Structure de groupe

I Structure de groupe (MP2I)

Remarque : Quelques rappels

R 1 –

- **Loi de composition interne** sur un ensemble E : toute application
$$\star : \left| \begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x \star y \end{array} \right. .$$
- 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.
> - ⋆ $\left(\exists\, g \in E^E,\ \ f \circ g = g \circ f = \mathrm{id}_E\right) \iff$
> - ⋆ $\left(\exists\, g \in E^E,\ \ f \circ g = \mathrm{id}_E\right) \iff$
> - ⋆ $\left(\exists\, g \in E^E,\ \ g \circ f = \mathrm{id}_E\right) \iff$

- 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 $\left(x^{-1}\right)^{-1} = x$.

CC BY NC SA

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

E 3 – $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs de neutre 0.

E 4 – 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.

E 5 – $(\mathbb{Q}^*,\times)$, $(\mathbb{Q}_+^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}_+^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes commutatifs de neutre 1.

E 6 – 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

R 3 – Autrement dit, $x^n=\prod_{k=1}^{n}x=\underbrace{x\star\cdots\star x}_{n\text{ fois}}$.

R 4 – 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 $(x^n)^{-1}=\left(x^{-1}\right)^n$.

Notation 1 : Exposant négatif

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

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.

Corollaire 1 : Régularité dans un groupe

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

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

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.*

Corollaire 3

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

$$G = \{a \star x,\ x \in G\} = \{x \star a,\ x \in G\}\,.$$

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 $\times$, quelle est sa table ?

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.

CC BY NC SA

Remarque

R7 – 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 $(G, \star)$.

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

(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

R8 – 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
$$\begin{cases} H \subset G,\ H \neq \varnothing \quad (0_G \in H) \\ \forall\, x, y \in H,\ \ x - y \in H \end{cases}$$

Remarque

R9 – 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 $(G,\star)$.

Exercice 3 : Réunion de sous-groupes

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

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

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 $a\mathbb{Z} = \{\ldots, -2a, -a, 0, a, 2a, \ldots\}$, 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

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.

CC BY NC SA

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

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 $\left(\mathbb{U}_n, \times\right)$.

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 – $\left|\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array}\right.$ 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 $x \in G$, $f\left(\mathrm{sym}(x)\right) = \mathrm{sym}(f(x))$.

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 $f(-x) = (f(x))^{-1}$.

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

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.

CC BY NC SA

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

$$\operatorname{Ker} f =$$

Ainsi, $x \in \operatorname{Ker} f \iff f(x) = e_{G'}$.

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

$$\operatorname{Im} f =$$

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

Exemple

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

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 $f(x) = e_{G'} (= f(e_G)) \implies x = e_G$!

Exemple

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

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 $(G, \star)$.

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

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

Exemple

E 19 – $f : \left| \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array} \right.$

E 20 – $f : \left| \begin{array}{ccc} (\mathbb{C}^*, \times) & \longrightarrow & (\mathbb{C}^*, \times) \\ z & \longmapsto & z^n \end{array} \right.$

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 $(G, \star)$.

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 $k\in\mathbb{N}$, $(a_1,\dots,a_k)\in A^k$ et $(\varepsilon_1,\dots,\varepsilon_k)\in\{-1,1\}^k$ tel que

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*

*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

E 25 – $(\mathbb{U}_n,\times)$ est cyclique engendré par

CC BY NC SA

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

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique, dont les générateurs sont exactement les

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

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 $m \in \mathbb{N}$.
En distinguant les cas $m = 0$ et $m \neq 0$, on obtient des informations sur l'ordre de a.

Exemple : À observer sur un dessin

E 27 – Dans $\mathbb{U}_6$, $\mathrm{e}^{5i\pi/3}$ est d'ordre 6 et $\mathrm{e}^{2i\pi/3}$ 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 $\mathrm{e}^{i\theta}$ 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*
- $\langle a \rangle =$
- $|\langle a \rangle| =$

Remarque

R 20 – Ainsi, $a^k = a^\ell$ peut se traduire par la congruence

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.**

Propriété 23 : Morphie des groupes monogènes

Tout groupe monogène infini est isomorphe à
Tout groupe monogène fini (donc cyclique) de cardinal n est isomorphe à

Théorème 2 : de Lagrange (HP mais très classique)

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

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 $a \in G$, $a^{|G|} = e$.

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

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 $\sigma = \begin{pmatrix} 1 & 2 & 3 \cdots\cdots\cdots n \\ \sigma(1) & \sigma(2) & \sigma(3) \cdots\cdots \sigma(n) \end{pmatrix}$.

Remarque

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

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 $\mathcal{O}(x) = \left\{x, \sigma(x), \ldots, \sigma^{\ell-1}(x)\right\}$ (deux à deux distincts).

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.

CC BY NC SA

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.

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 $n = 2$.**

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 $i_1, i_2, \ldots, i_p$ de $[\![1,n]\!]$ et laisse les autres invariants ie dont le support est $\{i_1, \ldots, i_p\}$ 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.

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 $\mathfrak{S}_n$.

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 $\sigma(n+1) \neq (n+1)$,

- **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 $\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \dfrac{\sigma(j) - \sigma(i)}{j - i}$.

Une permutation σ est dite **paire** lorsque $I(\sigma)$ est pair et donc $\varepsilon(\sigma) = 1$. Elle est dite **impaire** dans le cas contraire.

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 $\sigma, \sigma' \in \mathfrak{S}_n$, $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$.

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, $\varepsilon(c) =$.

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

CC BY NC SA

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).***

Propriété 30

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

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

et $\mathfrak{A}_4$: il contient

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 !).