– Chapitre 4 : Structure de groupes –

I. Rappels sur les groupes.

I.1. Définition, exemples.

Définition 1. On appelle *groupe* tout couple de la forme $(G, *)$ où G est un ensemble et $*$ une loi de composition interne sur G vérifiant les propriétés suivantes :

1. $*$ est *associative* :

2. G possède un *élément neutre* pour la loi $*$:

3. tout élément de G possède un *symétrique* pour $*$:

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

Exemple 1. Parmi les exemples suivants, lesquels sont des groupes ?

$$(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{D}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}, \times), (\mathbb{R}^*, \times), (\mathbb{R}_+^*, \times), (\mathbb{C}^*, \times).$$

I.2. Groupe produit.

Définition 2. Soit $(G_1, \triangle)$ et $(G_2, \diamond)$ deux groupes.
On définit une loi $*$ sur le produit cartésien $G_1 \times G_2$ par :

$$\forall (x_1, x_2) \in G_1 \times G_2, \forall (y_1, y_2) \in G_1 \times G_2,\ (x_1, x_2) * (y_1, y_2) = (x_1 \triangle y_1, x_2 \diamond y_2).$$

Muni de cette loi, le produit cartésien $G_1 \times G_2$ est un groupe, appelé *groupe produit*.
La loi ainsi définie est appelée la *loi produit*.

Exemples 2.
- Le produit cartésien $\mathbb{R}^2$ peut donc être muni d'une structure de groupe en définissant la loi produit : $(x_1, x_2) + (y_1, y_2) =$
- De même pour $\mathbb{R}_+^* \times \mathbb{R}$ en posant : $(r, \theta) * (r', \theta') =$

I.3. Notion de sous-groupe.

Définition 3. Soit $(G, *)$ un groupe. On dit qu'une partie H de G est un *sous-groupe* de $(G, *)$ si :

- H est stable par la loi $*$,
- H est stable par passage au symétrique :
- H contient l'élément neutre de $(G, *)$.

Remarque 1. Si $(G, *)$ est un groupe et que l'on note e son élément neutre, alors $\{e\}$ et G sont des sous-groupes de $(G, *)$, appelés *sous-groupes triviaux*.

Exemples 3.

- $\mathbb{Z}$ est un sous-groupe de
- $\mathbb{R}_+^*$ est un sous-groupe de
- $\mathcal{U}$ et $\mathcal{U}_n$ sont des sous-groupes de
- $\mathbb{R}$ et $i\mathbb{R}$ sont des sous-groupes de

Proposition 1. Soit $(G, *)$ un groupe. Une partie H de G est un sous-groupe de G, si, et seulement si, H est non vide et vérifie :

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

Proposition 2. Tout sous-groupe muni de la loi induite, est un groupe.

Remarque 2. La plupart du temps, pour montrer qu'un ensemble (muni d'une lci) est un groupe, on montre que c'est le sous-groupe d'un groupe connu.

Proposition 3. Une intersection quelconque de sous-groupes de G est un sous-groupe de G. Autrement-dit, si $(H_i)_{i\in I}$ est un famille quelconque de sous-groupes de G, alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Démonstration.

□

⚠ Une union de de sous-groupes de G n'est en général pas un sous-groupe de G. Plus précisément :

Exercice 1. Soit H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si, et seulement si, $H \subset K$ ou $K \subset H$.

I.4. Morphisme de groupes.

Soit $(G, *)$ et $(G', \diamond)$ deux groupes.

Définition 4. On appelle *morphisme de groupes* de G dans G' toute application f de G dans G' vérifiant:

$$\forall (x, y) \in G^2,\ f(x * y) = f(x) \diamond f(y).$$

Dans le cas particulier où les deux groupes $(G, *)$ et $(G', \diamond)$ sont égaux, on dira que f est un *endomorphisme de groupe* de G.

Exemples 4. La fonction ln est un morphisme de

La fonction exp est un morphisme de

L'application $\theta \mapsto \mathrm{e}^{i\theta}$ est un morphisme de

Soit $n \in \mathbb{N}^*$. L'application $z \mapsto z^n$ est un endomorphisme de

Remarque 3. Pour n'importe quel groupe $(G, *)$, l'application constante égale à e et Id_G sont des endomorphismes de groupe.

Proposition 4. Soit f un morphisme de groupes de G (de neutre e) dans G' (de neutre e').

1. $f(e) = e'$,

2. $\forall x \in G, f(x^{-1}) = (f(x))^{-1}$

3. $\forall x \in G, \forall n \in \mathbb{Z}, f(x^n) = (f(x))^n$.

⚠ Si n est un entier négatif x^n désigne $(x^{-1})^{-n}$. Par exemple : x^{-3} signifie $(x^{-1})^3$.

Démonstration.

□

Définition 5.
On appelle *isomorphisme* de groupes de G dans G', tout morphisme de groupes bijectif de G dans G'.

On appelle *automorphisme* de groupes de G, tout morphisme de groupe bijectif de G dans G. Autrement-dit, un automorphisme est un endomorphisme bijectif.

Proposition 5. La composée de deux morphismes de groupes est un morphisme de groupes.
La réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.

Démonstration.

□

I.5. Noyau et image d'un morphisme de groupes.

Soit $(G, *)$ (de neutre e) et $(G', \diamond)$ (de neutre e') deux groupes.

Proposition 6. Soit f un morphisme de G dans G'.
- Si H est un sous-groupe de G, alors $f(H)$ est un sous-groupe de G'.
- Si H' est un sous-groupe de G', alors $f^{-1}(H')$ est un sous-groupe de G.

Rappel. $f(H) =$ $f^{-1}(H') =$.

Démonstration.

□

Définition 6. Soit f un morphisme de G dans G'. On appelle :

- *noyau* de f et on note $\text{Ker } f$ l'ensemble défini par :
$$\text{Ker } f = f^{-1}(\{e'\}) = \{x \in E \mid f(x) = e'\},$$
- *image* de f et on note $\text{Im } f$ l'ensemble défini par :
$$\text{Im } f = f(G) = \{f(x) \mid x \in G\}.$$

Proposition 7. $\text{Ker } f$ est un sous-groupe de G, et $\text{Im } f$ est un sous-groupe de G'.

Démonstration.

□

Exemples 5. Ker(ln)= et Im(ln)=

Ker(exp)= et Im(exp)=

Soit $f : \theta \mapsto \mathrm{e}^{i\theta}$ le morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$. Alors, Ker(f)=
et Im(f)=

Soit $n \in \mathbb{N}^*$ et $f : z \mapsto z^n$ l'endomorphisme de $(\mathbb{C}^*, \times)$. Alors, Ker(f)= et Im(f)=

Remarque importante. Par définition de la surjectivité, un morphisme f, de G dans G', est surjectif, si, et seulement si, $\text{Im } f = G'$.

Théorème 1. Soit f un morphisme de G dans G'. Les affirmations suivantes sont équivalentes :

1. f est injective,

2. $\text{Ker } f = \{e\}$,

3. $\forall x \in G,\ f(x) = e' \ \Rightarrow\ x = e$.

Démonstration.

□

II. Sous-groupe engendré par une partie. Partie génératrice d'un groupe.

Soit A une partie quelconque d'un groupe $(G, *)$.

Définition 7. On appelle *sous-groupe engendré par* A l'intersection de tous les sous-groupes de G contenant A. On le note $\langle A \rangle$.

Exemple 6. $\langle \varnothing \rangle =$
$\langle \{e\} \rangle =$
$\langle G \rangle =$

Proposition 8. Pour toute partie A d'un groupe $(G, *)$, $\langle A \rangle$ est le plus petit sous-groupe (au sens de l'inclusion) de $(G, *)$ contenant A. Autrement-dit :
- $\langle A \rangle$ est un sous-groupe de $(G, *)$ contenant A,
- pour tout sous-groupe H de $(G, *)$: $A \subset H \Rightarrow \langle A \rangle \subset H$.

Démonstration.

□

Exercice 2. Montrer que $A = \langle A \rangle$ si, et seulement si, A est un sous-groupe de $(G, *)$.

Remarque 5. Dans le cas particulier où $A = \{a\}$ avec a un élément de G, on notera $\langle a \rangle$ au lieu de $\langle \{a\} \rangle$. On montre que :

$$\langle a \rangle = \{ka \mid k \in \mathbb{Z}\} \quad \text{en notation additive, et} \quad \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} \quad \text{en notation multiplicative.}$$

Remarque 6. Plus généralement, on montre facilement que $\langle A \rangle$ est l'ensemble des produits d'éléments de A et d'inverses d'éléments de A :

$$\langle A \rangle = \{x_1 \cdots x_n \mid n \in \mathbb{N} \text{ et } (\forall i \in [\![1, n]\!],\ x_i \in A \text{ ou } x_i^{-1} \in A)\}.$$

Remarque 7. Si H est un sous-groupe de $(G, *)$ et si $a \in H$, alors $\langle a \rangle \subset H$.

Définition 8. On dit que A est une *partie génératrice* du groupe $(G, *)$, si le sous-groupe engendré par A est égal à G i.e. si $\langle A \rangle = G$.

III. Les sous-groupes de $(\mathbb{Z}, +)$.

Théorème 2. Une partie H de $\mathbb{Z}$ est un sous-groupe du groupe $(\mathbb{Z}, +)$ si, et seulement si, il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Autrement-dit, les sous-groupes de $(\mathbb{Z}, +)$ sont les sous-groupes de la forme $\langle n \rangle$ avec $n \in \mathbb{N}$.

Démonstration.

□

⚠ On notera que l'entier naturel n tel que $H = n\mathbb{Z}$ est unique. Dans le cas où $H \neq \{0\}$, n est défini par $n =$.

IV. Groupe monogène, groupe cyclique.

Définition 9. On dit qu'un groupe $(G, *)$ est *monogène* s'il est engendré par une partie à un seul élément i.e. s'il existe un élément a de G tel que $G = \langle a \rangle$.
Un tel élément a est appelé un *générateur* de G.

Remarque 8. Un groupe monogène est nécessairement commutatif.

Remarque importante. Si $(G, *)$ est un groupe monogène et si a est un générateur de G, on a donc :

$$G = \{ka \mid k \in \mathbb{Z}\} \quad \text{en notation additive, et} \quad G = \{a^k \mid k \in \mathbb{Z}\} \quad \text{en notation multiplicative.}$$

Exemple 7. $(\mathbb{Z}, +)$ est un groupe monogène engendré par 1 (il est aussi engendré par -1).

Définition 10. On appelle groupe *cyclique* tout groupe monogène et fini.

Rappel. Le groupe $(\mathbb{U}_n, \times)$ des racines n-ièmes de l'unité.
Soit $n \in \mathbb{N}^*$.

Par ailleurs, $\mathbb{U}_n$ est un sous-groupe du groupe $(\mathbb{C}^*, \times)$.

Géométriquement, $\mathbb{U}_n$ est l'ensemble des affixes des n sommets de l'unique polygone régulier à n côtés inscrit dans le cercle unité et passant par le point d'affixe 1.

Proposition 9. $(\mathbb{U}_n, \times)$ est un groupe cyclique engendré par $e^{\frac{2i\pi}{n}}$ i.e. engendré par ξ_1.

Démonstration. □

⚠ Déterminer tous les générateurs du groupe $(\mathbb{U}_n, \times)$ est une question importante à laquelle il faudra savoir répondre.

V. Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Soit n entier naturel.

Définition 11. On dit que deux entiers a et b sont *congrus modulo* n si n divise $a - b$, i.e. s'il existe $k \in \mathbb{Z}$ tel que : $a = b + kn$. On le note : $a \equiv b\ [n]$. On a ainsi :

$$a \equiv b\ [n] \ \Leftrightarrow\ n \mid (a-b) \ \Leftrightarrow\ \exists k \in \mathbb{Z},\ a = b + kn.$$

- On rappelle que la relation de congruence modulo n est *réflexive*, *symétrique* et *transitive* : c'est donc une *relation d'équivalence*.
- On rappelle que l'on définit la classe d'équivalence d'un élément a comme l'ensemble des éléments qui lui sont équivalents. On a donc, pour tout $a \in \mathbb{Z}$:

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b\ [n]\} = \{a + kn \mid k \in \mathbb{Z}\}.$$

- On rappelle également que l'ensemble des classes d'équivalence forme une *partition* de $\mathbb{N}$ et que pour tout $(a, b) \in \mathbb{Z}^2$:

$$a \equiv b\ [n] \ \Leftrightarrow\ \overline{a} = \overline{b}.$$

- Dans le cas de la congruence, on parle parfois de *classe de congruence*, au lieu de *classe d'équivalence*.
- L'entier a est appelé un *représentant* de $\overline{a}$. Vu ce qui précède, si $a \equiv b\ [n]$, alors b est un autre représentant de $\overline{a}$ puisque $\overline{a} = \overline{b}$.

Exercice 3. Quelles sont les classes de congruence modulo 0 ?

modulo 1 ?

modulo 2 ?

Définition 12. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence i.e. $\mathbb{Z}/n\mathbb{Z} = \{\overline{x} \mid x \in \mathbb{Z}\}$.

⚠ Dorénavant, on fera l'hypothèse que $\boxed{n \in \mathbb{N}^*}$.

Proposition 10. Pour $n \in \mathbb{N}^*$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ contient exactement n classes d'équivalence.
Plus précisément :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

Démonstration.

□

Remarque 10. On a par exemple : $\overline{0} = \overline{n}, \overline{1} = \overline{n+1}, \dots$

Lemme. Soit $(a, b, a', b') \in \mathbb{Z}^4$. Si $a \equiv a'\ [n]$ et si $b \equiv b'\ [n]$, alors : $a + b \equiv a' + b'\ [n]$.

Démonstration.

□

Proposition 11. On définit une loi d'addition sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ en posant :

$$\forall (a, b) \in \mathbb{Z}^2, \quad \overline{a} + \overline{b} = \overline{a+b}.$$

Démonstration.

⚠ Il est important de prouver que le résultat ne dépend pas des représentants a et b choisis pour les classes d'équivalence $\overline{a}$ et $\overline{b}$.

□

Exemple 8. Dans $\mathbb{Z}/6\mathbb{Z}$: $\overline{2}+\overline{3}=$
Dans $\mathbb{Z}/5\mathbb{Z}$: $\overline{2}+\overline{3}=$
Dans $\mathbb{Z}/4\mathbb{Z}$: $\overline{2}+\overline{3}=$

Proposition 12. $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe abélien.

Démonstration.

□

Remarque 11. Soit $a\in\mathbb{Z}$. Pour tout $k\in\mathbb{N}$,

$$k\overline{a}=\overline{a}+\cdots+\overline{a}=\overline{ka}.$$

Si k est un entier négatif : $k\overline{a}=$

Proposition 13. L'application, notée π_n et définie par :

$$\begin{array}{rccc}\pi_n & : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z}\\ & & x & \mapsto & \overline{x}\end{array}$$

est un morphisme de groupe. Il est surjectif et son noyau est $n\mathbb{Z}$.
Ce morphisme est appelé la *projection canonique*.

Démonstration.

□

Proposition 14. $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique engendré par $\overline{1}$.
De plus, pour tout $a\in\mathbb{Z}$, la classe $\overline{a}$ de a engendre le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ si, et seulement si, $a\wedge n=1$.

Démonstration.

□

Exemple 9. Les générateurs de $\mathbb{Z}/4\mathbb{Z}$ sont :
Les générateurs de $\mathbb{Z}/5\mathbb{Z}$ sont :
Plus généralement, si p est premier, les générateurs de $\mathbb{Z}/p\mathbb{Z}$ sont :

VI. Ordre d'un élément d'un groupe.

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

Définition 13. On dit que a est un *élément d'ordre fini* s'il existe un entier $n \in \mathbb{N}^*$ tel que $a^n = e$.
On appelle *ordre* de a le plus petit élément d de $\mathbb{N}^*$ tel que $a^d = e$.
On dit que a est un *élément d'ordre infini* s'il n'existe aucun entier $n \in \mathbb{N}^*$ tel que $a^n = e$.

Exemple 10. Le neutre est d'ordre 1. C'est d'ailleurs le seul élément d'ordre 1.

⚠ En notation additive, l'ordre de a est le plus petit élément d de $\mathbb{N}^*$ tel que $da = e$.

Exemple 11. Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}$ est d'ordre et $\overline{3}$ est d'ordre

Exemple 12. Dans $\mathbb{U}_3 = \{1, j, j^2\}$, les éléments sont respectivement d'ordre
Dans $\mathbb{U}_4 = \{1, i, -1, -i\}$, les éléments sont respectivement d'ordre

Exemple 13. L'ensemble des éléments d'ordre fini du groupe $(\mathbb{C}^*, \times)$ est :

Proposition 15. Soit $a \in G$ et soit φ l'application :

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \to & G \\ & & k & \mapsto & a^k. \end{array}$$

1. φ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(G, *)$,
2. $\mathrm{Im}(\varphi) = \langle a \rangle$,
3. a est un élément d'ordre fini si, et seulement si, φ est non injective.

Démonstration.

□

Proposition 16. Soit a un élément d'ordre fini d.

1. $\mathrm{Ker}(\varphi) = d\,\mathbb{Z}$.

2. Pour tout $n \in \mathbb{Z},\ a^n = e \Leftrightarrow d \mid n$.

3. Pour tout $(n,m) \in \mathbb{Z}^2$, $n \equiv m\ [d] \ \Leftrightarrow\ a^n = a^m$.

4. L'ordre d de a est égal au cardinal de $\langle a \rangle$. Plus précisément :

$$\langle a \rangle = \{e, a, \ldots, a^{d-1}\},$$

et les éléments de l'ensemble $\{e, a, \ldots, a^{d-1}\}$ sont 2 à 2 distincts.

⚠ L'ordre de a est donc le plus petit entier naturel d vérifiant $a^d = e$, aussi bien pour la relation d'ordre usuelle de $\mathbb{N}$ que pour la relation de divisibilité.

Démonstration.

□

Proposition 17. Si a est un élément d'ordre infini, alors les éléments de l'ensemble $\{a^k \mid k \in \mathbb{Z}\}$ sont 2 à 2 distincts. En particulier, $\langle a \rangle$ est un ensemble infini.

Démonstration. □

Remarque 12. Finalement, que a soit d'ordre fini ou pas, on peut dire que l'ordre de a est égale au cardinal de $\langle a \rangle$.

Corollaire 1. Dans un groupe fini, tout élément est d'ordre fini.

Démonstration. Conséquence de la contraposée de la proposition précédente. □

Corollaire 2. Soit $(G, *)$ un groupe fini à n éléments. Un élément a de G est générateur de G si, et seulement si, a est un élément d'ordre n.

Démonstration.

□

Exercice 4. Soit f un morphisme de groupes d'un groupe $(G, *)$ dans un groupe $(G', *)$.
On notera e et e' leur élément neutre respectif. Soit x un élément d'ordre fini, noté d.

1. Montrer que $f(x)$ est d'ordre fini. Notons d' l'ordre de $f(x)$. Quel lien y a-t-il entre d et d' ?

2. On suppose de plus que f est injective. Montrer que $d = d'$.

Exercice 5. Les groupes additifs $\mathbb{Z}/24\mathbb{Z}$ et $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$ sont-ils isomorphes ?

Exercice 6. Soit n et m deux entiers naturels non nuls. Montrer que si les groupes additifs $\mathbb{Z}/(nm)\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ sont isomorphes alors $n \wedge m = 1$.

Théorème 3. Théorème de Lagrange.
L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.

Conformément au programme, nous démontrerons ce théorème uniquement dans le cas particulier des groupes abéliens.

Démonstration. Soit $(G, *)$ un groupe fini à n éléments. Soit a un élément de G.
Comme G est fini, on a déjà vu que a est nécessairement d'ordre fini. Notons d l'ordre de a. Pour montrer que $d \mid n$ il suffit de montrer que $a^n = e$.

□

⚠ On a utilisé deux fois la commutativité du groupe.

VII. Structure des groupes monogènes.

Théorème 4. Structure des groupes monogènes.
1. Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.
2. Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration. Soit $(G, *)$ un groupe monogène. Soit a un générateur de G i.e. $G = \langle a \rangle$.

□

Représentation d'un groupe monogène infini.

Représentation d'un groupe monogène fini.

Corollaire 3. $(\mathbb{U}_n, \times)$ est un groupe cyclique de cardinal n, il est donc isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.
De plus, pour tout $k \in [\![0, n-1]\!]$, le nombre ξ_k engendre le groupe $(\mathbb{U}_n, \times)$ si, et seulement si, $k \wedge n = 1$.

Démonstration.

□

Remarque 13. Une racine n-ième de l'unité est dite *primitive* quand elle est d'ordre exactement n, i.e. quand c'est un générateur de $(\mathbb{U}_n, \times)$.

Les racines primitives 3-ième de l'unité sont : .

Les racines primitives 4-ième de l'unité sont : .

VIII. Groupe symétrique.

VIII.1. Permutations de l'ensemble $[\![1, n]\!]$.

Rappels.
- Si X est un ensemble, on appelle permutation de X, toute bijection de X dans X.
- On note $\mathcal{S}_n$ ou $\mathfrak{S}_n$ l'ensemble des permutations de l'ensemble $[\![1, n]\!]$.
- Si X est un ensemble fini de cardinal n, il y a $n!$ permutations de X. En particulier : Card $\mathcal{S}_n = n!$.
- Muni de la composition, $\mathcal{S}_n$ est un groupe, appelé le *groupe symétrique*.

Notations. Les éléments de $\mathcal{S}_n$ sont habituellement notés par des lettres grecques : σ, τ ...
Si $(\sigma, \tau) \in \mathcal{S}_n^2$, la composée $\sigma \circ \tau$ est parfois simplement notée $\sigma\tau$, et par abus de langage, est appelée produit des permutations σ et τ. De même, σ^2 désignera la composée $\sigma \circ \sigma$.

Proposition 18. Soit $(i,j) \in [\![1,n]\!]^2$ tel que $i \neq j$.
L'application σ définie par :

$$\sigma(i) = j, \quad \sigma(j) = i, \quad \text{et} \quad \forall x \in [\![1,n]\!] \setminus \{i,j\},\ \sigma(x) = x,$$

est une permutation de $[\![1,n]\!]$.
Une telle permutation est appelée *transposition* et notée (i,j).

Démonstration.

□

Bien noter que la transposition (i,j) et (j,i) sont égales.

Proposition 19. Soit $p \geqslant 2$ et $(a_1, a_2, \dots, a_p)$ des éléments deux à deux distincts de $[\![1,n]\!]$.
L'application σ définie par :

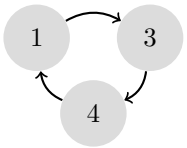
$$\begin{aligned} \forall x \in [\![1,n]\!] \setminus \{a_1, a_2, \dots, a_p\},\ \sigma(x) &= x, \\ \forall i \in [\![1,p-1]\!],\ \sigma(a_i) &= a_{i+1} \\ \sigma(a_p) &= a_1 \end{aligned}$$

est une permutation de $[\![1,n]\!]$.
Une telle permutation est appelée *p-cycle* ou *cycle d'ordre p* et notée $(a_1, a_2, \dots, a_p)$.

Démonstration.

□

Représentation du cycle $(1,3,4)$ de $\mathcal{S}_5$:



Cette représentation montre que les permutations $(1,3,4)$, $(3,4,1)$ et $(4,1,3)$ sont égales.

Définition 14. Soit $\sigma = (a_1, a_2, \dots, a_p)$ un p-cycle de $\mathcal{S}_n$. L'ensemble $\{a_1, a_2, \dots, a_p\}$ est appelé *support* du cycle σ.

Remarque 14. Soit $x \in [\![1,n]\!]$. Alors x appartient au support de σ si, et seulement si, $\sigma(x) \neq x$.

Étude de $\mathcal{S}_1$ et $\mathcal{S}_2$.
$S_1 = \{\mathrm{Id}\}$ et $\mathcal{S}_2 = \{\mathrm{Id}, (1,2)\}$. Il est donc simple d'obtenir la table de $\mathcal{S}_2$:

$\circ$	Id	$(1,2)$
Id		
$(1,2)$		

On constate, en particulier, que les groupes $\mathcal{S}_1$ et $\mathcal{S}_2$ sont abéliens (i.e. commutatifs).

Proposition 20. Si $n \geqslant 3$, alors le groupe $\mathcal{S}_n$ n'est pas abélien (i.e. n'est pas commutatif).

Démonstration. Contre-exemple : $(1,2)(1,3) =$ $(1,3)(1,2) =$. □

Remarque 15. Nous venons de voir une écriture simple, pour les permutations particulières que sont les transpositions et les cycles.
Mais une permutation quelconque peut s'écrire « matriciellement » ainsi :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

ce qui donne par exemple :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 4 & 6 & 5 & 10 & 8 & 9 & 3 & 1 & 2 \end{pmatrix}.$$

Exercice 7. Déterminer la permutation $\sigma\sigma'$ où :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \qquad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \qquad \sigma\sigma' =$$

⚠ Une puissance d'un cycle n'est pas toujours un cycle : $(1,2,3,4,5,6)^2 =$.

VIII.2. Décomposition d'une permutation.

L'exemple ci-dessus, montre que toute permutation n'est pas un cycle. Cependant, nous allons voir comment exprimer n'importe quelle permutation en un produit de cycles.

On a vu que pour $n \geqslant 3$, alors $\mathcal{S}_n$ n'est pas commutatif, mais cependant :

Proposition 21. Deux cycles à supports disjoints commutent.

Démonstration.
Soit σ_1 et σ_2 deux cycles de supports respectifs A_1 et A_2 tels que $A_1 \cap A_2 = \varnothing$.
Soit $x \in [\![1, n]\!]$. Montrons que $\sigma_1\sigma_2(x) = \sigma_2\sigma_1(x)$.

□

Théorème 5. Toute permutation (différente de l'identité) se décompose en produit de cycles à supports deux à deux disjoints.
Cette décomposition est unique à l'ordre près des facteurs.

Bien que cette démonstration soit admise, il est important de connaître l'algorithme de décomposition :

Exercice 8. On considère la permutation suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 4 & 6 & 5 & 10 & 8 & 9 & 3 & 1 & 2 \end{pmatrix}.$$

1. Déterminer la décomposition en produit de cycles à supports deux à deux disjoints de σ.
2. En déduire l'ordre de la permutation σ.

Corollaire 4. Toute permutation se décompose en produit de transpositions.

Démonstration.

□

⚠ Cette décomposition n'est pas unique : $(1,2,3) = (\ ,\ )(\ ,\ )$ et $(1,2,3) = (2,3,1) = (\ ,\ )(\ ,\ )$.

Remarque 16. Si $n = 1$, alors Id ne peut se décomposer en produit de transpositions, puisqu'il n'y a pas de transposition dans $\mathcal{S}_1$. Cependant, si $n \geqslant 2$, on peut obtenir la décomposition suivante :
$\mathrm{Id} = (\ ,\ )(\ ,\ )$.

VIII.3. Signature d'une permutation.

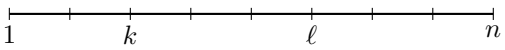
Définition 15. Soit $\sigma \in \mathcal{S}_n$. On dit qu'un couple (i,j) d'éléments de $[\![1,n]\!]$ est une *inversion* si $i<j$ et $\sigma(i)>\sigma(j)$. On note $I(\sigma)$ le nombre d'inversions de σ.

Soit la transposition $\sigma=(2,5)$. Lesquels de ces couples sont des inversions : $(1,2),(1,3),(2,3),(2,5),(3,5)$?

Définition 16. On appelle *signature* d'une permutation $\sigma \in \mathcal{S}_n$, le réel $\varepsilon(\sigma)=(-1)^{I(\sigma)}$.
On appelle permutation *paire*, toute permutation de signature 1.
On appelle permutation *impaire*, toute permutation de signature 1.

Proposition 22. Les transpositions sont des permutations impaires.

Démonstration. Soit $\tau=(k,\ell)$ une transposition avec $k<\ell$.



□

Théorème 6. Si $(\sigma,\sigma') \in \mathcal{S}_n^2$, alors $\varepsilon(\sigma\sigma')=\varepsilon(\sigma)\varepsilon(\sigma')$.
L'application ε est donc un morphisme de groupes de $(S_n,\circ)$ dans $(\{-1,1\},\times)$.

Il découle de la proposition et du théorème précédents que :

Corollaire 5. Si $\sigma=\tau_1\tau_2\cdots\tau_p$ est une décomposition de la permutation σ en produit de p transpositions, alors $\varepsilon(\sigma)=(-1)^p$.

On a vu précédemment qu'un cycle d'ordre p, $\sigma=(a_1,a_2,\ldots,a_p)$, se décompose en $p-1$ transpositions. Ainsi, $\varepsilon(\sigma)=(-1)^{p-1}$. Le théorème précédent, donne ainsi :

Corollaire 6. Si $\sigma=\tau_1\tau_2\cdots\tau_p$ est une décomposition de la permutation σ en produit de p cycles d'ordres (i.e. de longueurs) respectifs $\ell_1,\ldots,\ell_p$, alors :

$$\varepsilon(\sigma)=\prod_{i=1}^{p}(-1)^{\ell_i-1}=(-1)^{\sum_{i=1}^{p}(\ell_i-1)}.$$

Exercice 9. Donner la signature de la permutation σ de la page 17.

Remarque importante. On prouve facilement que ε est le seul morphisme de groupes de $\mathcal{S}_n$ dans $\{-1,1\}$, vérifiant : pour toute transposition τ, $\varepsilon(\tau)=-1$.

Définition 17. On appelle *groupe alterné* $\mathcal{A}_n$ l'ensemble des permutations paires de $\mathcal{S}_n$.

C'est bien un groupe puisque