8 Structure de groupe

Extrait du programme officiel :

Contenus	Capacités & commentaires
a) Compléments sur les groupes	
Intersection de sous-groupes.	
Sous-groupe engendré par une partie. Partie génératrice d'un groupe.	
Sous-groupes du groupe $(\mathbb{Z}, +)$.	
Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.	
Groupe monogène, groupe cyclique.	Groupe des racines n-ièmes de l'unité.
Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.	
Ordre d'un élément d'un groupe.	L'ordre de x est le cardinal du sous-groupe de G engendré par x.
Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour tout $n \in \mathbb{Z}$, $x^n = e \iff d \mid n$.	
L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.	La démonstration n'est exigible que pour G commutatif.

Table des matières

8 Structure de groupe 1

I Structure de groupe (MP2I) 2

II Puissances ou itérées d'un élément (MP2I) 4

III Régularité 5

IV Groupe produit (MP2I) 6

V Sous-groupes 7
1 Définition et caractérisation (MP2I) . . . 7
2 Intersection et réunion (MPI) . . . 8
3 Sous-groupes de $(\mathbb{Z},+)$ (MPI) . . . 9
4 Sous-groupes de $(\mathbb{R},+)$ (HP) . . . 9

VI Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ 10
1 Congruences (MP2I) . . . 10
2 Le groupe $\mathbb{Z}/n\mathbb{Z}$ (MPI) . . . 10

VII Morphismes (MP2I) 12
1 Définition . . . 12
2 Noyau et image . . . 13
3 Isomorphismes . . . 15

VIII Groupes monogènes (MPI) 15
1 Sous-groupes engendré par une partie . . . 15
2 Groupes monogènes et cycliques . . . 16
3 Ordre d'un élément dans un groupe . . . 17

IX Groupes symétriques (MP2I) 20
1 Définition, structure . . . 20
2 Cycles . . . 21
3 Signature . . . 23
4 Groupe alterné (HP) . . . 25

I Structure de groupe (MP2I)

Remarque : Quelques rappels

R 1 –

- **Loi de composition interne** sur un ensemble E : toute application $\star$: $\begin{array}{ccc} E\times E & \longrightarrow & E \\ (x,y) & \longmapsto & x\star y \end{array}$.
- Elle est dite
  - ⋆ **associative** lorsque
  $$\forall\,(x,y,z)\in E^3,\ \ (x\star y)\star z = x\star(y\star z)$$
  (que l'on peut alors noter $x\star y\star z$.)
  - ⋆ **commutative** lorsque
  $$\forall\,(x,y)\in E^2,\ \ x\star y = y\star x.$$

- On dit que e est **élément neutre** pour $\star$ si pour tout $x \in E$, $x \star e = e \star x = x$.

> **Exercice 1**
> S'il existe, l'élément neutre est unique.

  - ⋆ **Notation additive** : $0x = e$ avec e souvent noté 0 ou 0_E appelé élément nul.
  - ⋆ **Notation multiplicative** : $x^0 = e$ avec e souvent noté 1 ou 1_E appelé élément unité.

- Un élément x de E est dit **symétrisable** pour $\star$ si on a $y \in E$ tel que $x \star y = y \star x = e$.

> **Exercice 2**
> S'il existe, y est unique.

  - ⋆ **Notation additive** : on parle d'opposé, noté $-x$. Pour $x + (-y)$, on note $x - y$.
  - ⋆ **Notation multiplicative** : on parle d'inverse, noté x^{-1}.
    ⚠ $\frac{x}{y}$ n'a pas de sens en général : cela désigne $x \star y^{-1}$ ou $y^{-1} \star x$?

> **Exemple**
> **E 1** – L'élément neutre e (lorsqu'il existe) est toujours symétrisable, de symétrique lui-même.

Être symétrisable à gauche ou à droite ne suffit pas.

> **Exemple**
> **E 2** – Sur E^E pour $\circ$, l'élément neutre est id_E.
>
> - ⋆ $\left(\exists\, g \in E^E,\ \ f \circ g = g \circ f = \mathrm{id}_E\right) \iff f$ bijective (ie inversible pour $\circ$).
> - ⋆ $\left(\exists\, g \in E^E,\ \ f \circ g = \mathrm{id}_E\right) \iff f$ surjective.
> - ⋆ $\left(\exists\, g \in E^E,\ \ g \circ f = \mathrm{id}_E\right) \iff f$ injective.

- Soit $\star$ une loi de composition interne associative sur E notée multiplicativement.
  Si x et y sont symétrisables, alors
  - ⋆ $x \star y$ l'est aussi. De plus, $(x \star y)^{-1} = y^{-1} \star x^{-1}$.
  - ⋆ x^{-1} l'est aussi et $\left(x^{-1}\right)^{-1} = x$.

Définition 1 : Groupe

On appelle **groupe** tout couple $(G, \star)$ où G est un ensemble tel que

(i) $\star$ est une loi de composition interne sur G
(ii) $\star$ est associative
(iii) G admet un élément neutre pour $\star$
(iv) Tout élément de G admet un symétrique dans G pour $\star$.

Si, de plus, $\star$ est commutative, on dit que $(G, \star)$ est un **groupe commutatif** ou **groupe abélien**.

> **Remarque**
> **R 2** – En particulier, un groupe n'est jamais vide.

Exemple

E3 – $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs de neutre 0.

E4 – Si D est un ensemble non vide, $(\mathbb{R}^D,+)$ et $(\mathbb{C}^D,+)$ et en particulier $(\mathbb{R}^{\mathbb{N}},+)$ et $(\mathbb{C}^{\mathbb{N}},+)$ sont des groupes commutatifs, de neutre la fonction / suite nulle.

E5 – $(\mathbb{Q}^*,\times)$, $(\mathbb{Q}_+^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}_+^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes commutatifs de neutre 1.

E6 – Si E est un ensemble non vide, on note $\mathfrak{S}(E)$ l'ensemble des permutations de E (bijection de E sur E). Alors $(\mathfrak{S}(E),\circ)$ est un groupe d'élément neutre id_E.
Si $|E|\geqslant 3$, ce groupe n'est pas commutatif.
Si $n\in\mathbb{N}\setminus\{0,1\}$, et $E=[\![1,n]\!]$, on note $\mathfrak{S}_n=\mathfrak{S}([\![1,n]\!])$.
$(\mathfrak{S}_n,\circ)$ est appelé **groupe symétrique d'ordre** n (et contient $n!$ éléments).

II Puissances ou itérées d'un élément (MP2I)

Définition 2 : Itérées d'un élément

Soir E un ensemble muni d'une loi de composition interne $\star$ (notée multiplicativement) **associative** et possédant un élément neutre e.
Pour tout $x\in E$ et tout $n\in\mathbb{N}$, on définit récursivement

$$x^n=\begin{cases}e & \text{si } n=0\\ x^{n-1}\star x & \text{sinon.}\end{cases}$$

Remarque

R3 – Autrement dit, $x^n=\prod_{k=1}^{n}x=\underbrace{x\star\cdots\star x}_{n\text{ fois}}$.

R4 – En notation additive,

$$n\cdot x=\begin{cases}0 & \text{si } n=0\\ (n-1)\cdot x+x & \text{sinon.}\end{cases}$$

Propriété 1 : des exposants

Soient $x,y\in E$ et $n,m\in\mathbb{N}$.

(i) $x^{n+m}=x^n\star x^m=x^m\star x^n$.
(ii) $(x^n)^m=x^{nm}=(x^m)^n$.
(iii) *Si* $x\star y=y\star x$, $(x\star y)^n=x^n\star y^n$.
(iv) *Si x est inversible, x^n est inversible et* $(x^n)^{-1}=(x^{-1})^n$.

Démonstration

(i) Par récurrence sur m (par exemple) à n fixé et par associativité.
(ii) Par récurrence sur m à n fixé.
(iii) Par récurrence sur n.
(iv) On calcule avec la propriété précédente $x^n\star(x^{-1})^n=(x\star x^{-1})^n=e$ et de même $(x^{-1})^n\star x^n=e$.

Notation 1 : Exposant négatif

Si $x\in E$ inversible et $n\in\mathbb{N}$, on note x^{-n} l'élément $(x^{-1})^n=(x^n)^{-1}$.

Remarque

R 5 – Les propriétés (i) à (iii) restent vraies pour $n, m \in \mathbb{Z}$ lorsque x et y sont inversibles.

III RÉGULARITÉ

Soit[1] E un ensemble muni d'une loi de composition interne associative $\star$ et possédant un élément neutre e.

Définition 3 : Régularité

Soit $x \in E$. On dit que x est **régulier** (ou **simplifiable**)

- **à gauche** lorsque
$$\forall\, a, b \in E,\quad x \star a = x \star b \Longrightarrow a = b$$
- **à droite** lorsque
$$\forall\, a, b \in E,\quad a \star x = b \star x \Longrightarrow a = b$$

On dit que x est **régulier** lorsqu'il l'est à gauche et à droite.

Propriété 2 : Régularité d'un inversible

Tout élément inversible de $(E, \star)$ est régulier.

Démonstration

Si x est inversible et si $x \star a = x \star b$, alors
$$a = \left(x^{-1} \star x\right) \star a = x^{-1} \star (x \star a) = x^{-1} \star (x \star b) = \left(x^{-1} \star x\right) \star b = b$$
par associativité. ■

Corollaire 1 : Régularité dans un groupe

Si $(G, \star)$ est un groupe, alors tout élément de G est régulier.

Corollaire 2 : Bijectivité des translations

Si $(G, \star)$ est une groupe et $a \in G$ fixé.

Les applications $\varphi_a : \left|\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a \star x \end{array}\right.$ *et* $\psi_a : \left|\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x \star a \end{array}\right.$ *(appelées translations à gauche et à droite) sont bijectives.*

Démonstration

On vérifie que $\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a^{-1}} \circ \varphi_a = \mathrm{id}_G$ et $\psi_a \circ \psi_{a^{-1}} = \psi_{a^{-1}} \circ \psi_a = \mathrm{id}_G$. ■

Corollaire 3

Si $(G, \star)$ est une groupe et $a \in G$ fixé.
$$G = \{a \star x,\ x \in G\} = \{x \star a,\ x \in G\}\,.$$

1. On dit que $(E, \star)$ est un **monoïde**.

Démonstration

Il s'agit de la surjectivité des deux applications précédentes. ■

Remarque

R 6 – Cela signifie que dans la table de la loi $\star$ du groupe G, chaque élément de G apparaît une et une seule fois sur chaque ligne et sur chaque colonne.

Exemple

E 7 – Si on considère le groupe des racines cubique de l'unité : $\mathbb{U}_3 = \{1, \mathrm{j}, \mathrm{j}^2\}$ muni de la loi $\times$, on a la table

$\times$	1	j	j^2
1	1	j	j^2
j	j	j^2	1
j^2	j^2	1	j

IV Groupe produit (MP2I)

Propriété 3 : Groupe produit

Soit $(G, \star)$ et (H, Δ) des groupes.
Pour tout (g, h) et (g', h') dans $G \times H$, on pose

$$(g, h) \top (g', h') = (g \star g', h \Delta h').$$

Alors $(G \times H, \top)$ a une structure de groupe.
Si, de plus, les lois $\star$ et Δ sont commutatives, alors $\top$ l'est.

Démonstration

- Le fait que $\top$ soit une loi de composition interne sur $G \times H$ provient du fait que $\star$ et Δ le sont sur G et H respectivement.
- Un calcul facile mais pénible à écrire permet de vérifier que les associativités de $\star$ et Δ donnent celle de $\top$.
- Si e_G et e_H sont les éléments neutres de G et H, alors (e_G, e_H) est bien neutre sur $G \times H$.
- Si $g \in G$ et $h \in H$ d'inverses g^{-1} et h^{-1}, alors (g^{-1}, h^{-1}) est l'inverse de (g, h).

■

Remarque

R 7 – Cela se généralise à un nombre de groupes quelconque $\left(G_1, \underset{1}{\star}\right), \ldots, \left(G_p, \underset{p}{\star}\right)$ avec pour tout $(x_1, \ldots, x_p)$ et $(y_1, \ldots, y_p)$ dans $G_1 \times \cdots \times G_p$,

$$(x_1, \ldots, x_p) \top (y_1, \ldots, y_p) = \left(x_1 \underset{1}{\star} y_1, \ldots, x_p \underset{p}{\star} y_p\right).$$

V SOUS-GROUPES

1 Définition et caractérisation (MP2I)

Définition 4 : Sous-groupe

Soit $(G,\star)$ groupe. On note $\star|_{H^2}$ la restriction à H^2 de la loi $\star$.
On dit que H est un **sous-groupe** de $(G,\star)$ si $H \subset G$ et $(H,\star|_{H^2})$ est un groupe.

Propriété 4 : Sous-groupes triviaux

*Soit $(G,\star)$ groupe. G et $\{e_G\}$ sont des sous-groupes de $(G,\star)$ appelés **sous-groupes triviaux**.*

Propriété 5

Soit H un sous-groupe de $(G,\star)$.

(i) $(H,\star)$ possède le même élément neutre que $(G,\star)$.

(ii) Si $x \in H$, alors x a même inverse dans $(H,\star)$ et dans $(G,\star)$.

Démonstration

(i) Soient e_H et e_G les éléments neutres respectifs. Alors $e_H \star e_G = e_H = e_H \star e_H$ car $e_H \in G$ et e_G neutre sur G d'une part, et e_H neutre sur H d'autre part. Puis, par régularité à gauche de e_H dans G, $e_G = e_H$.

(ii) Si $x \in H$, alors x a un symétrique $\mathrm{sym}_H(x) \in H \subset G$ tel que $x \star \mathrm{sym}_H(x) = \mathrm{sym}_H(x) \star x = e_H = e_G$ et donc par unicité, x inversible dans G et $\mathrm{sym}_G(x) = \mathrm{sym}_H(x)$. ■

Propriété 6 : caractérisation des sous-groupes

Soit $(G,\star)$ un groupe (multiplicatif). Les propositions suivantes sont équivalentes :

(i) H est un sous-groupe de $(G,\star)$

(ii)
$$\begin{cases} H \subset G \\ H \neq \varnothing \quad (e_G \in H) \\ H \text{ est stable par } \star \ : \ \forall x,y \in H,\ \ x \star y \in H \\ H \text{ est stable par inverse } \ : \ \forall x \in H,\ \ x^{-1} \in H \end{cases}$$

(iii)
$$\begin{cases} H \subset G \\ H \neq \varnothing \quad (e_G \in H) \\ \forall x,y \in H,\ \ x \star y^{-1} \in H \end{cases}$$

Remarque

R 8 – En notation additive, (ii) devient $\begin{cases} H \subset G \\ H \neq \varnothing \quad (0_G \in H) \\ H \text{ est stable par } \star \ : \ \forall x,y \in H,\ \ x+y \in H \\ H \text{ est stable par opposé } \ : \ \forall x \in H,\ \ -x \in H \end{cases}$ et (iii) devient

$$\begin{cases} H \subset G,\ H \neq \varnothing \quad (0_G \in H) \\ \forall\, x, y \in H,\ \ x - y \in H \end{cases}$$

Démonstration

- $(i) \Longrightarrow (ii)$: si $H < G$, $H \subset G$, $H \neq \varnothing$, H stable par $\star$ (Ici) et, d'après la propriété précédente, H est bien stable par inverse.
- $(ii) \Longrightarrow (iii)$: facile.
- $(iii) \Longrightarrow (i)$: si on a (iii), alors $H \subset G$. La loi $\star$ est associative sur G donc a fortiori, elle l'est aussi sur H.
  Comme H est non vide, on a $x \in H$ avec $x \star x^{-1} = e_G \in H$. Alors pour tout $x \in H$, $e_G \star x^{-1} = x^{-1} \in H$. e_G est neutre pour $\star$ sur G donc l'est aussi sur H.
  L'inverse x^{-1} d'un élément de $x \in H$ dans G est dans H, donc tout élément de H est symétrisable dans H.
  Donc H est bien un sous-groupe de $(G, \star)$. ■

Remarque

R 9 – Un sous-groupe d'un groupe abélien est facilement encore commutatif.

Exemple

E 8 – $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont des sous-groupes (additifs et abéliens) de $(\mathbb{C}, +)$.

E 9 – $\mathbb{R}^D$ où $D \neq \varnothing$ est un sous-groupe additif abélien de $(\mathbb{C}^D, +)$.

E 10 – $\mathbb{Q}^*, \mathbb{Q}_+^*, \mathbb{R}^*, \mathbb{R}_+^*, \mathbb{U}, \mathbb{U}_n$ pour $n \in \mathbb{N}^*$ sont des sous-groupes multiplicatifs abéliens de $(\mathbb{C}^*, \times)$. (On rappelle que $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$ et pour $n \in \mathbb{N}^*$, $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\} = \left\{ \mathrm{e}^{\frac{2ik\pi}{n}},\ k \in [\![0, n-1]\!] \right\}$.)

2 Intersection et réunion (MPI)

Propriété 7 : Intersection de sous-groupes

Soit $(G, \star)$ un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, \star)$. Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de $(G, \star)$.

Démonstration

- $(H_i)_{i \in I} \subset G$ car $\forall\, i \in I,\ \ H_i \subset G$.
- $(H_i)_{i \in I} \neq \varnothing$ car $\forall\, i \in I,\ \ e_G \in H_i$.
- Si $x, y \in (H_i)_{i \in I}$, alors $\forall\, i \in I,\ \ x \star y^{-1} \in H_i$ donc $x \star y^{-1} \in \bigcap_{i \in I} H_i$. ■

Exercice 3 : Réunion de sous-groupes

Soit $(G, \star)$ un groupe, H, K sont des sous groupes de $(G, \star)$, alors

$$H \cup K \textbf{ sous-groupe de } G \iff H \subset K \text{ ou } K \subset H.$$

- $\Longleftarrow$: ok
- $\Longrightarrow$: Si $H \cup K$ sous- groupe de G et $H \not\subset K$, on va montrer que $K \subset H$.
  On a $h \in H \setminus K$.
  Soit $k \in K$. Alors $k \star h \in H \cup K$ par stabilité de $\star$ sur $H \cup G$.

Si $k \star h \in K$, alors $h = k^{-1} \star (k \star h) \in K$, ce qui n'est pas possible.
C'est donc que $k \star h \in H$ et donc $k = (k \star h) \star h^{-1} \in H$.
Finalement, on a bien $K \subset H$.

3 Sous-groupes de $(\mathbb{Z}, +)$ (MPI)

Notation 2

Pour tout $a \in \mathbb{Z}$, on note $a\mathbb{Z} = \{ak,\ k \in \mathbb{Z}\}$.

Remarque

R 10 – On vérifie avec la caractérisation que $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
Avec $a\mathbb{Z} = \{\dots, -2a, -a, 0, a, 2a, \dots\}$, il s'agit du plus petit sous-groupe (au sens de l'inclusion) contenant a.
On dit qu'il est engendré par a (sur le même principe que les Vect en algèbre linéaire.)

Propriété 8 : Sous-groupes de $(\mathbb{Z}, +)$

Les sous-groupes G de $(\mathbb{Z}, +)$ sont exactement les $a\mathbb{Z}$ pour $a \in \mathbb{N}$.
De plus, si $G \neq \{0\}$, $a = \min(G \cap \mathbb{N}^*)$.

Démonstration

- On a déjà que, si $a \in \mathbb{N}$, $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ par la caractérisation.
- Réciproquement, considérons G un sous-groupe de $(\mathbb{Z}, +)$.
  - ⋆ Soit $G = \{0\}$ et alors $G = a\mathbb{Z}$ avec $a = 0$.
  - ⋆ Soit $G \neq \{0\}$ et on peut trouver $p \in G \setminus \{0\}$. Soit $p > 0$ et alors $p \in G \cap \mathbb{N}^* \neq \varnothing$, soit $p < 0$ et alors $-p \in G \cap \mathbb{N}^* \neq \varnothing$.
    On peut donc introduire $a = \min(G \cap \mathbb{N}^*)$.
    Montrons que $G = a\mathbb{Z}$ par double inclusion.
    - $a \in G$, puis par stabilité et récurrence, pour tout $n \in \mathbb{N}$, $na \in G$ et par stabilité par passage à l'opposé, $-an \in G$. Finalement, $a\mathbb{Z} \subset G$.
    - Réciproquement, si $x \in G \subset \mathbb{Z}$, par division euclidienne, on a $(q, r) \in \mathbb{Z}^2$ tel que $x = aq + r$ et $0 \leqslant r < a$.
      Or $x \in G$ et $aq \in a\mathbb{Z} \subset G$ donc, comme on a un sous-groupe $r = x - aq \in G \cap \mathbb{N}$. Mais comme $r < a = \min(G \cap \mathbb{N}^*)$, $r \notin \mathbb{N}^*$ et donc $r = 0$.
      Finalement, $x = aq \in a\mathbb{Z}$.

    On a donc bien $G = a\mathbb{Z}$.

4 Sous-groupes de $(\mathbb{R}, +)$ (HP)

Théorème 1 : Hors-Programme

Soit G est un sous-groupe de $(\mathbb{R}, +)$.
Alors G est soit dense dans $\mathbb{R}$, soit discret (de la forme $\alpha\mathbb{Z}$).

Exercice 4 : Démonstration

Traiter le cas où $G = \{0\}$. On suppose dorénavant que $G \neq \{0\}$.

Montrer que $G \cap \mathbb{R}_+^*$ est non vide. En déduire que $G \cap \mathbb{R}_+^*$ admet une borne inférieure. On note α cette borne inférieure.

Cas où $\alpha = 0$ Montrer que G est dense dans $\mathbb{R}$ *en s'inspirant de la démonstration de la densité de* $\mathbb{Q}$ *dans* $\mathbb{R}$.

Cas où $\alpha > 0$ *On s'inspire de la démonstration des sous-groupes de* $(\mathbb{Z}, +)$.

Montrer qu'il existe $x \in G$ tel que $\alpha \leqslant x < 2\alpha$.

En déduire que $x = \alpha$, puis que $\alpha\mathbb{Z} \subset G$.

Soit réciproquement $x \in G$. *On simule une division euclidienne.*

Montrer que l'on peut trouver $q \in \mathbb{Z}$ tel que $q\alpha \leqslant x < (q+1)\alpha$.

En déduire que $x = q\alpha$. Conclure.

VI Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

1 Congruences (MP2I)

Définition 5 : Rappel : Congruence

Soit $n \in \mathbb{N}^*$. On dit que $a, b \in \mathbb{Z}$ sont **congrus modulo** n et on note $a \equiv b \ [n]$ lorsque $n|(a-b)$ ie lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

Propriété 9 : Rappel : Relation d'équivalence

C'est une relation d'équivalence sur $\mathbb{Z}$.

Propriété 10 : Rappel : Nombre d'entiers modulo n

$\forall\, a \in \mathbb{Z},\ \exists !\, r \in [\![0, n-1]\!],\ a \equiv r \ [n]$. *$r$ est le reste de la division euclidienne de a par n.*
Ainsi, la relation d'équivalence $\cdot \equiv \cdot \ [n]$ possède exactement n classes d'équivalences.

Propriété 11 : Rappel : Compatibilité de $+$

Soient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \ [n]$ et $c \equiv d \ [n]$.
Alors $a + c \equiv b + d \ [n]$.

2 Le groupe $\mathbb{Z}/n\mathbb{Z}$ (MPI)

Soit $n \in \mathbb{N}$ tel que $n \geqslant 1$ fixé.

Définition 6 : $\mathbb{Z}/n\mathbb{Z}$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble (quotient) des n classes d'équivalences de $\cdot \equiv \cdot \ [n]$, notées $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. Ainsi

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

Remarque

R 11 – $\overline{k}$ est l'ensemble des entiers congrus à k modulo n, donc l'ensemble des $k + n\ell$ pour $\ell \in \mathbb{Z}$.
On peut toujours se ramener à un entier r entre 0 et $n-1$ en prenant le reste de la division euclidienne de k par n : $k \equiv r \ [n]$ donc $\overline{k} = \overline{r} = \overline{r + pn}$ pour tout $p \in \mathbb{Z}$.

Définition 7 : Surjection canonique

L'application surjective $\left|\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \overline{k} \end{array}\right.$ est appelée **surjection canonique**.

Lemme 1 : Compatibilité avec $+$

Soient $a, b, c, d \in \mathbb{Z}$ tels que $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$. Alors $\overline{a+b} = \overline{c+d}$.

Démonstration

En effet $a \equiv c\ [n]$ et $b \equiv d\ [n]$ implique $a + b \equiv c + d\ [n]$. ■

Ce lemme rend licite la définition suivante, car la somme de deux entiers modulo n ne dépend pas du choix de leurs représentants.

Définition 8 : Loi $+$

Si $a, b \in \mathbb{Z}$, on pose $\overline{a} + \overline{b} = \overline{a+b}$, ce qui définit une loi de composition interne $+$ sur $\mathbb{Z}/n\mathbb{Z}$.

Propriété 12 : Structure de groupe additif

$\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est un groupe commutatif isomorphe à $\left(\mathbb{U}_n, \times\right)$.

Démonstration

En effet,

- $+$ est une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$,
- commutative car si $a, b \in \mathbb{Z}$, $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{a} + \overline{b}$,
- d'élément neutre $\overline{0}$ car pour tout $a \in \mathbb{Z}$, $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$,
- associative car si $a, b, c \in \mathbb{Z}$,

$$\left(\overline{a} + \overline{b}\right) + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \left(\overline{b} + \overline{c}\right),$$

- si $a \in \mathbb{Z}$, $\overline{a} + \overline{-a} = \overline{0}$ donc $\overline{-a} = -\overline{a}$ est l'opposé de $\overline{a}$.

De plus, on remarque que si $k \equiv \ell\ [n]$, alors $\mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} = \mathrm{e}^{\frac{2\mathrm{i}\ell\pi}{n}}$ ne dépend pas du choix du représentant de $\overline{k}$.

Donc $f : \left|\begin{array}{ccc} \left(\mathbb{Z}/n\mathbb{Z}, +\right) & \longrightarrow & \left(\mathbb{U}_n, \times\right) \\ \overline{k} & \longmapsto & \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} \end{array}\right.$ est

- bien définie,
- un morphisme car pour tout $k, \ell \in \mathbb{Z}$, $f\left(\overline{k} + \overline{\ell}\right) = f\left(\overline{k}\right) f\left(\overline{\ell}\right)$,
- injectif car $\operatorname{Ker} f = \left\{\overline{k},\ \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} = 1\right\} = \left\{\overline{k},\ n|k\right\} = \left\{\overline{0}\right\}$
- bijectif car de plus $|\mathbb{Z}/n\mathbb{Z}| = n = |\mathbb{U}_n|$. ■

Remarque

R 12 – On a alors facilement, pour $k \in \mathbb{Z}$, $k \cdot \overline{a} = \overline{ka}$.

Exemple

E 11 – Table d'addition dans $\mathbb{Z}/4\mathbb{Z}$.

VII Morphismes (MP2I)

1 Définition

Définition 9 : Morphisme de groupe

Soient $(G,\star)$ et $(G',\bullet)$ deux groupes.
$f:(G,\star)\to(G',\bullet)$ est un **morphisme de groupes** si et seulement si

$$\forall\,(x,y)\in G^2,\quad f(x\star y)=f(x)\bullet f(y)$$

Lorsque $(G,\star)=(G',\bullet)$, on parle d'**endomorphisme** de groupes.
Lorsque f est bijective, on parle d'**isomorphisme**.
Lorsqu'il existe un isomorphisme entre G et G', on dit que G et G' sont **isomorphes.**
Lorsque f est bijective et $G=G'$, on parle d'**automorphisme**.

Exemple

E 12 – $\ln:(\mathbb{R}_+^*,\times)\to(\mathbb{R},+)$ isomorphisme de groupes.

E 13 – $\exp:(\mathbb{R},+)\to(\mathbb{R}_+^*,\times)$ isomorphisme de groupes.

E 14 – $\begin{array}{ccc}(\mathbb{R},+)&\longrightarrow&(\mathbb{U},\times)\\ \theta&\longmapsto&\mathrm{e}^{\mathrm{i}\theta}\end{array}$ morphisme de groupes (non injectif).

E 15 – Si $n\in\mathbb{N}^*$, $\sigma\in\mathfrak{S}_n$, $\varepsilon(\sigma)$ sa signature[a], alors $\varepsilon:(\mathfrak{S}_n,\circ)\to(\{-1,1\},\times)$ est un morphisme de groupes, c'est-à-dire

$$\forall\,\sigma,\sigma'\in\mathfrak{S}_n,\quad\varepsilon\left(\sigma\circ\sigma'\right)=\varepsilon(\sigma)\times\varepsilon\left(\sigma'\right).$$

E 16 – $\det:(\mathrm{GL}(E),\circ)\to(\mathbb{R}^*,\times)$ et $\det:(\mathrm{GL}_n(\mathbb{K}),\times)\to(\mathbb{R}^*,\times)$ sont des morphismes de groupes.

a. C'est-à-dire $(-1)^{I(\sigma)}$ où $I(\sigma)$ est le nombre d'inversions de σ ou encore $(-1)^N$ si σ s'écrit comme produit (composée) de N transpositions.

Propriété 13 : Image du neutre et du symétrique par un morphisme de groupes

Si $f:(G,\star)\to(G',\bullet)$ est un morphisme de groupes, alors $f(e_G)=e_{G'}$ et pour tout $x\in G$, $f(\mathrm{sym}(x))=\mathrm{sym}(f(x))$.

Remarque

R 13 – En notation multiplicative : $f\left(x^{-1}\right)=(f(x))^{-1}$.
En notation additive : $f(-x)=-f(x)$.
On peut avoir un mix des deux : par exemple, si c'est additif au départ et multiplicatif à l'arrivée, ça devient $f(-x)=(f(x))^{-1}$.

Démonstration

$f(e_G)=f(e_G\star e_G)=f(e_G)\star f(e_G)$ donc comme $f(e_G)$ est inversible, $f(e_G)=e_{G'}$.
$f(x)\bullet f(\mathrm{sym}(x))=f\left(x\star\mathrm{sym}(x)\right)=f(e_G)=e_{G'}$
et $f(\mathrm{sym}(x))\star f(x)=f\left(\mathrm{sym}(x)\star x\right)=f(e_G)=e_{G'}$ ■

Propriété 14 : Image d'une itérée

En notation multiplicative, si $f : (G, \star) \to (G', \bullet)$ est un morphisme de groupes, pour tout $x \in G$ et pour tout $k \in \mathbb{Z}$, $f\left(x^k\right) = f(x)^k$.

Démonstration

Par récurrence pour $k \in \mathbb{N}$, puis par passage à l'inverse et d'après la propriété précédente pour $k \in \mathbb{Z}^-$. ■

Propriété 15 : Composée de morphismes

Si $f : (G, \star) \to (G', \bullet)$ et $g : (G', \bullet) \to (G'', \Delta)$ sont des morphismes de groupes, alors $g \circ f$ en est encore un.

2 Noyau et image

Définition 10 : Image et noyau d'un morphisme

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupes.

- On appelle **noyau** de f l'ensemble

$$\operatorname{Ker} f = f^{(-1)}\left(\{e_{G'}\}\right) = \{x \in G \mid f(x) = e_{G'}\} \subset G.$$

  Ainsi, $x \in \operatorname{Ker} f \iff f(x) = e_{G'}$.
- On appelle **image** de f l'ensemble

$$\operatorname{Im} f = f(G) = \{f(x),\ x \in G\} \subset G'.$$

  Ainsi, $y \in \operatorname{Im} f \iff \exists\, x \in G,\ \ y = f(x)$.

Exemple

E 17 – $f : \left| \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array} \right.$: $\operatorname{Ker} f = 2\pi\mathbb{Z}$.

Propriété 16 : Caractérisations de l'injectivité et de la surjectivité

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupe.

- *f est injectif si et seulement si $\operatorname{Ker} f = \{e_G\}$.*
- *f est surjectif si et seulement si $\operatorname{Im} f = G'$.*

Remarque

R 14 – Ainsi, f est injective si et seulement si $f(x) = e_{G'} (= f(e_G)) \implies x = e_G$!

Démonstration

- Remarquons qu'on a toujours $e_G \in \operatorname{Ker} f$ car $f(e_G) = e_{G'}$.
  Si f est injectif, alors $x \in \operatorname{Ker} f \iff f(x) = e_{G'} = f(e_G) \iff x = e_G$, donc $\operatorname{Ker} f = \{e_G\}$.

Si $\mathrm{Ker}\, f = \{e_G\}$ et si $f(x) = f(x')$, alors (en notation multiplicative)

$$e'_G = f(x) \bullet \left(f(x')\right)^{-1} = f(x) \bullet f\left(x'^{-1}\right) = f\left(x \star x'^{-1}\right)$$

donc $x \star x'^{-1} \in \mathrm{Ker}\, f$ donc $x \star x'^{-1} = e_G$ donc $x = x'$.
f est bien injectif.

- La caractérisation est valable pour les fonctions en général. Par définition,

$$f \text{ est surjective} \iff \mathrm{Im}\, f = \{f(x),\ x \in G\} = G'$$

Exemple

E 18 – La fonction f de l'exemple précédent est donc non injective car $\mathrm{Ker}\, f = 2\pi\mathbb{Z} \neq \{0\}$.

Propriété 17 : Images directe et réciproque d'un sous-groupe

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupes.

(i) Si H est un sous-groupe de $(G, \star)$, alors $f(H)$ est un sous-groupe de $(G', \bullet)$

(ii) Si H' est un sous-groupe de $(G', \bullet)$, $f^{(-1)}(H')$ est un sous-groupe de $(G, \star)$.

Démonstration

- $f(H)$ est un sous groupe de $(G', \bullet)$:
  - $f(H) \subset G'$
  - $f(H) \neq \varnothing$ car $H \neq \varnothing$
  - Si $y, y'\ \inf(H)$, on a $x, x' \in H$ tels que $y = f(x)$ et $y' = f(x')$. f étant un morphisme de groupes,

$$y \bullet y'^{-1} = f(x) \bullet f(x')^{-1} = f(\underbrace{x \star x'^{-1}}_{\in H}) \in f(H).$$

- $f^{(-1)}(H')$ est un sous groupe de G :
  - $f^{(-1)}(H') \subset G$
  - $f^{(-1)}(H') \neq \varnothing$ car $e_G\ \inf^{(-1)}(H')$ car $f(e_G) = e_{G'} \in H'$.
  - Si $x, x'\ \inf^{(-1)}(H')$, f étant un morphisme de groupes, $f\left(x \star x'^{-1}\right) = \underbrace{f(x)}_{\in H'} \bullet \underbrace{f(x')}_{\in H'}^{-1} \in H'$, donc $x \star x'^{-1} \in f^{(-1)}(H')$.

Corollaire 4 : Cas particulier du noyau et de l'image

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupes.
Alors $\mathrm{Ker}\, f$ est un sous-groupe de $(G, \star)$ et $\mathrm{Im}\, f$ est un sous-groupe de $(G', \bullet)$.

Démonstration

- $\mathrm{Ker}\, f = f^{(-1)}\left(\{e_{G'}\}\right)$ avec $\{e_{G'}\}$ sous-groupe de $(G', \bullet)$
- $\mathrm{Im}\, f = f(G)$ avec G sous-groupe de $(G, \star)$.

Exemple

E 19 – $f : \left|\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array}\right.$ étant un morphisme de groupes, $\mathrm{Im}\, f = \mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, \times)$ et

$\mathrm{Ker}\, f = 2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$.
$\mathbb{U}$ est aussi le noyau du morphisme $|\cdot| : \mathbb{C}^* \to \mathbb{R}^*$.

E 20 – $f : \left| \begin{array}{ccc} (\mathbb{C}^*, \times) & \longrightarrow & (\mathbb{C}^*, \times) \\ z & \longmapsto & z^n \end{array} \right.$ étant un morphisme de groupes, $\mathrm{Ker}\, f = \mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$. C'est aussi l'image du morphisme $k \in \mathbb{Z} \mapsto \mathrm{e}^{\frac{2ik\pi}{n}}$.

3 Isomorphismes

Propriété 18 : Réciproque d'un isomorphisme

Soit $f : (G, \star) \to (G', \bullet)$ un isomorphisme de groupes.
Alors f^{-1} est un isomorphisme du groupe $(G', \bullet)$ sur le groupe $(G, \star)$.

Démonstration

f^{-1} est bijective, et si $y, y' \in G'$, alors, comme f est un morphisme de groupes,

$$f^{-1}(y \bullet y') = f^{-1}\left(f\left(f^{-1}(y)\right) \bullet f\left(f^{-1}(y')\right)\right) = f^{-1}\left(f\left(f^{-1}(y) \star f^{-1}(y')\right)\right) = f^{-1}(y) \star f^{-1}(y').$$

Remarque

R 15 – « Être isomorphe à » est une relation d'équivalence sur l'ensemble des groupes.

VIII GROUPES MONOGÈNES (MPI)

1 Sous-groupes engendré par une partie

Définition 11 : Groupe engendré par une partie

Soit $(G, *)$ un groupe, A partie non vide de G.
On appelle **sous-groupe engendré par** A le plus petit (au sens de l'inclusion) sous-groupe de G contenant A, noté $\langle A \rangle$.
On dit alors que A est une **partie génératrice** de $\langle A \rangle$.

Remarque

R 16 – À mettre en parallèle avec la définition de Vect en algèbre linéaire.

Propriété 19 : Éléments de $\langle A \rangle$

Les éléments de $\langle A \rangle$ sont exactement les produits (pour $*$) d'éléments de A ou de A^{-1}.
Autrement dit, $x \in \langle A \rangle$ si et seulement s'il existe $k \in \mathbb{N}$, $(a_1, \ldots, a_k) \in A^k$ et $(\varepsilon_1, \ldots, \varepsilon_k) \in \{-1, 1\}^k$ tel que

$$x = a_1^{\varepsilon_1} * \cdots * a_k^{\varepsilon_k}.$$

Démonstration

On note H l'ensemble de tels éléments.
On vérifie que H est un sous-groupe de $(G,*)$ par caractérisation (partie non vide de G stable par $*$ et par inverse).
Puis tout sous-groupe de G contenant A contient nécessairement H par stabilités.
Donc H est bien le plus petit sous-groupe de G contenant A : $H = \langle A \rangle$. ■

Remarque

R 17 – On a aussi que $\langle A \rangle$ est l'intersection de tous les sous-groupes contenant A (car c'est un sous-groupe, contenant A, plus petit que tous les autres.)

Exemple

E 21 – $\mathfrak{S}_n$ est engendré par les cycles.
(Toute permutation se décompose en produit de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.)

E 22 – $\mathfrak{S}_n$ est engendré par les transpositions.
(Les cycles eux-mêmes se décomposent en produit de transpositions. Cette fois, il n'y a plus unicité de la décomposition, mais seulement de la parité du nombre de termes.)

E 23 – Soit $\mathbb{K}$ un corps. $\mathrm{GL}_n(\mathbb{K})$ est engendré par les matrices de transvection $T_{i,j}(\lambda)$ (avec $i \neq j$), de dilatation $D_i(a)$ (avec $a \neq 0$) et de permutation $P_{i,j}$.
(C'est une conséquence du pivot de Gauß : par opérations élémentaires, on peut transformer une matrice inversible en I_n.)

2 Groupes monogènes et cycliques

Propriété 20 : Sous-groupe engendré par un élément

*Soit $a \in G$. Le sous-groupe **engendré par** a noté $\langle a \rangle$ plutôt que $\langle \{a\} \rangle$ est*

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

*On dit que a en est un **générateur**.*

Remarque

R 18 – En notation additive, on a $\langle a \rangle = \{ka,\ k \in \mathbb{Z}\}$.

Définition 12 : Groupe monogène

Un groupe G est dit **monogène** s'il est engendré par un seul élément, c'est-à-dire s'il existe $a \in G$ tel que $G = \langle a \rangle$.
Un groupe G est dite **cyclique** si et seulement s'il est monogène et fini.

Exemple

E 24 – Tout sous-groupe de $(\mathbb{Z},+)$ est monogène.

E 25 – $(\mathbb{U}_n,\times)$ est cyclique engendré par $\mathrm{e}^{\frac{2i\pi}{n}}$.

Propriété 21 : Groupe cyclique $\mathbb{Z}/n\mathbb{Z}$

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique, dont les générateurs sont exactement les $\overline{k}$ avec $k \wedge n = 1$.

Démonstration

On a en effet $\mathbb{Z}/n\mathbb{Z} = \{a \cdot \overline{1}, a \in \mathbb{Z}\} = \langle \overline{1} \rangle$ fini.
Si $k \wedge n = 1$, alors on a une relation de Bézout $ku + nv = 1$ avec $u, v \in \mathbb{Z}$. Alors pour tout $a \in \mathbb{Z}$, $a = auk + nva \equiv auk \ [n]$ donc $\overline{a} = au\overline{k}$ donc $\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle$.
Si, réciproquement, $\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle$, alors on a $a \in \mathbb{Z}$ tel que $\overline{1} = a\overline{k} = \overline{ak}$ donc on a $\ell \in \mathbb{Z}$ tel que $1 = ak + n\ell$ donc $n \wedge k = 1$ par théorème de Bézout. ■

Exercice 5 : Montrer que les générateurs de $\mathbb{U}_n$ sont les $\mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}$ avec $k \wedge n = 1$, appelées racines primitives n^{e} de l'unité.

S'obtient à partir de la propriété précédente via l'isomorphisme de groupe entre $\mathbb{U}_n$ et $\mathbb{Z}/n\mathbb{Z}$.
On peut aussi reprendre la démonstration : si $k \wedge n = 1$, alors on a une relation de Bézout $ku + nv = 1$ avec $u, v \in \mathbb{Z}$. Alors pour tout $a \in \mathbb{Z}$,

$$\mathrm{e}^{\frac{2\mathrm{i}a\pi}{n}} = \mathrm{e}^{\frac{2\mathrm{i}(auk+nva)\pi}{n}} = \mathrm{e}^{\frac{2\mathrm{i}auk\pi}{n}} = \left(\mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}\right)^{au}$$

donc $\mathbb{U}_n = \left\langle \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} \right\rangle$.
Si, réciproquement, $\mathbb{U}_n = \left\langle \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} \right\rangle$, alors on a $a \in \mathbb{Z}$ tel que $\mathrm{e}^{\frac{2\mathrm{i}\pi}{n}} = \mathrm{e}^{\frac{2\mathrm{i}ak\pi}{n}}$ donc on a $\ell \in \mathbb{Z}$ tel que $1 = ak + n\ell$ donc $n \wedge k = 1$ par théorème de Bézout.

Exemple : À observer sur un dessin

E 26 – Générateurs de $\mathbb{Z}/6\mathbb{Z}$ et détails de la génération pour $n = 5$ par exemple.

3 Ordre d'un élément dans un groupe

$(G, *)$ est un groupe d'élément neutre e.

Définition 13 : Ordre d'un élément

On dit que $a \in G$ est **d'ordre fini** s'il existe $k \in \mathbb{N}^*$ tel que $a^k = e$.
Dans ce cas, on appelle **ordre de** a le plus petit $k \in \mathbb{N}^*$ tel que $a^k = e$.

Remarque

R 19 – $f : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & a^k \end{array} \right.$ est un morphisme de groupe donc son noyau est de la forme $m\mathbb{Z}$ où $m \in \mathbb{N}$.
Soit $m = 0$ et a n'est pas d'ordre fini (sa seule puissance égale à e est a^0.)
Soit $m > 0$ et m est le plus petit élément > 0 du noyau de f : il s'agit de l'ordre de a.

Exemple : À observer sur un dessin

E 27 – Dans $\mathbb{U}_6$, $\mathrm{e}^{5\mathrm{i}\pi/3}$ est d'ordre 6 et $\mathrm{e}^{2\mathrm{i}\pi/3}$ est d'ordre 3.

Exercice 6 : Sans calcul ! Montrer que $\begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$ est d'ordre fini.

Exercice 7 : Caractériser dans $(\mathbb{U}, \times)$ les $e^{i\theta}$ qui sont d'ordre fini.

Propriété 22 : de l'ordre d'un élément

Soit a un élément de G d'ordre fini m.

- *Si $k \in \mathbb{Z}$, $a^k = e$ si et seulement si $k \in m\mathbb{Z}$ ie m divise k.*
- *$\langle a \rangle = \{a^k, k \in [\![0, m-1]\!]\}$ et $|\langle a \rangle| = m$.*

Démonstration

- Avec $f : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & a^k \end{array} \right.$, $\operatorname{Ker} f = m\mathbb{Z}$ d'où le résultat.
- On a déjà $\{a^k, k \in [\![0, m-1]\!]\} \subset \langle a \rangle$.
  Puis, si $k \in \mathbb{Z}$, par division euclidienne, on a $q, r \in \mathbb{Z}$ tel que $k = mq + r$ avec $0 \leqslant r \leqslant m-1$ et alors $a^k = (a^m)^q * a^r = a^r$ d'où l'autre inclusion.
  Puis, les termes sont deux à deux distincts car si $a^k = a^\ell$ avec $0 \leqslant k \leqslant \ell \leqslant m-1$, alors $a^{\ell-k} = e$ donc par minimalité de m, $k = \ell$.
  D'où le cardinal égal à m.

Remarque

R 20 – Ainsi, $a^k = a^\ell$ peut se traduire par la congruence $k \equiv \ell \ [n]$.

Exercice 8

Soit $(G, *)$ un groupe commutatif. On suppose que g_1 et g_2 sont d'ordres n_1 et n_2.

1. **On suppose n_1 et n_2 premiers entre eux. Montrer que $g_1 * g_2$ est d'ordre fini et calculer cet ordre.**
2. **Si $G = \mathrm{GL}_2(\mathbb{R})$, $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$, vérifier que A et B sont d'ordre fini, mais pas AB.**
3. **Si n_1 et n_2 ne sont pas premiers entre eux, montrer que $g_1 * g_2$ n'est pas nécessairement d'ordre $n_1 n_2$ ou $n_1 \vee n_2$.**
4. - **Si d_1 est un diviseur de n_1, montrer qu'il existe un élément d'ordre d_1 dans G.**
   - **En déduire que G admet des éléments d'ordre $n_1 \vee n_2$.**
   - **Si G est fini, montrer que G admet un élément d'ordre le ppcm de l'ordre des éléments de G.**

1. $(g_1 * g_2)^{n_1 n_2} = g_1^{n_1 n_2} g_2^{n_1 n_2} = e$ donc $g_1 * g_2$ est d'ordre fini $n | n_1 n_2$.
   On a $g_1^n * g_2^n = e$ donc $g_1^n = g_2^{-n}$ donc $g_1^{n n_2} = g_2^{-n n_2} = e$ donc $n_1 | n n_2$.
   Or $n_1 \wedge n_2 = 1$ donc, par lemme de Gauß, $n_1 | n$. Par symétrie, $n_2 | n$ aussi.
   Et comme $n_1 \wedge n_2 = 1$, $n_1 n_2 | n$.
   Par positivité, $n = n_1 n_2$.
2. $A^2 = -I_2$ donc $A^4 = I_2$ et $B^3 = I_2$. Pour tout $n \in \mathbb{N}^*$, $(AB)^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \neq 0_2$.
3. Si g_1 est d'ordre $n_1 \geqslant 2$, et g_1^{-1} est d'ordre n_1 et $g_1 * g_1^{-1} = e$ est d'ordre $1 \notin \{n_1, n_1^2\}$...
4. - $n_1 = d_1 k_1$ et $g_1^{k_1}$ est d'ordre d_1.
   - On écrit les décompositions primaires : $n_1 = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ et $n_2 = p_1^{\beta_1} \cdots p_m^{\beta_m}$ avec des exposants éventuellement nuls. Puis, $n_1 \wedge n_2 = p_1^{\max(\alpha_1, \beta_1)} \cdots p_m^{\max(\alpha_m, \beta_m)}$.
     Avec la première partie de la question, on construit à partir de g_1 ou de g_2 des éléments d'ordre $p_i^{\max(\alpha_i, \beta_i)}$, puis avec la question 1, on obtient en les composant un élément d'ordre $n_1 \wedge n_2$.
   - Si G est fini, on répond à la question en itérant le procédé précédent avec tous les éléments de G en remarquant que $n_1 \vee \cdots \vee n_k = (\cdots((n_1 \vee n_2) \vee n_2) \cdots)$.

Propriété 23 : Morphie des groupes monogènes

Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$.
Tout groupe monogène fini (donc cyclique) de cardinal n est isomorphe à $(\mathbb{U}_n,+)$ et à $(\mathbb{Z}/n\mathbb{Z},+)$

Démonstration

Si G est engendré par a et infini, $f : \left|\begin{array}{ccc}(\mathbb{Z},+) & \longrightarrow & (G,*)\\ k & \longmapsto & a^k\end{array}\right.$ alors f est un morphisme de groupes surjectif car $G=\langle a\rangle$, et injectif car si $k\in\operatorname{Ker} f$, $a^k=1$ donc a d'ordre fini, donc G est fini.

Si G est engendré par a et de cardinal n, alors a est d'ordre n, donc $a^n=e$, $f : \left|\begin{array}{ccc}(\mathbb{Z}/n\mathbb{Z},+) & \longrightarrow & (G,*)\\ \overline{k} & \longmapsto & a^k\end{array}\right.$ est bien définie (quel que soit le représentant k de $\overline{k}$, la valeur de a^k est la même car $a^n=e$), est un morphisme de groupe et est surjectif, donc est un isomorphisme car $n=|\mathbb{Z}/n\mathbb{Z}|=|G|$. ■

Théorème 2 : de Lagrange (HP mais très classique)

Soit $(G,*)$ un groupe fini, H un sous-groupe de G. Alors $|H|$ divise $|G|$.

Démonstration

On montre que la relation définie par $x\mathcal{R}y \iff x^{-1}*y\in H$ est une relation d'équivalence sur G (facile).

Puis on montre que toutes les classes d'équivalence ont même cardinal : celui de H. En effet, il s'agit des $xH=\{x*h, h\in H\}$ et l'application (translation) $f : h\mapsto x*h$ est une bijection de H sur xH (de réciproque $h\mapsto x^{-1}*h$.)

Comme les classes d'équivalences forment une partition de G, $|G|=n\,|H|$ où n est le nombre de classes, d'où le résultat. ■

Propriété 24 : de l'ordre

Soit $(G,*)$ un groupe fini de neutre e.

(i) Tout élément de G est d'ordre fini.

(ii) L'ordre de tout élément de G divise le cardinal de G.

(iii) Pour tout $a\in G$, $a^{|G|}=e$.

Démonstration

(i) $\langle a\rangle$ est un sous-groupe de G, donc d'ordre fini. Donc on a $i<j$ tel que $a^i=a^j$ et $a^{j-i}=e$ avec $j-i\in\mathbb{N}^*$.

(ii) L'ordre de a est la cardinal du sous-groupe $\langle a\rangle$ de G, donc d'après le théorème de Lagrange (HP), il divise celui de G.

Seule la démonstration dans le cas commutatif est au programme.

En effet, dans ce cas, on considère le produit $\left(\prod_{x\in G} x\right)\in G$ et on effectue le changement de variable (bijectif) $x\mapsto a*x$.

Par commutativité, on obtient $\prod_{x\in G} x=\prod_{x\in G}(a*x)=a^{|G|}\prod_{x\in G} x$. Comme $\prod_{x\in G} x$ est régulier (car inversible), on en déduit que $a^{|G|}=e$.

(iii) Conséquence du (ii). ■

Exercice 9 : Quels sont les sous-groupes finis de $(\mathbb{C}^*,\times)$?

Soit G un sous-groupe fini de $(\mathbb{C}^*,\times)$. Tous ses éléments sont d'ordre fini, divisant l'ordre du groupe. Soit $d=|G|$. Tous les éléments de G vérifient $z^d=1$. Donc G est inclus dans $\mathbf{U}_d$. Mais ils ont même cardinal, ils sont donc égaux.

IX Groupes symétriques (MP2I)

1 Définition, structure

Définition 14 : Permutation, groupe symétrique

Si E est un ensemble, on appelle **permutation** de E toute bijection de E dans E. On note $\mathfrak{S}(E)$ leur ensemble.

Si $E = [\![1, n]\!]$ où $n \in \mathbb{N}^*$, on note $\mathfrak{S}_n$ appelé **groupe symétrique d'ordre n (ou de degré n)** cet ensemble.

Si $\sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & 3 \cdots\cdots n \\ \sigma(1) & \sigma(2) & \sigma(3) \cdots\cdots \sigma(n) \end{pmatrix}$.

Remarque

R 21 – Attention ! $\mathfrak{S}_n$ n'est pas de cardinal n mais $n!$ (!)

R 22 – Comme $\mathfrak{S}_n$ est fini, toute permutation est d'ordre fini, divisant $n!$ (théorème de Lagrange).

Propriété 25 : Structure

$(\mathfrak{S}_n, \circ)$ est un groupe d'ordre (ie *de cardinal*) *$n!$, non abélien dès que $n \geqslant 3$.*

Définition 15 : Orbites

Soit $\sigma \in \mathfrak{S}_n$. La relation binaire définie sur $[\![1, n]\!]$ par

$$x \sim y \iff \exists\, k \in \mathbb{Z},\ \ y = \sigma^k(x)$$

est une relation d'équivalence dont les classes d'équivalence sont les **orbites** de σ.

Si $x \in [\![1, n]\!]$,

$$\mathcal{O}(x) = \left\{\sigma^k(x),\ k \in \mathbb{Z}\right\}.$$

Propriété 26 : Description d'une orbite

Soit $\sigma \in \mathfrak{S}_n$, $x \in [\![1, n]\!]$. Alors il existe $\ell \in \mathbb{N}$ tel que $\mathcal{O}(x) = \{x, \sigma(x), \ldots, \sigma^{\ell-1}(x)\}$ (deux à deux distincts).

Démonstration

$\{k \in \mathbb{N}^*,\ \sigma^k(x) = x\}$ est une partie non vide de $\mathbb{N}$ donc admet un minimum ℓ.

Il suffit ensuite, si $k \in \mathbb{Z}$, de poser la division euclidienne de k par ℓ. Les éléments sont bien distincts par minimalité de ℓ. ■

Remarque

R 23 – $\ell \leqslant$ ordre(σ).

Définition 16 : Support

Si $\sigma \in \mathfrak{S}_n$, son **support** est l'ensemble des éléments de $[\![1, n]\!]$ qui **ne sont pas** invariants par σ.

Remarque

R 24 – C'est la réunion de toutes les orbites non réduites à un élément.

Propriété 27 : Commutation de permutations à supports disjoints

(i) *Le support d'une permutation est stable par cette permutation.*

(ii) *Deux permutations à supports disjoints commutent.*

Démonstration

On commence par vérifier que $\mathrm{Supp}(\sigma)$ est stable par σ : si $i \in \mathrm{Supp}(\sigma)$, $\sigma(i) \neq i$ donc $\sigma^2(i) \neq \sigma(i)$ par injectivité, donc $\sigma(i) \in \mathrm{Supp}(\sigma)$.

Soient σ et σ' à supports S et S' disjoints.

- Si $i \notin S \sqcup S'$, $\sigma \circ \sigma'(i) = i = \sigma' \circ \sigma(i)$.
- Si $i \in S$, $i \notin S'$ donc $\sigma'(i) = i$ et $\sigma \circ \sigma'(i) = \sigma(i)$.
  Mais $\sigma(i) \in S$ donc $\sigma(i) \notin S'$ d'où $\sigma' \circ \sigma(i) = \sigma(i) = \sigma \circ \sigma'(i)$.
- Si $i \notin S$, $i \in S'$ et on conclut de la même manière.

On a donc bien $\sigma' \circ \sigma = \sigma \circ \sigma'$. ■

Exercice 10 : Centre de $\mathfrak{S}_n$

1. **Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$, et $(i,j) \in [\![1,n]\!]^2$ tel que $i \neq j$. Montrer que si $\sigma \in \mathfrak{S}_n$ et $(i\ j)$ commutent, $\{i,j\}$ est stable par σ. La réciproque est-elle vraie ?**
2. **Montrer que, pour $n \in \mathbb{N}$ tel que $n \geqslant 3$ le centre de $\mathfrak{S}_n$, partie de $\mathfrak{S}_n$ des permutations commutant avec toutes les permutations de $\mathfrak{S}_n$ est $\mathcal{Z}(\mathfrak{S}_n) = \{\mathrm{id}_{[\![1,n]\!]}\}$. Étudier le cas où $n = 2$.**

---

1. Si $\sigma \circ (i\ j) = (i\ j) \circ \sigma$, en évaluant en i, $\sigma(j) = (i\ j)(\sigma(i)) \neq \sigma(i)$ par injectivité donc $\sigma(i)$ est dans le support de $(i\ j)$ donc dans $\{i,j\}$.
   Par symétrie, c'est aussi le cas de $\sigma(j)$.
   Pour la réciproque qui est bien vraie, il y a deux cas :
   - Ou bien $\sigma(i) = i$ et $\sigma(j) = j$ et alors σ et $(i\ j)$ sont à supports disjoints donc commutent.
   - Ou bien $\sigma(i) = j$ et $\sigma(j) = i$ et on vérifie que $\sigma \circ (i\ j)$ et $(i\ j) \circ \sigma$ envoient sur les mêmes images les nombres i, j et $k \notin \{i,j\}$.
2. Si $\sigma \in \mathcal{Z}(\mathfrak{S}_n)$ elle commute avec des transpositions $(i\ j)$ et $(i\ k)$ où i,j,k sont deux à deux distincts.
   Avec la question précédente, $\sigma(i) \in \{i,j\} \cap \{i,k\} = \{i\}$. Comme c'est vrai pour tout $i \in [\![1,n]\!]$, on en déduit que $\sigma = \mathrm{id}$. La réciproque est facile.
   $\mathcal{Z}(\mathfrak{S}_2) = \{\mathrm{id}_{[\![1,2]\!]}, (1\ 2)\} = \mathfrak{S}_2$

2 Cycles

Définition 17 : Transposition, cycle

- Une **transposition** τ est une permutation qui échange deux éléments i et j de $[\![1,n]\!]$, et laisse les autres invariants ie dont le support est $\{i,j\}$.
  On la note $\tau = (i\ j)$ ou parfois $\tau_{i,j}$.
  $\tau_{i,j}(i) = j$, $\tau_{i,j}(j) = i$ et si $k \notin \{i,j\}$, $\tau_{i,j}(k) = k$.

- Soit $p \in \mathbb{N}$ tel que $2 \leqslant p \leqslant n$.
  On appelle **p-cycle** une permutation c de $\mathfrak{S}_n$ qui permute circulairement p éléments $i_1, i_2, \dots, i_p$ de $[\![1, n]\!]$ et laisse les autres invariants ie dont le support est $\{i_1, \dots, i_p\}$ et telle que

$$c(i_1) = i_2 \ ; \ c(i_2) = i_3 \ ; \ \cdots \ ; \ c(i_{p-1}) = i_p \ ; \ c(i_p) = i_1$$

  p est la **longueur** du cycle c. On note $c = (i_1 \ i_2 \ \cdots \ i_p)$.

Exercice 11 : Conjugaison de cycle (souvent utile)

Si $\sigma \in \mathfrak{S}_n$ et c un cycle, décrire $\sigma \circ c \circ \sigma^{-1}$.

Propriété 28 : Ordre d'un cycle

Un p-cycle est d'ordre p.

Démonstration

Si $c = (i_1 \ i_2 \ \cdots \ i_p)$ est un p-cycle, on a bien $c^p = \mathrm{id}$ et pour tout $j \in [\![1, p-1]\!]$, $c^j(i_1) = i_{j+1} \neq i_1$ donc $c^j \neq \mathrm{id}$. ■

Théorème 3 : Unique décomposition en produit de cycles à supports disjoints

Toute permutation se décompose en produit (composée) de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.

Remarque

R 25 – Donc les cycles de $\mathfrak{S}_n$ engendrent $\mathfrak{S}_n$.

Démonstration

- **Analyse** : Si on a une décomposition en produit de cycles à support disjoints, alors pour tout $x \in [\![1, n]\!]$, soit x est invariant, soit x est un élément d'un et un seul des cycles qui s'écrit $\begin{pmatrix} x & \sigma(x) & \cdots\cdots & \sigma^{\ell-1}(x) \end{pmatrix}$ avec $\sigma^\ell(x) = x$ et correspond donc à l'orbite de x.
- **Synthèse** : Soient $x_1, \dots, x_m$ un élément de chaque orbite non réduite à un point. Alors $\mathcal{O}(x_i) = \{x_i, \sigma(x_i), \dots, \sigma^{\ell_i - 1}(x_i)\}$ avec $\sigma^{\ell_i}(x_i) = x_i$ et

$$\varphi = \prod_{i=1}^{m} \begin{pmatrix} x_i & \sigma(x_i) & \cdots\cdots & \sigma^{\ell_i - 1}(x_i) \end{pmatrix}$$

  est égale à σ car les images sont les mêmes pour tout élément de $[\![1, n]\!]$, chacun apparaissant dans exactement une orbite.

■

Remarque

R 26 – Par commutativité des cycles à supports disjoints, on a facilement que si m est le ppcm des ordres des cycles, $\sigma^m = \mathrm{id}$. Voir TD : montrer que le ppcm est égal à l'ordre de σ.

Corollaire 5 : Décomposition en produit de transpositions (non unique)

Toute permutation se décompose en produit (composée) de transpositions.

Remarque

R 27 – Donc les transpositions de $\mathfrak{S}_n$ engendrent $\mathfrak{S}_n$.

Démonstration

Se déduit du théorème précédent en sachant décomposer un cycle produit de transposition.
Voici deux propositions adaptables à tout cycle :

$$(1 \quad 2 \quad \cdots \quad p) \quad = \quad (1 \quad p)\,(1 \quad p-1)\,\cdots\,(1 \quad 2) \quad = \quad (1 \quad 2)\,(2 \quad 3)\,\cdots\,(p-1 \quad p)$$

Mais savoir le démontrer directement n'est pas inintéressant (technique utile dans d'autres contextes.) Par récurrence sur $n \geqslant 2$.

- **Initialisation** : pour $n = 2$, $\mathfrak{S}_2 = \{\mathrm{id}, (1\ 2)\}$ avec $\mathrm{id} = (1\ 2)^2$.
- **Hérédité** : Supposons que, pour un $n \geqslant 2$, $\mathfrak{S}_n$ est engendré par ses transpositions (HR).
  Soit $\sigma \in \mathfrak{S}_{n+1}$; on veut écrire σ comme un produit de transpositions. On va discuter suivant $\sigma(n+1)$:
  - ⋆ **1er Cas** : Si $\sigma(n+1) = (n+1)$, alors $[\![1, n]\!]$ est stable par σ, et celle-ci induit une permutation $\sigma' \in \mathfrak{S}_n$ de $[\![1, n]\!]$,
  $$\sigma' : \left| \begin{array}{ccc} [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ k & \longmapsto & \sigma(k) \end{array} \right. .$$
  Par (HR), on peut trouver des transpositions $\tau'_1, \tau'_2, \ldots, \tau'_p \in \mathfrak{S}_n$ telles que $\sigma' = \tau'_1\tau'_2\cdots\tau'_p$.
  On peut alors prolonger les τ'_i en des permutations τ_i de $[\![1, n+1]\!]$ en posant $\tau_i(n+1) = n+1$.
  On obtient la décomposition en remarquant que σ et $\tau_1\tau_2\cdots\tau_p$ coïncident sur $[\![1, n]\!]$ par définition des τ'_i et en $n+1$ qui est laissé invariant par toutes ces permutations. Donc
  $$\sigma = \tau_1\tau_2\cdots\tau_p.$$
  - ⋆ **2e Cas** : Si $\sigma(n+1) \neq (n+1)$, on se ramène au premier cas en remarquant posant
  $$\rho = (\sigma(n+1)\ \ n+1)\sigma.$$
  $\rho \in \mathfrak{S}_{n+1}$ et $\rho(n+1) = n+1$: d'après ce qui précède, on peut trouver $\tau_1, \tau_2, \ldots, \tau_p$ des transpositions de $[\![1, n+1]\!]$ telles que $\rho = \tau_1\tau_2\cdots\tau_p$.
  Alors $(\sigma(n+1)\ \ n+1)\sigma = \tau_1\tau_2\cdots\tau_p$ et donc
  $$\sigma = (\sigma(n+1)\ \ n+1)\tau_1\tau_2\cdots\tau_p$$
  ce qui prouve le résultat dans ce cas.
- **La récurrence est établie.** Remarquons qu'à chaque étape, on ajoute au plus une transposition.

3 Signature

Définition 18 : Inversions, signature

Soit $\sigma \in \mathfrak{S}_n$. On appelle **inversion** par σ tout couple (i, j) tel que $i < j$ et $\sigma(i) > \sigma(j)$.
On note $I(\sigma)$ le nombre d'inversions par σ.
On appelle **signature** de σ le nombre $\varepsilon(\sigma) = (-1)^{I(\sigma)} \in \{-1, 1\}$.
On vérifie que $\varepsilon(\sigma) = \displaystyle\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$.
Une permutation σ est dite **paire** lorsque $I(\sigma)$ est pair et donc $\varepsilon(\sigma) = 1$. Elle est dite **impaire** dans le cas contraire.

Démonstration

Par définition,

$$\varepsilon(\sigma) = \prod_{1\leqslant i<j\leqslant n} \operatorname{sgn}(\sigma(j)-\sigma(i)) = \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(j)-\sigma(i)}{|\sigma(j)-\sigma(i)|} = \frac{\displaystyle\prod_{1\leqslant i<j\leqslant n}(\sigma(j)-\sigma(i))}{\displaystyle\prod_{1\leqslant i<j\leqslant n}|\sigma(j)-\sigma(i)|}$$

et l'on peut transformer le dénominateur en utilisant la bijectivité de σ

$$\prod_{1\leqslant i<j\leqslant n}|\sigma(j)-\sigma(i)| = \prod_{\{i,j\}\in\mathcal{P}}|\sigma(j)-\sigma(i)| = \prod_{\{k,l\}\in\mathcal{P}}|k-l| = \prod_{1\leqslant i<j\leqslant n}(j-i). \quad \blacksquare$$

Remarque

R 28 – La définition avec les inversions peut être oubliée tout de suite. Ce n'est pas ce qui importe dans la signature : il vaut mieux savoir se ramener à des cycles ou à des transpositions (voir ci-après).

Théorème 4 : Morphisme de signature

Soit $n \geqslant 2$. L'application

$$\varepsilon : \left| \begin{array}{ccc} (\mathfrak{S}_n, \circ) & \longrightarrow & (\{-1,1\}, \times) = (\mathbb{U}_2, \times) \\ \sigma & \longmapsto & \varepsilon(\sigma) \end{array} \right.$$

est un morphisme de groupe, ie si $\sigma, \sigma' \in \mathfrak{S}_n$, $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$.

Démonstration : (Non exigible)

1re méthode

$$\begin{aligned}\varepsilon(\sigma\circ\sigma') &= \prod_{\{i,j\}\in\mathcal{P}} \frac{(\sigma\circ\sigma')(j)-(\sigma\circ\sigma')(i)}{j-i} \\ &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(\sigma'(j))-\sigma(\sigma'(i))}{\sigma'(j)-\sigma'(i)} \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma'(j)-\sigma'(i)}{j-i}.\end{aligned}$$

Dans le deuxième facteur de la dernière expression, on reconnaît directement $\varepsilon(\sigma')$.
Pour le premier, il faut au préalable réindexer (grâce à la bijectivité de σ') en posant

$$\{k,\ell\} = \{\sigma'(i), \sigma'(j)\}$$

$$\prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(\sigma'(j))-\sigma(\sigma'(i))}{\sigma'(j)-\sigma'(i)} = \prod_{\{k,\ell\}\in\mathcal{P}} \frac{\sigma(k)-\sigma(\ell)}{k-\ell} = \varepsilon(\sigma).$$

2e méthode Il s'agit de comparer les nombres d'inversions de $\sigma\circ\sigma'$ aux nombres d'inversions de σ et de σ'.
Les couples $(i,j) \in [\![1,n]\!]$ tels que $i<j$, se classent en quatre cas distincts :

- $\sigma'(i) < \sigma'(j)$ et $\sigma\circ\sigma'(i) < \sigma\circ\sigma'(j)$ (on note N_1 le nombre de tels couples.)
- $\sigma'(i) < \sigma'(j)$ et $\sigma\circ\sigma'(i) > \sigma\circ\sigma'(j)$ (on note N_2 le nombre de tels couples.)
- $\sigma'(i) > \sigma'(j)$ et $\sigma\circ\sigma'(i) < \sigma\circ\sigma'(j)$ (on note N_3 le nombre de tels couples.)
- $\sigma'(i) > \sigma'(j)$ et $\sigma\circ\sigma'(i) > \sigma\circ\sigma'(j)$ (on note N_4 le nombre de tels couples.)

Le nombre d'inversion $I(\sigma')$ de σ' est le nombres de couples $(i,j) \in [\![1,n]\!]$ tels que $i<j$ tels que $\sigma'(i) > \sigma'(j)$:

$$I(\sigma') = N_3 + N_4.$$

Le nombre d'inversion $I(\sigma\circ\sigma')$ de $\sigma\circ\sigma'$ est le nombres de couples $(i,j) \in [\![1,n]\!]$ tels que $i<j$ tels que $\sigma\circ\sigma'(i) > \sigma\circ\sigma'(j)$:

$$I(\sigma\circ\sigma') = N_2 + N_4.$$

Pour le nombre d'inversions de σ, il y a un peu plus de travail : remarquons que $(i,j) \mapsto \{\sigma'(i), \sigma'(j)\}$ est une bijection de l'ensemble des couples (i,j) de $[\![1,n]\!]$ tels que $i<j$ dans l'ensemble des paires de $[\![1,n]\!]$ par bijectivité de σ'.

Or compter les couples (k,l), $k<l$ tels que $\sigma(k)>\sigma(\ell)$ revient

— à compter les paires $\{k,\ell\}$ distinctes telles que

$$\begin{cases} k<\ell \\ \sigma(k)>\sigma(\ell) \end{cases} \text{ ou } \begin{cases} k>\ell \\ \sigma(k)<\sigma(\ell) \end{cases}$$

— ou encore, par la bijection précédente, à compter les couples (i,j) de $[\![1,n]\!]$ tels que $i<j$ et

$$\begin{cases} \sigma'(i)<\sigma'(j) \\ \sigma(\sigma'(i))>\sigma(\sigma'(j)) \end{cases} \text{ ou } \begin{cases} \sigma'(i)>\sigma'(j) \\ \sigma(\sigma'(i))<\sigma(\sigma'(j)) \end{cases}$$

Ainsi,

$$I(\sigma)=N_2+N_3.$$

Finalement, $\varepsilon(\sigma)\varepsilon(\sigma')=(-1)^{2N_3+N_2+N_4}=(-1)^{N_2+N_4}=\varepsilon(\sigma\sigma')$.

Propriété 29 : de la signature

(i) Si $\sigma\in\mathfrak{S}_n$ se décompose en produit de N transpositions, $\varepsilon(\sigma)=(-1)^N$.
En particulier, cette décomposition n'est pas unique mais la parité du nombre de termes est toujours celle de la permutation.

(ii) Si c est un p-cycle, $\varepsilon(c)=(-1)^{p-1}$.

(iii) Si $\sigma\in\mathfrak{S}_n$, $\varepsilon\left(\sigma^{-1}\right)=\varepsilon(\sigma)$.

Exercice 12

Montrer que si $\sigma\in\mathfrak{S}_n$ et si p est le nombre d'orbites de σ, alors $\varepsilon(\sigma)=(-1)^{n-p}$.

4 Groupe alterné (HP)

Définition 19 : Groupe alterné

Le sous-groupe $\mathfrak{A}_n=\mathrm{Ker}(\varepsilon)$ des permutations paires de $\mathfrak{S}_n$ est appelé ***groupe alterné d'ordre n (ou de degré n)***.

Démonstration

On a bien $\mathfrak{A}_n=\mathrm{Ker}(\varepsilon)=\varepsilon^{-1}(\{1\})=\{\sigma\in\mathfrak{S}_n,\ \varepsilon(\sigma)=1\}$ sous-groupe de $\mathfrak{S}_n$.

Propriété 30

Pour tout $n\geqslant 2$, $|\mathfrak{A}_n|=\dfrac{n!}{2}$.

Démonstration

Soit τ une transposition (ou n'importe quelle autre permutation impaire), $\varphi:\left|\begin{array}{ccc}\mathfrak{A}_n & \longrightarrow & \mathfrak{S}_n\setminus\mathfrak{A}_n \\ \sigma & \longmapsto & \tau\circ\sigma\end{array}\right.$ est bijective, d'inverse $\psi:\left|\begin{array}{ccc}\mathfrak{S}_n\setminus\mathfrak{A}_n & \longrightarrow & \mathfrak{A}_n \\ \rho & \longmapsto & \tau^{-1}\circ\rho\end{array}\right.$.

Ainsi, ces sous-ensembles de $\mathfrak{S}_n$ (donc finis) vérifient $|\mathfrak{A}_n|=|\mathfrak{S}_n\setminus\mathfrak{A}_n|$ et $|\mathfrak{A}_n|+|\mathfrak{S}_n\setminus\mathfrak{A}_n|=|\mathfrak{S}_n|=n!$ donc $|\mathfrak{A}_n|=\dfrac{n!}{2}$.

Remarque

R 29 – Il y a donc autant de permutations paires que de permutations impaires dans $\mathfrak{S}_n$.

Exemple

E 28 – Décrivons $\mathfrak{S}_4$: il contient $4! = 24$ permutations.

$$\mathfrak{S}_4 = \{\mathrm{id}, (1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4), (1\,2)\circ(3\,4), (1\,3)\circ(2\,4), (1\,4)\circ(2\,3)$$
$$(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3),$$
$$(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4), (1\,3\,4\,2), (1\,4\,2\,3), (1\,4\,3\,2)\}$$

et $\mathfrak{A}_4$: il contient $24/2 = 12$ permutations.

$$\mathfrak{A}_4 = \{\mathrm{id}, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3),$$
$$(1\,2)\circ(3\,4), (1\,3)\circ(2\,4), (1\,4)\circ(2\,3)\}$$

Soit $G = \{\mathrm{id}, \sigma_1 = (1\,2)\circ(3\,4), \sigma_2 = (1\,3)\circ(2\,4), \sigma_3 = (1\,4)\circ(2\,3)\}$.

Il s'agit d'un sous-groupe commutatif de $\mathfrak{A}_4$ comme l'atteste sa table ci-contre, appelé groupe de Klein[1].

On peut montrer qu'il est isomorphe à $(\mathbb{U}_2^2, \times)$ et que tout groupe d'ordre 4 est soit isomorphe au groupe de Klein, soit isomorphe à $(\mathbb{U}_4, \times)$ (en examinant les différentes tables possibles pour la loi de groupe.)

$\circ$	id	σ_1	σ_2	σ_3
id	id	σ_1	σ_2	σ_3
σ_1	σ_1	id	σ_3	σ_2
σ_2	σ_2	σ_3	id	σ_1
σ_3	σ_3	σ_2	σ_2	id

Remarque

R 30 – On peut facilement trouver des sous-groupes de $\mathfrak{A}_4$ d'ordre 1, 2, 3, 4, et 12 mais il n'y a pas de sous-groupe d'ordre 6. On peut démontrer que ceux-ci sont soit cycliques (mais $\mathfrak{S}_4$ ne contient pas d'élément d'ordre 6), soit isomorphes au groupe diédral D_6 des isométries laissant invariant un triangle équilatéral (contenant 3 rotations et 3 symétries, engendré par une des rotations et une des symétries).

Par contre, on en trouve dans $\mathfrak{S}_4$ engendrés par un 3-cycle et une transposition facilement isomorphe à D_6 (qui est aussi isomorphe à $\mathfrak{S}_3$, par ailleurs !).