{Z}$.

Proposition 5.1. *Les sous-groupes de* $(\mathbb{Z},+)$ *sont les* $n\mathbb{Z}$, *pour* $n \in \mathbb{Z}$.

L'ensemble $n\mathbb{Z}$ désigne l'ensemble des multiples de n :

$$n\mathbb{Z} = \left\{ k \cdot n \mid k \in \mathbb{Z} \right\}.$$

Par exemple :

- $2\mathbb{Z} = \{\ldots, -4, -2,0,2,4,6, \ldots\}$ est l'ensemble des entiers pairs,
- $7\mathbb{Z} = \{\ldots, -14, -7,0,7,14,21, \ldots\}$ est l'ensemble des multiples de 7.

Preuve. Fixons $n \in \mathbb{Z}$. L'ensemble $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$, en effet :

- $n\mathbb{Z} \subset \mathbb{Z}$,
- l'élément neutre 0 appartient à $n\mathbb{Z}$,

- pour $x = kn$ et $y = k'n$ des éléments de $n\mathbb{Z}$ alors $x + y = (k + k')n$ est aussi un élément de $n\mathbb{Z}$,
- enfin si $x = kn$ est un élément de $n\mathbb{Z}$ alors $-x = (-k)n$ est aussi un élément de $n\mathbb{Z}$.

Réciproquement soit H un sous-groupe de $(\mathbb{Z},+)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$ et c'est fini. Sinon H contient au moins un élément non-nul et positif (puisque tout élément est accompagné de son opposé) et notons

$$n = \min\big\{h > 0 \mid h \in H\big\}.$$

Alors $n > 0$. Comme $n \in H$ alors $-n \in H$, $2n = n + n \in H$, et plus généralement pour $k \in \mathbb{Z}$ alors $kn \in H$. Ainsi $n\mathbb{Z} \subset H$. Nous allons maintenant montrer l'inclusion inverse. Soit $h \in H$. Écrivons la division euclidienne :

$$h = kn + r, \qquad \text{avec } k,r \in \mathbb{Z} \text{ et } 0 \leq r < n.$$

Mais $h \in H$ et $kn \in H$ donc $r = h - kn \in H$. Nous avons un entier $r \geq 0$ qui est un élément de H et strictement plus petit que n. Par la définition de n, nécessairement $r = 0$. Autrement dit $h = kn$ et donc $h \in n\mathbb{Z}$. Conclusion $H = n\mathbb{Z}$. □

5.2.3. *Sous-groupes engendrés.*

Soit $(G,\star)$ un groupe et $E \subset G$ un sous-ensemble de G. Le **sous-groupe engendré** par E est le plus petit sous-groupe de G contenant E.

Par exemple si $E = \{2\}$ et le groupe est $(\mathbb{R}^*,\times)$, le sous-groupe engendré par E est $H = \{2^n \mid n \in \mathbb{Z}\}$. Pour le prouver : il faut montrer que H est un sous-groupe, que $2 \in H$, et que si H' est un autre sous-groupe contenant 2 alors $H \subset H'$.

Autre exemple avec le groupe $(\mathbb{Z},+)$: si $E_1 = \{2\}$ alors le sous-groupe engendré par E_1 est $H_1 = 2\mathbb{Z}$. Si $E_2 = \{8,12\}$ alors $H_2 = 4\mathbb{Z}$ et plus généralement si $E = \{a,b\}$ alors $H = n\mathbb{Z}$ où $n = \operatorname{pgcd}(a,b)$.

5.3. **Morphismes de groupes.**

5.3.1. *Définition et Propriétés.*

Définition 5.6. Soient $(G,\star)$ et $(G',\diamond)$ deux groupes. Une application $f : G \longrightarrow G'$ est un **morphisme de groupes** si :

$$\boxed{\text{pour tout } x,x' \in G \qquad f(x \star x') = f(x) \diamond f(x').}$$

L'exemple que vous connaissez déjà est le suivant : soit G le groupe $(\mathbb{R},+)$ et G' le groupe $(\mathbb{R}_+^*,\times)$. Soit $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ l'application exponentielle définie par $f(x) = \exp(x)$. Nous avons bien

$$f(x + x') = \exp(x + x') = \exp(x) \times \exp(x') = f(x) \times f(x').$$

Et donc f est bien un morphisme de groupes.

Proposition 5.2. *Soit $f : G \longrightarrow G'$ un morphisme de groupes alors :*

- $f(e_G) = e_{G'}$,
- *pour tout $x \in G$, $f(x^{-1}) = \big(f(x)\big)^{-1}$.*

Il faut faire attention à l'ensemble auquel appartiennent les éléments considérés : e_G est l'élément neutre de G, $e_{G'}$ celui de G'. Il n'y a pas de raison qu'ils soient égaux (ils ne sont même pas dans le même ensemble). Aussi x^{-1} est l'inverse de x dans G, alors que $\big(f(x)\big)^{-1}$ est l'inverse de $f(x)$ mais dans G'.

Reprenons l'exemple de la fonction $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ définie par $f(x) = \exp(x)$. Nous avons bien $f(0) = 1$: l'élément neutre de $(\mathbb{R},+)$ a pour image l'élément neutre de $(\mathbb{R}_+^*,\times)$. Pour $x \in \mathbb{R}$ son inverse dans $(\mathbb{R},+)$ est ici son opposé $-x$, alors $f(-x) = \exp(-x) = \frac{1}{\exp(x)} = \frac{1}{f(x)}$ est bien l'inverse (dans $(\mathbb{R}_+^*,\times)$) de $f(x)$.

Preuve.

- $f(e_G) = f(e_G \star e_G) = f(e_G) \diamond f(e_G)$, en multipliant (à droite par exemple) par $f(e_G)^{-1}$ on obtient $e_{G'} = f(e_G)$.
- Soit $x \in G$ alors $x \star x^{-1} = e_G$ donc $f(x \star x^{-1}) = f(e_G)$. Cela entraîne $f(x) \diamond f(x^{-1}) = e_{G'}$, en composant à gauche par $\big(f(x)\big)^{-1}$, nous obtenons $f(x^{-1}) = \big(f(x)\big)^{-1}$.

□

Proposition 5.3.

- *Soient deux morphismes de groupes $f : G \longrightarrow G'$ et $g : G' \longrightarrow G''$. Alors $g \circ f : G \longrightarrow G''$ est un morphisme de groupes.*
- *Si $f : G \longrightarrow G'$ est un morphisme bijectif alors $f^{-1} : G' \longrightarrow G$ est aussi un morphisme de groupes.*

Preuve. La première partie est facile. Montrons la deuxième : Soit $y,y' \in G'$. Comme f est bijective, il existe $x,x' \in G$ tels que $f(x) = y$ et $f(x') = y'$. Alors $f^{-1}(y \diamond y') = f^{-1}\big(f(x) \diamond f(x')\big) = f^{-1}\big(f(x \star x')\big) = x \star x' = f^{-1}(y) \star f^{-1}(y')$. Et donc f^{-1} est un morphisme de G' vers G. □

Définition 5.7. Un morphisme bijectif est un **isomorphisme**. Deux groupes G, G' sont **isomorphes** s'il existe un morphisme bijectif $f : G \longrightarrow G'$.

Continuons notre exemple $f(x) = \exp(x)$, $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ est une application bijective. Sa bijection réciproque $f^{-1} : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ est définie par $f^{-1}(x) = \ln(x)$. Par la proposition 5.3 nous savons que f^{-1} est aussi un morphisme (de $(\mathbb{R}_+^*,\times)$ vers $(\mathbb{R},+)$) donc $f^{-1}(x \times x') = f^{-1}(x) + f^{-1}(x')$. Ce qui s'exprime ici par la formule bien connue :

$$\ln(x \times x') = \ln(x) + \ln(x').$$

Ainsi f est un isomorphisme et les groupes $(\mathbb{R},+)$ et $(\mathbb{R}_+^*,\times)$ sont isomorphes.

5.3.2. *Noyau et image.*

Soit $f : G \longrightarrow G'$ un morphisme de groupes. Nous définissons deux sous-ensembles importants qui vont être des sous-groupes.

Définition 5.8. Le **noyau** de f est

$$\boxed{Ker f = \big\{x \in G \mid f(x) = e_{G'}\big\}}$$

C'est donc un sous-ensemble de G. En terme d'image réciproque nous avons par définition $Ker f = f^{-1}\big(\{e_{G'}\}\big)$. (Attention, la notation f^{-1} ici désigne l'image réciproque, et ne signifie pas que f est bijective.) Le noyau est donc l'ensemble des éléments de G qui s'envoient par f sur l'élément neutre de G'.

Définition 5.9. L'**image** de f est

$$\boxed{Im f = \big\{f(x) \mid x \in G\big\}}$$

C'est donc un sous-ensemble de G' et en terme d'image directe nous avons $Im f = f(G)$. Ce sont les éléments de G' qui ont (au moins) un antécédent par f.

Proposition 5.4. *Soit $f : G \longrightarrow G'$ un morphisme de groupes.*

(1) $Ker f$ est un sous-groupe de G.
(2) $Im f$ est un sous-groupe de G'.
(3) f est injectif si et seulement si $Ker f = \{e_G\}$.
(4) f est surjectif si et seulement si $Im f = G'$.

Preuve.

(1) Montrons que le noyau est un sous-groupe de G.
   (a) $f(e_G) = e_{G'}$ donc $e_G \in Ker f$.
   (b) Soient $x,x' \in Ker f$. Alors $f(x \star x') = f(x) \diamond f(x') = e_{G'} \diamond e_{G'} = e_{G'}$ et donc $x \star x' \in Ker f$.
   (c) Soit $x \in Ker f$. Alors $f(x^{-1}) = f(x)^{-1} = e_{G'}^{-1} = e_{G'}$. Et donc $x^{-1} \in Ker f$.

(2) Montrons que l'image est un sous-groupe de G'.
   (a) $f(e_G) = e_{G'}$ donc $e_{G'} \in Im f$.
   (b) Soient $y,y' \in Im f$. Il existe alors $x,x' \in G$ tels que $f(x) = y$, $f(x') = y'$. Alors $y \diamond y' = f(x) \diamond f(x') = f(x \star x') \in Im f$.
   (c) Soit $y \in Im f$ et $x \in G$ tel que $y = f(x)$. Alors $y^{-1} = f(x)^{-1} = f(x^{-1}) \in Im f$.

(3) Supposons f injective. Soit $x \in Ker f$, alors $f(x) = e_{G'}$ donc $f(x) = f(e_G)$ et comme f est injective alors $x = e_G$. Donc $Ker f = \{e_G\}$. Réciproquement supposons $Ker f = \{e_G\}$. Soient $x,x' \in G$ tels que $f(x) = f(x')$ donc $f(x) \diamond \big(f(x')\big)^{-1} = e_{G'}$, d'où $f(x) \diamond f(x'^{-1}) = e_{G'}$ et donc $f(x \star x'^{-1}) = e_{G'}$. Ceci implique que $x \star x'^{-1} \in Ker f$. Comme $Ker f = \{e_G\}$ alors $x \star x'^{-1} = e_G$ et donc $x = x'$. Ainsi f est injective.

(4) C'est clair !

$\square$

Exemples 26. (1) Soit $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ définie par $f(k) = 3k$. $(\mathbb{Z},+)$ est considéré comme ensemble de départ et d'arrivée de l'application. Alors f est un morphisme du groupe $(\mathbb{Z},+)$ dans lui-même car $f(k + k') = 3(k + k') = 3k + 3k' = f(k) + f(k')$. Calculons le noyau : $Ker f = \{k \in \mathbb{Z} \mid f(k) = 0\}$. Mais si $f(k) = 0$ alors $3k = 0$ donc $k = 0$. Ainsi $Ker f = \{0\}$ est réduit à l'élément neutre et donc f est injective. Calculons maintenant l'image $Im f = \{f(k) \mid k \in \mathbb{Z}\} = \{3k \mid k \in \mathbb{Z}\} = 3\mathbb{Z}$. Nous retrouvons que $3\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$.

Plus généralement si l'on fixe $n \in \mathbb{Z}$, $n \neq 0$, et que f est définie par $f(k) = k \cdot n$ alors $Ker f = \{0\}$ et $Im f = n\mathbb{Z}$.

(2) Soient les groupes $(\mathbb{R},+)$ et $(\mathbb{U},\times)$ (où $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$) et f l'application $f : \mathbb{R} \longrightarrow \mathbb{U}$ définie par $f(t) = e^{it}$. Montrons que f est un morphisme : $f(t+t') = e^{i(t+t')} = e^{it} \times e^{it'} = f(t) \times f(t')$. Calculons le noyau $Ker f = \{t \in \mathbb{R} \mid f(t) = 1\}$. Mais si $f(t) = 1$ alors $e^{it} = 1$ donc $t = 0 \pmod{2\pi}$. D'où $Ker f = \{2k\pi \mid k \in \mathbb{Z}\} = 2\pi\mathbb{Z}$. Ainsi f n'est pas injective. L'image de f est $\mathbb{U}$ car tout nombre complexe de module 1 s'écrit sous la forme $f(t) = e^{it}$.

5.4. Le groupe $\mathbb{Z}/n\mathbb{Z}$.

Fixons $n \geq 1$. Rappelons que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}$$

où $\overline{p}$ désigne la classe d'équivalence de p modulo n.

Autrement dit

$$\boxed{\overline{p} = \overline{q} \iff p \equiv q \pmod{n}}$$

ou encore $\overline{p} = \overline{q} \iff \exists k \in \mathbb{Z} \quad p = q + kn$.

On définit une **addition** sur $\mathbb{Z}/n\mathbb{Z}$ par :

$$\boxed{\overline{p} + \overline{q} = \overline{p+q}}$$

Par exemple dans $\mathbb{Z}/60\mathbb{Z}$, on a $\overline{31} + \overline{46} = \overline{31+46} = \overline{77} = \overline{17}$.

Nous devons montrer que cette addition est bien définie : si $\overline{p'} = \overline{p}$ et $\overline{q'} = \overline{q}$ alors $p' \equiv p \pmod{n}$, $q' \equiv q \pmod{n}$ et donc $p' + q' \equiv p + q \pmod{n}$. Donc $\overline{p'+q'} = \overline{p+q}$. Donc on a aussi $\overline{p'} + \overline{q'} = \overline{p} + \overline{q}$. Nous avons montré que l'addition est indépendante du choix des représentants.

Proposition 5.5. $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe commutatif.*

C'est facile. L'élément neutre est $\overline{0}$. L'opposé de $\overline{k}$ est $-\overline{k} = \overline{-k} = \overline{n-k}$. L'associativité et la commutativité découlent de celles de $(\mathbb{Z},+)$.

Définition 5.10. Un groupe $(G,\star)$ est un groupe **monogène** s'il existe un élément $a \in G$ tel que :

$$\text{pour tout } x \in G, \text{ il existe } k \in \mathbb{Z} \text{ tel que } x = a^k$$

Autrement dit le groupe G est engendré par un seul élément a.

$(\mathbb{Z},+)$ est un groupe monogène engendré par 1 (ou par -1).

Définition 5.11. Un groupe $(G,\star)$ est dit **cyclique** lorsqu' il est monogène et fini.

Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique de cardinal n. En effet il est engendré par $a = \overline{1}$, car tout élément $\overline{k}$ s'écrit $\overline{k} = \underbrace{\overline{1} + \overline{1} + \cdots \overline{1}}_{k \text{ fois}} = k \cdot \overline{1}$.

Voici un résultat intéressant : il n'existe, à isomorphisme près, qu'un seul groupe cyclique à n éléments, c'est $\mathbb{Z}/n\mathbb{Z}$:

Théorème 5.6. *Si* $(G,\star)$ *un groupe cyclique de cardinal* n*, alors* $(G,\star)$ *est isomorphe à* $(\mathbb{Z}/n\mathbb{Z},+)$.

Preuve. Comme G est cyclique alors $G = \left\{ \ldots, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots \right\}$. Dans cette écriture il y a de nombreuses redondances (car de toute façon G n'a que n éléments). Nous allons montrer qu'en fait

$$G = \left\{e, a, a^2, \ldots, a^{n-1}\right\} \quad \text{et que} \quad a^n = e.$$

Tout d'abord l'ensemble $\left\{e, a, a^2, \ldots, a^{n-1}\right\}$ est inclus dans G. En plus il a exactement n éléments. En effet si $a^p = a^q$ avec $0 \leq q < p \leq n-1$ alors $a^{p-q} = e$ (avec $p - q > 0$) et ainsi $a^{p-q+1} = a^{p-q} \star a = a$, $a^{p-q+2} = a^2$ et alors le groupe G serait égal à $\left\{e, a, a^2, \ldots, a^{p-q-1}\right\}$ et n'aurait pas n éléments. Ainsi $\left\{e, a, a^2, \ldots, a^{n-1}\right\} \subset G$ et les deux ensembles ont le même nombre n d'éléments, donc ils sont égaux.

Montrons maintenant que $a^n = e$. Comme $a^n \in G$ et que $G = \left\{e, a, a^2, \ldots, a^{n-1}\right\}$ alors il existe $0 \leq p \leq n-1$ tel que $a^n = a^p$. Encore une fois si $p > 0$ cela entraîne $a^{n-p} = e$ et donc une contradiction. Ainsi $p = 0$ donc $a^n = a^0 = e$.

Nous pouvons maintenant construire l'isomorphisme entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(G,\star)$. Soit $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ l'application définie par $f(\overline{k}) = a^k$.

- Il faut tout d'abord montrer que f est bien définie car notre définition de f dépend du représentant k et pas de la classe $\overline{k}$: si $\overline{k} = \overline{k'}$ (une même classe définie par deux représentants distincts) alors $k \equiv k' \pmod n$ et donc il existe $l \in \mathbb{Z}$ tel que $k = k' + ln$. Ainsi $f(\overline{k}) = a^k = a^{k'+ln} = a^{k'} \star a^{ln} = a^{k'} \star (a^n)^l = a^{k'} \star e^l = a^{k'} = f(\overline{k'})$. Ainsi f est bien définie.
- f est un morphisme de groupes car $f(\overline{k} + \overline{k'}) = f(\overline{k + k'}) = a^{k+k'} = a^k \star a^{k'} = f(\overline{k}) \star f(\overline{k'})$ (pour tout $\overline{k}, \overline{k'}$).
- Il est clair que f est surjective car tout élément de G s'écrit a^k.
- Comme l'ensemble de départ et celui d'arrivée ont le même nombre d'éléments et que f est surjective alors f est bijective.

Conclusion : f est un isomorphisme entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(G,\star)$. □

5.5. **Groupe des permutations $\mathcal{S}_n$.**

Fixons un entier $n \geq 2$.

5.5.1. *Groupe des permutations.*

Proposition 5.7. *L'ensemble des bijections de $\{1,2,\ldots,n\}$ dans lui-même, muni de la composition des fonctions est un groupe, noté $(\mathcal{S}_n,\circ)$.*

Une bijection de $\{1,2,\ldots,n\}$ (dans lui-même) s'appelle une **permutation**. Le groupe $(\mathcal{S}_n,\circ)$ s'appelle le **groupe des permutations** (ou le **groupe symétrique**).

Preuve.

(1) La composition de deux bijections de $\{1,2,\ldots,n\}$ est une bijection de $\{1,2,\ldots,n\}$.
(2) La loi est associative (par l'associativité de la composition des fonctions).
(3) L'élément neutre est l'identité.
(4) L'inverse d'une bijection f est sa bijection réciproque f^{-1}.

□

Il s'agit d'un autre exemple de groupe ayant un nombre fini d'éléments :

Lemme 5.8. *Le cardinal de $\mathcal{S}_n$ est $n!$.*

Preuve. La preuve est simple. Pour l'élément 1, son image appartient à $\{1,2,\ldots,n\}$ donc nous avons n choix. Pour l'image de 2, il ne reste plus que $n-1$ choix (1 et 2 ne doivent pas avoir la même image car notre application est une bijection). Ainsi de suite... Pour l'image du dernier élément n il ne reste qu'une possibilité. Au final il y a $n \times (n-1) \times \cdots \times 2 \times 1 = n!$ façon de construire des bijections de $\{1,2,\ldots,n\}$. $\square$

5.5.2. *Notation et exemples.*

Décrire une permutation $f : \{1,2,\ldots,n\} \longrightarrow \{1,2,\ldots,n\}$ équivaut à donner les images de chaque i allant de 1 à n. Nous notons donc f par

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{bmatrix}$$

Par exemple la permutation de $\mathcal{S}_7$ notée

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{bmatrix}$$

est la bijection $f : \{1,2,\ldots,7\} \longrightarrow \{1,2,\ldots,7\}$ définie par $f(1) = 3$, $f(2) = 7$, $f(3) = 5$, $f(4) = 4$, $f(5) = 6$, $f(6) = 1$, $f(7) = 2$. C'est bien une bijection car chaque nombre de 1 à 7 apparaît une fois et une seule sur la deuxième ligne.

L'élément neutre du groupe est l'identité id ; pour $\mathcal{S}_7$ c'est donc $\left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{smallmatrix}\right]$.

Il est facile de calculer la composition de deux permutations f et g avec cette notation. Si $f = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{smallmatrix}\right]$ et $g = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{smallmatrix}\right]$ alors $g \circ f$ s'obtient en superposant la permutation f puis g

$$g \circ f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 7 & 1 & 5 & 4 & 3 \end{bmatrix}$$

ensuite on élimine la ligne intermédiaire du milieu et donc $g \circ f$ se note $\left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 7 & 1 & 5 & 4 & 3 \end{smallmatrix}\right]$.

Il est tout aussi facile de calculer l'inverse d'une permutation : il suffit d'échanger les lignes du haut et du bas et de réordonner le tableau. Par exemple l'inverse de

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{bmatrix}$$

se note $f^{-1} = \left[\begin{smallmatrix} 3 & 7 & 5 & 4 & 6 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{smallmatrix}\right]$ ou plutôt après réordonnement $\left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 1 & 4 & 3 & 5 & 2 \end{smallmatrix}\right]$.

5.5.3. *Le groupe $\mathcal{S}_3$.*

Nous allons étudier en détails le groupe $\mathcal{S}_3$ des permutations de $\{1,2,3\}$. Nous savons que $\mathcal{S}_3$ possède $3! = 6$ éléments que nous énumérons :

- $\mathrm{id} = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right]$ l'identité,
- $\tau_1 = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right]$ une transposition,
- $\tau_2 = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right]$ une deuxième transposition,
- $\tau_3 = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right]$ une troisième transposition,
- $\sigma = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right]$ un cycle,
- $\sigma^{-1} = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right]$ l'inverse du cycle précédent.

Donc $\mathcal{S}_3 = \left\{\mathrm{id}, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\right\}$.

Calculons $\tau_1 \circ \sigma$ et $\sigma \circ \tau_1$:

$$\tau_1 \circ \sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \tau_2 \quad \text{et} \quad \sigma \circ \tau_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \tau_3.$$

Ainsi $\tau_1 \circ \sigma = \tau_2$ est différent de $\sigma \circ \tau_1 = \tau_3$, ainsi le groupe $\mathcal{S}_3$ n'est pas commutatif. Et plus généralement :

Lemme 5.9. *Pour $n \geq 3$, le groupe $\mathcal{S}_n$ n'est pas commutatif.*

Nous pouvons calculer la table du groupe $\mathcal{S}_3$

$g \circ f$	id	τ_1	τ_2	τ_3	σ	σ^{-1}
id	id	τ_1	τ_2	τ_3	σ	σ^{-1}
τ_1	τ_1	id	σ	σ^{-1}	$\tau_1 \circ \sigma = \tau_2$	τ_3
τ_2	τ_2	σ^{-1}	id	σ	τ_3	τ_1
τ_3	τ_3	σ	σ^{-1}	id	τ_1	τ_2
σ	σ	$\sigma \circ \tau_1 = \tau_3$	τ_1	τ_2	σ^{-1}	id
σ^{-1}	σ^{-1}	τ_2	τ_3	τ_1	id	σ

FIGURE 2. Table du groupe $\mathcal{S}_3$

Comment avons-nous rempli cette table ? Nous avons déjà calculé $\tau_1 \circ \sigma = \tau_2$ et $\sigma \circ \tau_1 = \tau_3$. Comme $f \circ \mathrm{id} = f$ et $\mathrm{id} \circ f = f$ il est facile de remplir la première colonne noire ainsi que la première ligne noire. Ensuite il faut faire les calculs !

On retrouve ainsi que $\mathcal{S}_3 = \left\{\mathrm{id}, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\right\}$ est un groupe : en particulier la composition de deux permutations de la liste reste une permutation de la liste. On lit aussi sur la table l'inverse de chaque élément, par exemple sur la ligne de τ_2 on cherche à quelle colonne on trouve l'identité, c'est la colonne de τ_2. Donc l'inverse de τ_2 est lui-même.

5.5.4. *Décomposition en cycles.*

- Nous allons définir ce qu'est un **cycle** : c'est une permutation σ qui fixe un certain nombre d'éléments ($\sigma(i) = i$) et dont les éléments non fixés sont obtenus par itération : $j, \sigma(j), \sigma^2(j), \ldots$ C'est plus facile à comprendre sur un exemple :

$$\sigma = \begin{bmatrix} 1 & \mathbf{2} & 3 & \mathbf{4} & \mathbf{5} & 6 & 7 & \mathbf{8} \\ 1 & \mathbf{8} & 3 & \mathbf{5} & \mathbf{2} & 6 & 7 & \mathbf{4} \end{bmatrix}$$

  est un cycle : les éléments $1, 3, 6, 7$ sont fixes, les autres s'obtiennent comme itération de 2 : $2 \mapsto \sigma(2) = 8 \mapsto \sigma(8) = \sigma^2(2) = 4 \mapsto \sigma(4) = \sigma^3(2) = 5$, ensuite on retrouve $\sigma^4(2) = \sigma(5) = 2$.
- Nous noterons ce cycle par

$$(2\ 8\ 4\ 5)$$

Il faut comprendre cette notation ainsi : l'image de 2 est 8, l'image de 8 est 4, l'image de 4 est 5, l'image de 5 est 2. Les éléments qui n'apparaissent pas (ici $1, 3, 6, 7$) sont fixes. On aurait pu aussi noter ce même cycle par : $(8\ 4\ 5\ 2)$, $(4\ 5\ 2\ 8)$ ou $(5\ 2\ 8\ 4)$.

- Pour calculer l'inverse on renverse les nombres : l'inverse de $\sigma = (2\ 8\ 4\ 5)$ est $\sigma^{-1} = (5\ 4\ 8\ 2)$.
- Le **support** d'un cycle sont les éléments qui ne sont pas fixes : le support de σ est $\{2, 4, 5, 8\}$. La **longueur** (ou l'**ordre**) d'un cycle est le nombre d'éléments qui ne sont pas fixes (c'est donc le cardinal du support). Par exemple $(2\ 8\ 4\ 5)$ est un cycle de longueur 4.
- Autres exemples : $\sigma = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right] = (1\ 2\ 3)$ est un cycle de longueur 3 ; $\tau = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{smallmatrix}\right] = (2\ 4)$ est un cycle de longueur 2, aussi appelé une **transposition**.
- Par contre $f = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 5 & 4 & 6 & 3 & 1 \end{smallmatrix}\right]$ n'est pas un cycle ; il s'écrit comme la composition de deux cycles $f = (1\ 7) \circ (3\ 5\ 6)$. Comme les supports de $(1\ 7)$ et $(3\ 5\ 6)$ sont disjoints alors on a aussi $f = (3\ 5\ 6) \circ (1\ 7)$.

Ce dernier point fait partie d'un résultat plus général que nous admettons :

Théorème 5.10. *Toute permutation de $\mathcal{S}_n$ se décompose en composition de cycles à supports disjoints. De plus cette décomposition est unique.*

Pour l'unicité il faut comprendre : unique à l'écriture de chaque cycle près (exemple : $(3\ 5\ 6)$ et $(5\ 6\ 3)$ sont le même cycle) et à l'ordre près (exemple : $(1\ 7) \circ (3\ 5\ 6) = (3\ 5\ 6) \circ (1\ 7)$).

Exemple : la décomposition de $f = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 8 & 3 & 7 & 6 & 4 \end{smallmatrix}\right]$ en composition de cycle à supports disjoints est $(1\ 5\ 3) \circ (4\ 8) \circ (6\ 7)$.

Attention, si les supports ne sont pas disjoints alors cela ne commute plus : par exemple $g = (1\ 2) \circ (2\ 3\ 4)$ n'est pas égale à $h = (2\ 3\ 4) \circ (1\ 2)$. En effet l'écriture de g en produit de cycle à support disjoint est $g = (1\ 2) \circ (2\ 3\ 4) = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right] = (1\ 2\ 3\ 4)$ alors que celle de h est $h = (2\ 3\ 4) \circ (1\ 2) = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{smallmatrix}\right] = (1\ 3\ 4\ 2)$.