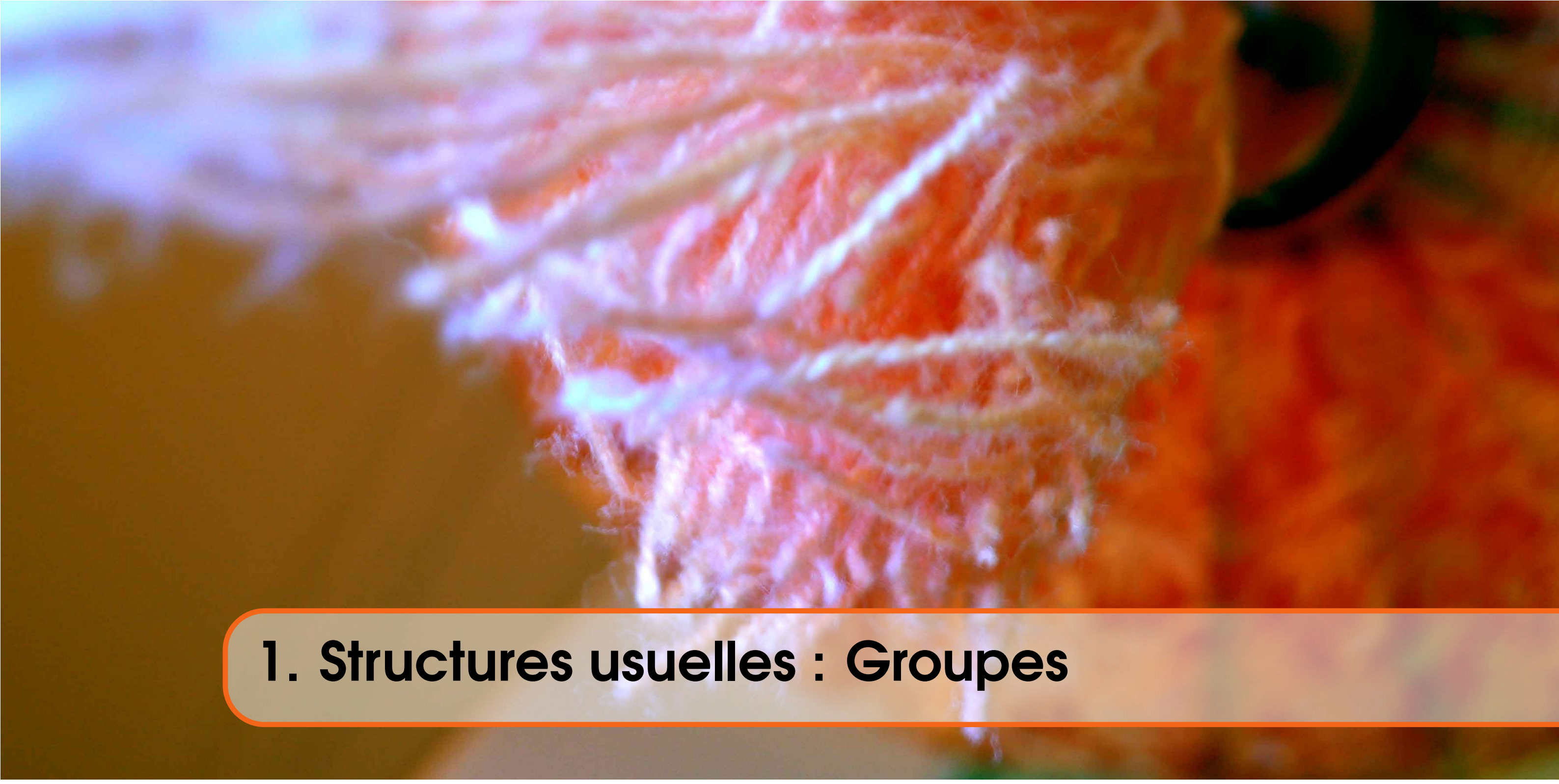

1. Structures usuelles : Groupes

1.1 Groupes

1.1.1 Généralités

Définition 1.1 Soit G un ensemble non vide muni d'une loi de composition interne $*$. On dit que $(G,*)$ est un groupe lorsque

1. l'opération $*$ est associative, c'est à dire

$$\forall x, y, z \in G, \quad (x*y)*z = x*(y*z),$$

2. l'opération $*$ admet un élément neutre (noté e), c'est à dire

$$\exists e \in G, \forall x \in G, \quad x*e = e*x = x,$$

3. et que tout élément admet un symétrique, c'est à dire

$$\forall x \in G, \exists y \in G, , \quad x*y = y*x = e.$$

Un groupe $(G,*)$ est dit commutatif ou abélien lorsque l'opération $*$ est commutative.

Notation. *Étant donné un groupe, sa loi de composition interne est souvent notée $+$, quand elle est commutative. Dans ce cas le symétrique d'un élément $g \in G$ est appelé son opposé et noté $-g$.*

Remarque Dans un groupe $(G,\cdot)$, on note en général ab le produit $a \cdot b$ de a et b dans G. Dans ce cas le symétrique d'un élément $g \in G$ est appelé son inverse et noté g^{-1} et on a

$$\forall a, b \in G, \quad (ab)^{-1} = b^{-1}a^{-1}.$$

Théorème 1.1 Dans un groupe $(G,\cdot)$ d'élément neutre e, tout élément est simplifiable, c-à-dire

$$\forall a,b,c\in G,\quad ac=bc \implies a=b \text{ et } ca=cb \implies a=b.$$

Preuve *soient a, b et c dans G tels que $ac=bc$ et soit c' le symétrique de c. Nous avons*

$$(ac)c'=(bc)c'.$$

Utilisons l'associativité de la loi interne, il vient $a(cc')=b(cc')$, d'où $ae=be$ et donc $a=b$. ■

Exemples
1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la loi $+$ usuel, sont des groupes commutatifs.
2. $(\mathbb{N},+)$ et $(\mathbb{R},\times)$ ne sont pas des groupes car il y'a des éléments qui n'ont pas de symétrique.
3. $(\mathscr{V}_2,+)$ l'ensemble des vecteurs du plan, est un groupe commutatif.

Exercice 1.1 *Dans un groupe d'élément neutre e, montrer que*

$$(a^{-1}ba=b^{-1} \text{ et } b^{-1}ab=a^{-1}) \implies a^4=b^4=e.$$

Exercice 1.2 *Soient a et b deux éléments d'un groupe $(G,\cdot)$ d'élément neutre e et n un entier naturel non nul tels que $(ab)^n=e$. Montrer que $(ba)^n=e$.*

Exercice 1.3 *Sur $G=\mathbb{R}_+^*\times\mathbb{R}$, on définit l'opération $*$ par*

$$(x,y)*(x',y')=(xx',xy'+y).$$

Montrer que $(G,*)$ est un groupe.

1.1.2 Sous groupes

Définition 1.2 Soit $(G,\cdot)$ un groupe. Une partie $H\neq\emptyset$ de G est un sous-groupe de $(G,\cdot)$ lorsque

1. le produit d'éléments de H est dans H, c'est à dire
$$\forall x,y\in H,\quad xy\in H,$$
2. tout élément de H a son inverse (symétrique) dans H, c'est à dire
$$\forall x\in H,\quad x^{-1}\in H.$$

Remarque On dit alors qu'une partie non vide H de G est un sous-groupe de $(G,\cdot)$ si elle est stable pour le produit et par le passage au symétrique.

Théorème 1.2 Une partie non vide H de G est un sous-groupe de $(G,\cdot)$ si et seulement si

$$\forall x,y\in H,\ xy^{-1}\in H.$$

Preuve *Soit H un sous-groupe de $(G,\cdot)$ et $(x,y)\in H^2$. Comme $y\in H$, alors $y^{-1}\in H$. Puis, puisque*

$(x, y^{-1}) \in H^2$, il vient $xy^{-1} \in H$. Inversement, supposons que

$$\forall x, y \in H,\ xy^{-1} \in H.$$

Comme $H \neq \emptyset$, il existe un élément $h \in H$ et donc $hh^{-1} = e \in H$ où e est l'élément neutre de $(G, \cdot)$. De plus, pour tout $x \in H$, puisque $(e, x) \in H^2$, on obtient $ex^{-1} = x^{-1} \in H$. Finalement, étant donné x et y deux éléments de H, on a $x(y^{-1})^{-1} = xy \in H$. Finalement, H est un sous-groupe de $(G, \cdot)$.

■

Corollaire 1.1 Si $(G, \cdot)$ est un groupe d'élément neutre e, tout sous-groupe H de G contient e.

Remarque 1. $e \in H$ assure que $H \neq \emptyset$ et $e \notin H$ donne que H ne peut pas être un sous-groupe.

2. Soit $(G, \cdot)$ un groupe, les sous-ensembles $\{e\}$ et G sont des sous-groupes de G. Tout sous-groupe H de $(G, \cdot)$, autre que $\{e\}$ ou G, est appelé un sous-groupe propre.

Proposition 1.1 Soit $(G, \cdot)$ est un groupe et H un de ces sous-groupes. Pour la restriction de la loi interne $\cdot$ à $H \times H$, notée encore $\cdot$, on a $(H, \cdot)$ est un groupe.

Exemple — Centre d'un groupe. On appelle centre du groupe $(G, \cdot)$, l'ensemble suivant

$$C = \{c \in G;\ \forall x \in G,\ cx = xc\}$$

Le centre C du groupe G est un sous-groupe de $(G, \cdot)$. En effet, on a

- soit e l'élément neutre de G, alors pour tout $x \in G$, on a $ex = xe$, d'où $e \in C$ et donc $C \neq \emptyset$.
- soit $(c, c') \in C$, avec l'associativité de la loi interne $\cdot$, il vient que $cc' \in C$, puisque on a

$$\forall x \in G,\ \ (cc')x = c(c'x) = c(xc') = (cx)c' = (xc)c' = x(cc').$$

- soit $c \in C$, alors pour tout $x \in G$, on a $cx = xc$ et en multipliant à gauche et à droite par c^{-1}, on obtient $c^{-1}(cx)c^{-1} = c^{-1}(xc)c^{-1}$, d'où $xc^{-1} = c^{-1}x$ et ceci montre que $c^{-1} \in C$.

Remarque De cet exemple, on déduit qu'un groupe $(G, \cdot)$ est commutatif si et seulement si

$$C = G.$$

Proposition 1.2 Soient $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, \cdot)$, l'intersection $\bigcap_{i \in I} H_i$ est encore un sous-groupe de $(G, \cdot)$.

Preuve *À faire en exercice.*

■

Définition 1.3 Soient $(G, \cdot)$ un groupe et A une partie de G. L'intersection de tous les sous-groupes contenant A est appelé le sous-groupe engendré par A, noté $gr(A)$ ou $< A >$. Et lorsque $gr(A) = G$, on dit que A est une partie génératrice de $(G, \cdot)$

Remarque 1. $A \subset G$ est un sous-groupe de G si et seulement si $A = gr(A)$, et on a le cas particulier

$$gr(\emptyset) = \{e\}.$$

2. Au sens de l'inclusion, $gr(A)$ est le plus petit sous-groupe de G qui contient A.

Définition 1.4 Un groupe $(G,\cdot)$ est dit monogène quand il admet une partie génératrice réduite à un seul élément. Et un groupe $(G,\cdot)$ est dit cyclique quand il est monogène et fini.

Exemple Les racines $n^{\text{ème}}$ de l'unité dans $\mathbb{C}$ forment un groupe multiplicatif $(U,\times)$ de cardinal n engendré par l'élément $\omega = e^{\frac{2i\pi}{n}}$. En effet, on a

$$U = \left\{e^{\frac{2ki\pi}{n}},\ k = 0,\cdots,n-1\right\} = <\omega> .$$

Par conséquent, le groupe $(U,\times)$ est cyclique, puisque il est monogène et fini.

Proposition 1.3 Le sous-groupe engendré par la partie A du groupe $(G,\cdot)$ est l'ensemble des produits d'un nombre fini d'éléments de A ou d'inverses d'éléments de A.

Preuve *Si $A=\emptyset$, on n'a rien à montrer car $gr(\emptyset)=\{e\}$. Supposons $A\neq\emptyset$ et notons Γ, l'ensemble des produits d'un nombre fini d'éléments de A ou d'inverses d'éléments de A. Il est clair que tout sous-groupe de G qui contient A, contient nécessairement Γ. Alors, il reste seulement à montrer que Γ est un sous-groupe de G. On a*

- *Γ contient l'élément neutre e de G car si h est un élément de $A\neq\emptyset$, alors $hh^{-1}=e\in\Gamma$,*
- *si $x=a_1a_2\cdots a_n\in\Gamma$ et $y=b_1b_2\cdots b_p\in\Gamma$ (c-à-dire $a_i, b_j\in A\cup A^{-1}$), alors $xy\in\Gamma$, puisque*

$$xy = c_1c_2\cdots c_{n+p} \text{ avec } c_i=a_i \text{ pour } 1\leqslant i\leqslant n \text{ et } c_i=b_{i-n} \text{ pour } n+1\leqslant i\leqslant n+p.$$

- *si $x=a_1a_2\cdots a_n\in\Gamma$ (c-à-dire $a_i\in A\cup A^{-1}$), alors $x^{-1}\in\Gamma$, puisque*

$$x^{-1}=a_n^{-1}a_{n-1}^{-1}\cdots a_1^{-1}\in\Gamma \ (\text{ car } a_i^{-1}\in A\cup A^{-1}).$$

■

Exercice 1.4 *Soit $(G,\cdot)$ un groupe et $a\in G$. Montrer que $H_a=\{x\in G, xa=ax\}$ est un sous-groupe de G.*

Exercice 1.5 *Soient $(G,\cdot)$ un groupe commutatif, 1 son élément neutre et $n\in\mathbb{N}^*$ un entier donné. Montrer que $R_n=\{a\in G, a^n=1\}$ est un sous-groupe de $(G,\cdot)$.*

Exercice 1.6 *Soit $A\neq\emptyset$ une partie d'un groupe G. Montrer que $N(A)=\{x\in G,\ x^{-1}Ax=A\}$ un sous-groupe de G.*

Exercice 1.7 *Soit A et B deux sous-groupes d'un groupe $(G,\cdot)$. Montrer que $A\cup B$ est un sous-groupe de G si et seulement si $A\subset B$ ou $B\subset A$.*

1.2 Morphismes de groupes

Définition 1.5 Soient $(G_1,\cdot)$ et $(G_2,*)$ deux groupes et f une application de G_1 dans G_1. On dit que f est un morphisme (ou encore un homomorphisme) de $(G_1,\cdot)$ dans $(G_2,*)$ si on a

$$\forall (x,y)\in G_1\times G_1,\ \ f(x\cdot y)=f(x)*f(y).$$

- Un isomorphisme est morphisme bijectif.

- Un endomorphisme est morphisme d'un groupe dans lui-même.
- Un automorphisme est un endomorphisme bijectif.

Notation. *Soient $(G,\cdot)$ et $(G',*)$ deux groupes, on adopte les notations suivantes*

- *$Hom(G,G')$ est l'ensemble des morphismes de $(G,\cdot)$ dans $(G',*)$.*
- *On note $G \cong G'$ s'il existe un isomorphisme de $(G,\cdot)$ dans $(G',*)$.*
- *$End(G,G')$ est l'ensemble des endomorphismes de $(G,\cdot)$.*
- *$Aut(G,G')$ est l'ensemble des automorphismes de $(G,\cdot)$.*

Proposition 1.4 Soient $(G_1,\cdot)$ et $(G_2,*)$ deux groupes d'éléments neutres respectifs e_1 et e_2. Pour tout morphisme f de $(G_1,\cdot)$ dans $(G_2,*)$, on a

$$f(e_1)=e_2 \quad \text{et} \quad \forall x\in G_1,\ f(x^{-1})=(f(x))^{-1}.$$

Preuve *Comme $e_1=e_1e_1$, on déduit $f(e_1)=f(e_1e_1)=f(e_1)*f(e_1)$, d'où*

$$f(e_1)*e_2=f(e_1)=f(e_1)*f(e_1).$$

Simplifions avec $f(e_1)$, il vient $e_2=f(e_1)$. D'autre part, de $xx^{-1}=e_1$ et $x^{-1}x=e_1$, on déduit

$$f(x)*f(x^{-1})=f(e_1)=e_2 \quad et \quad f(x^{-1})*f(x)=f(e_1)=e_2.$$

Par suite, on obtient $f(x^{-1})=(f(x))^{-1}$. ■

Proposition 1.5 Soient $(G_1,\cdot)$ et $(G_2,*)$ deux groupes et f un morphisme de $(G_1,\cdot)$ dans $(G_2,*)$. Si H_1 est un sous-groupe de $(G_1,\cdot)$, alors $f(H_1)$ est un sous-groupe de $(G_2,*)$.

Preuve *Comme H_1 est non vide, il en est de même pour $f(H_1)$. De plus, soient y_1 et y_2 dans $f(H_1)$ et x_1 et x_2 dans H_1 tels que $y_1=f(x_1)$ et $y_2=f(x_2)$, alors il vient*

$$y_1*y_2^{-1}=f(x_1)*(f(x_2))^{-1}=f(x_1)*f(x_2^{-1})=f(x_1x_2^{-1}).$$

Comme H_1 est un sous-groupe, on a $x_1x_2^{-1}\in H_1$ et donc on a $y_1*y_2^{-1}=f(x_1x_2^{-1})\in f(H_1)$. Par conséquent, on obtient que $f(H_1)$ est un sous-groupe de $(G_2,*)$.

■

Proposition 1.6 Si H_2 est un sous-groupe de $(G_2,*)$, alors son image réciproque $f^{-1}(H_2)$ est un sous-groupe de $(G_1,\cdot)$.

Preuve *On a $f(e_1)=e_2$ et $e_2\in H_2$ donnent $e_1\in f^{-1}(H_2)$, d'où $f^{-1}(H_2)$ est non vide. De plus, soient x_1 et x_2 dans $f^{-1}(H_2)$, alors $f(x_1)$ et $f(x_2)$ sont dans H_2 et donc il vient*

$$f(x_1x_2^{-1})=f(x_1)*(f(x_2))^{-1}\in H_2.$$

Par suite, on obtient $x_1x_2^{-1}\in f^{-1}(H_2)$ et donc $f^{-1}(H_2)$ est un sous-groupe de $(G_1,\cdot)$. ■

Définition 1.6 — Noyau et image d'un morphisme. Soit f un morphisme de $(G_1,\cdot)$ dans $(G_2,*)$, alors $f(G)$ est appelé l'image du morphisme f, notée $Im\,f$, et $f^{-1}(\{e_2\})$ est appelé le noyau du morphisme f, notée $Ker\,f$.

Théorème 1.3 Le morphisme de groupes f est injectif si et seulement si $Ker f = \{e_1\}$.

Preuve *Supposons f est injectif et considérons $x \in Ker f$. On a $f(x) = e_2$ et comme $f(e_1) = e_2$, il vient $f(x) = f(e_1)$ puis $x = e_1$. Ainsi, $\{e_1\} \subset Ker f \subset \{e_1\}$, soit $Ker f = \{e_1\}$. Inversement, supposons $Ker f = \{e_1\}$, et considérons x_1, x_2 dans G_1 tels que $f(x_1) = f(x_2)$. Il vient alors que $f(x_1) * (f(x_2))^{-1} = e_2$, c'est-à-dire $f(x_1x_2^{-1}) = e_2$ et donc $x_1x_2^{-1} \in Ker f$. Il s'ensuit $x_1x_2^{-1} = e_1$ et en multipliant à droite par x_2, on obtient $x_1 = x_2$. Ainsi, le morphisme f est injectif.* ■

Proposition 1.7 — Composition de morphismes. Soient $(G_1,\cdot)$, $(G_2,\cdot)$ et $(G_3,\cdot)$ des groupes. Si $f_1 \in Hom(G_1,G_2)$ et $f_2 \in Hom(G_2,G_3)$, alors $f_2 \circ f_1 \in Hom(G_1,G_3)$.

Remarque L'ensemble $End(G)$ des endomorphisme de $(G,\cdot)$ est stable par composition.

Proposition 1.8 — Ensemble des permutations. Si $S(E)$ est l'ensemble des permutations d'un ensemble E, c'est-à-dire l'ensemble des bijections de E dans E, alors $(S(E),\circ)$ est un groupe.

Preuve *L'ensemble $S(E)$ n'est pas vide car il contient Id_E. La composée de bijections est une bijection, la composition des applications est associative et Id_E est un élément neutre. Enfin, une bijection de E dans E admet une réciproque, qui est elle-même une permutation de E.* ■

Théorème 1.4 Soient $(G,\cdot)$ un groupe et $f \in Aut(G)$, alors f^{-1} est un automorphisme de G.

Preuve *f est bijective par hypothèse et soit f^{-1} sa permutation réciproque. Soit x, y des éléments de G et x' et y' leurs uniques antécédents par f, on a*

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

Ainsi, f^{-1} est un endomorphisme de $(G,\cdot)$. ■

Corollaire 1.2 Soit $(G,\cdot)$ un groupe, alors $(Aut(G),\circ)$ est groupe.

Preuve *C'est un sous-groupe du groupe des bijections de G.* ■

Exercice 1.8 *Soit $(G,\times)$ un groupe et S un sous-groupe de G. Montrer que, pour tout élément a de G, l'ensemble $a^{-1}Sa = \{a^{-1}sa \quad s \in S\}$ est un sous-groupe de G.*

Exercice 1.9 — Commutateurs d'un groupe $(G,\cdot)$. *Étant donné $(a,b) \in G^2$, l'élément $aba^{-1}b^{-1}$ est appelé le commutateur de a et b. On note C l'ensemble des commutateurs du groupe $(G,\cdot)$ et $Gr(C)$ le sous-groupe qu'il engendre. Soit $(G',\cdot)$ un groupe et $f \in Hom(G,G')$. Montrer que le sous-groupe $f(G)$ de $(G',\cdot)$ est commutatif si et seulement si $Gr(C) \subset Ker f$.*

Exercice 1.10 — Automorphismes intérieurs d'un groupe $(G,\cdot)$. *Étant donné $a \in G$, on considère l'application $\varphi_a : G \to G$, $x \mapsto axa^{-1}$.*

1. *Montrer que $\varphi_a \in Aut(G)$ (c'est l'automorphisme intérieur associé à a).*
2. *Montrer que l'ensemble $\mathscr{I}(G)$ des automorphismes intérieurs de $(G,\cdot)$, est un sous-groupe de $(Aut(G),\circ)$.*

3. *Montrer que $\varphi : G \to Aut(G)$, $a \mapsto \varphi_a$ est un morphisme de groupes et déterminer* $Ker\,\varphi$.

1.3 Groupe produit

Proposition 1.9 Soient $(G_1,\cdot)$ et $(G_2,\cdot)$ deux groupes d'éléments neutres respectifs e_1 et e_2, alors l'ensemble $G_1 \times G_2$ muni de la loi produit définie par

$$(x_1,x_2)\cdot(y_1,y_2) = \big(x_1\cdot y_1, x_2\cdot y_2\big).$$

est un groupe, dit groupe produit de G_1 et G_2 et noté $G_1 \times G_2$. L'élément neutre du groupe produit $G_1 \times G_2$ est (e_1,e_2) et l'inverse de tout élément $(x_1,x_2) \in G_1 \times G_2$ est $(x_1^{-1},x_2^{-1}) \in G_1 \times G_2$.

Remarque 1. Par définition de la loi produit, les projections $p_1 : G_1 \times G_2 \to G_1$, $(x_1,x_2) \mapsto x_1$ et $p_2 : G_1 \times G_2 \to G_2$, $(x_1,x_2) \mapsto x_2$ sont des morphismes de groupes surjectifs. Et les injections $q_1 : G_1 \to G_1 \times G_2$, $x_1 \mapsto (x_1,e_2)$ et $q_2 : G_2 \to G_1 \times G_2$, $x_2 \mapsto (e_1,x_2)$ sont des morphismes de groupes injectifs.

2. Le groupe produit $G_1 \times G_2$ est commutatif si et seulement si G_1 et G_2 le sont aussi.

Proposition 1.10 Soient I une famille non vide et $(G_i,\cdot)_{i\in I}$ une famille de groupes d'éléments neutres respectifs $(e_i)_{i\in I}$. L'ensemble $\prod\limits_{i\in I} G_i$ muni de la loi de composition interne

$$(x_i)_{i\in I}\cdot(y_i)_{i\in I} = (x_i\cdot y_i)_{i\in I},$$

est un groupe, noté $\prod\limits_{i\in I} G_i$ et appelé le groupe produit des groupes $(G_i)_{i\in I}$, dont l'élément neutre est $(e_i)_{i\in I}$ et dans lequel l'élément inverse de $(x_i)_{i\in I}$ est l'élément $(x_i^{-1})_{i\in I}$.

Exercice 1.11 *Établir la preuve de la proposition 1.9*

Exercice 1.12 *Soient $(G_1,\cdot)$ et $(G_2,\cdot)$ deux groupes, et H_1 et H_2 des sous-groupes de G_1 et G_2, respectivement. Montrer que $H_1 \times H_2$ est un sous-groupe du groupe produit $(G_1 \times G_2,\cdot)$.*

1.4 Groupe symétrique S_n

Soit $n \in \mathbb{N}^*$, rappelons dans cette section qu'on note $\mathbb{N}_n = [\![1,n]\!] = \{1,2,\cdots,n\}$

1.4.1 Permutations d'un ensemble fini

Définition 1.7 Soit $n \in \mathbb{N}^*$, l'ensemble $S(\mathbb{N}_n)$ muni de l'opération $\circ$ est appelé le groupe symétrique d'ordre n, et noté S_n. Un élément σ de S_n se note :

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

Théorème 1.5 Si E est fini de cardinal $n \in \mathbb{N}^*$, alors $(S(E),\circ)$ est un groupe de cardinal $n!$.

Exemple Dans l'ensemble S_4, soient $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$. Alors, on a

$$\sigma' \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \quad \text{et} \quad \sigma \circ \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \text{et} \quad \sigma'^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Définition 1.8 On appelle support d'une permutation $\sigma \in S_n$, l'ensemble des éléments de $\mathbb{N}_n$ qui ne sont pas invariants par σ. On le note $Supp(\sigma)$.

Exemple Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in S_4$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \in S_4$, on a

$$Supp(\sigma) = \{1,2,3,4\} \quad \text{et} \quad Supp(\sigma') = \{1,3,4\}.$$

1.4.2 Permutations remarquables

Définition 1.9 — Transpositions. Une transposition est une permutation qui échange deux éléments de $\mathbb{N}_n = [\![1,n]\!]$ et laisse les autres invariants. La transposition qui échange i et j se note (i,j) ou τ_{ij}.

Remarque On a $C_n^2 = \dfrac{n(n-1)}{2}$ paires $\{i,j\}$ dans $\mathbb{N}_n$ et donc $\dfrac{n(n-1)}{2}$ transpositions dans S_n.

Définition 1.10 — Permutations circulaires. Soit E un ensemble fini de cardinal $n \in \mathbb{N}^*$. On dit que $\sigma \in S(E)$ est une permutation circulaire lorsque il existe $a \in E$ tel que

$$\{a, \sigma(a), \sigma^2(a), \cdots, \sigma^{n-1}(a)\} = E.$$

Proposition 1.11 Si σ est une permutation circulaire de l'ensemble fini E ($card(E) = n$), alors

$$\forall x \in E, \quad \{x, \sigma(x), \sigma^2(x), \cdots, \sigma^{n-1}(x)\} = E.$$

Preuve *On considère une permutation circulaire de $\sigma \in S(E)$ et soit $a \in E$ tels que*

$$\{a, \sigma(a), \sigma^2(a), \cdots, \sigma^{n-1}(a)\} = E,$$

alors $\sigma^n(a) = a$. En effet, on a $\sigma(E) = E$ car σ est une bijection de E. Avec

$$\sigma(E) = \{\sigma(a), \sigma^2(a), \cdots, \sigma^n(a)\},$$

il vient que $\sigma^n(a) = a$. En conséquence, pour tout $k \in \mathbb{N}$, on a $\sigma^{n+k}(a) = \sigma^k(a)$. Par ailleurs, pour tout $x \in E$, il existe $p \in [\![0, n-1]\!]$ tel que $x = \sigma^p(a)$. Pour tout $k \in [\![0, n-1]\!]$, on a donc $\sigma^k(x) = \sigma^{p+k}(a)$. Il s'ensuit donc que

$$\{x, \sigma(x), \sigma^2(x), \cdots, \sigma^{n-1}(x)\} = \{\sigma^p(a), \sigma^{p+1}(a), \cdots, \sigma^{p+n-1}(a)\}$$

et puisque, pour tout $k \in \mathbb{N}$, on a $\sigma^{n+k}(a) = \sigma^k(a)$, il vient donc

$$\begin{aligned} \{\sigma^p(a), \sigma^{p+1}(a), \cdots, \sigma^{n+p-1}(a)\} &= \{\sigma^p(a), \cdots, \sigma^{n-1}(a), a, \sigma(a), \cdots, \sigma^{p-1}(a)\} \\ &= \{a, \sigma(a), \cdots, \sigma^{p-1}(a), \sigma^p(a), \cdots, \sigma^{n-1}(a)\} \\ &= E, \end{aligned}$$

c'est-à-dire

$$\{x, \sigma(x), \sigma^2(x), \cdots, \sigma^{n-1}(x)\} = E.$$

■

Notation. *Une telle permutation circulaire est notée* $(x, \sigma(x), \sigma^2(x), \cdots, \sigma^{n-1}(x))$.

Lemme 1.1 Soit σ une permutation de $[\![1,n]\!]$. Si $I \subset [\![1,n]\!]$ est inclus dans l'ensemble des éléments invariants par σ, alors σ induit une permutation de $J = [\![1,n]\!] \setminus I$, notée σ_J.

Remarque En particulier, toute permutation de $[\![1,n]\!]$ induit une permutation de son support.

Définition 1.11 — Cycle. On dit que $\sigma \in S_n$ de support J, est un cycle si σ_J est une permutation circulaire de J. Si σ est un cycle de support J, alors $Card(J)$ est appelé longueur de cycle.

Remarque On convient que Id_{S_n} est cycle de longueur 0.

Exemple Montrons que deux cycles de support disjoints commutent. En effet, soient σ et σ' deux cycles de supports S et S' tels que $S \cap S' = \emptyset$. On distingue les trois cas suivants

– si $x \notin S \cup S'$, alors x est invariant par σ et σ', et donc invariant par $\sigma \circ \sigma'$ et $\sigma' \circ \sigma$,

– si $x \in S$ et $x \notin S'$, alors x est invariant par σ', d'où $\sigma \circ \sigma'(x) = \sigma(x)$. De plus, par définition d'un cycle, pour $x \in S$, on a $\sigma(x) \in S$ et donc $\sigma(x) \notin S'$ d'où $\sigma' \circ \sigma(x) = \sigma(x)$, c'est-à-dire

$$\sigma' \circ \sigma(x) = \sigma \circ \sigma'(x),$$

– de la même manière, on vérifie que si $x \in S'$ et $x \notin S$, alors on a $\sigma' \circ \sigma(x) = \sigma \circ \sigma'(x)$.

En conclusion, on a $\sigma' \circ \sigma(x) = \sigma \circ \sigma'(x)$, pour tout $x \in \mathbb{N}_n$ et donc $\sigma' \circ \sigma = \sigma \circ \sigma'$.

Théorème 1.6 Le groupe S_n est engendré par les $\dfrac{n(n-1)}{2}$ transpositions τ_{ij}.

Preuve *On procède par récurrence sur* $n \in \mathbb{N}^*$. *D'abord, l'identité sur* $\mathbb{N}_n$ *est la composé* $\tau \circ \tau$ *où* τ *est une transposition quelconque. La propriété est vraie si* $n = 2$ *(les permutations de* $\mathbb{N}_2$ *sont* $Id_{\mathbb{N}_2}$ *et* τ_{12}*). Supposons-la vraie pour* $n-1$ *avec* $n \geq 3$, *et considérons* $\sigma \in S_n$.

– *Si* $\sigma(n) = n$, *la restriction* σ' *de* σ *à* $\mathbb{N}_{n-1}$ *est une permutation de* $\mathbb{N}_{n-1}$. *Elle se décompose en produit de transpositions :*

$$\sigma' = \tau'_1 \circ \tau'_2 \circ \cdots \circ \tau'_s.$$

À toute transposition τ' *de* $\mathbb{N}_{n-1}$, *associons la transposition* τ *de* $\mathbb{N}_n$ *telle que* $\tau(n) = n$ *et* $\tau(k) = \tau'(k)$ *pour tout* $k \in \mathbb{N}_{n-1}$. *Il s'ensuit alors que*

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_s.$$

– *Si* $\sigma(n) \neq n$, *en introduisons la transposition* $\tau = (\sigma(n), n)$, *il vient que* $\tau \circ \sigma$ *laisse* n *invariant et on est ramené au cas précédent. En conséquence,* $\tau \circ \sigma$ *est produit de transpositions*

$$\tau \circ \sigma' = \tau_1 \circ \tau'_2 \circ \cdots \circ \tau'_r,$$

et avec $\tau^{-1} = \tau$, *on obtient*

$$\sigma = \tau \circ \tau_1 \circ \tau'_2 \circ \cdots \circ \tau'_r.$$

■

Théorème 1.7 Toute permutation autre que l'identité peut se décomposer d'une manière unique (à l'ordre près des termes) en produit de cycles de supports deux à deux disjoints

Exemple Décomposer en produit de cycles disjoints la permutation de $\mathbb{N}_{10}$ suivantes

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

On a $\sigma(1) = 3$, $\sigma(3) = 6$ et $\sigma(6) = 1$, soit σ_1 le cycle $(1,3,6)$. En prenant $2 \notin \{1,3,6\}$, on a

$$\sigma(2) = 10\,,\ \sigma(10) = 9\,,\ \sigma(9) = 8\,,\ \sigma(8) = 5 \ \text{ et } \ \sigma(5) = 2.$$

Soit le cycle $\sigma_2 = (2,10,9,8,5)$. Les autres éléments 4 et 7 sont invariants par σ. On vérifie que

$$\sigma = \sigma_1 \circ \sigma_2.$$

En effet, 4 et 7 sont invariant par σ_1 et σ_2 et donc par leur composé $\sigma = \sigma_1 \circ \sigma_2$. Pour les autres éléments, étudions par exemple les images de 3 et 9, on a

$$\sigma_2(3) = 3\,,\ \sigma_1(3) = 6 \implies \sigma_1 \circ \sigma_2(3) = 6 = \sigma(3)$$

$$\sigma_2(9) = 8\,,\ \sigma_1(8) = 8 \implies \sigma_1 \circ \sigma_2(9) = 8 = \sigma(9).$$

Proposition 1.12 Un cycle $\sigma = (a_1, a_2, \cdots, a_{p-1}, a_p)$ se décompose en produit de $p-1$ transpositions avec

$$\sigma = (a_1, a_p) \circ (a_1, a_{p-1}) \circ \cdots \circ (a_1, a_2)$$

ou

$$\sigma = (a_1, a_2) \circ (a_2, a_3) \circ \cdots \circ (a_{p-1}, a_p).$$

Remarque La décomposition d'une permutation en produit de transpositions n'est pas unique.

Exemple Reprenons l'exemple précédent, nous avons

$$\sigma_1 = (1,3,6) = (1,6) \circ (1,3) \quad \text{et} \quad \sigma_2 = (2,10,9,8,5) = (2,5) \circ (2,8) \circ (2,9) \circ (2,10),$$

et donc

$$\sigma = \sigma_1 \circ \sigma_2 = (1,6) \circ (1,3) \circ (2,5) \circ (2,8) \circ (2,9) \circ (2,10).$$

D'autre part, nous avons aussi

$$\sigma_1 = (3,6,1) = (3,1) \circ (3,6) \quad \text{et} \quad \sigma_2 = (8,5,2,10,9) = (8,9) \circ (8,10) \circ (8,2) \circ (8,5),$$

et donc

$$\sigma = \sigma_1 \circ \sigma_2 = (3,1) \circ (3,6) \circ (8,9) \circ (8,10) \circ (8,2) \circ (8,5).$$

Définition 1.12 — Inversion d'une permutation. Une paire $\{i,j\}$ est une inversion pour $\sigma \in S_n$ lorsque $(i-j)(\sigma(i) - \sigma(j)) < 0$. On note $Inv(\sigma)$ le nombre d'inversions pour σ.

Définition 1.13 — Signature d'une permutation. La signature d'une permutation σ est le nombre $\varepsilon(\sigma) = (-1)^{Inv(\sigma)}$. Et selon que la signature $\varepsilon(\sigma) = 1$ ou $\varepsilon(\sigma) = -1$, on dit que la permutation σ est paire ou impaire.

Exemple — Méthode pratique de recherche de $Inv(\sigma)$**.** Soit

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

Pour chacun des nombres de la $2^{\text{ème}}$ ligne, on compte combien il y en a de plus petits qui sont écrit après lui. La somme de ces nombres est le nombre d'inversions de la permutation considérée. Sur la permutation σ, on a

terme étudié	3	10	6	4	2	1	7	5	8	9
nombre associé	2	8	4	2	1	0	1	0	0	0

La somme des nombres associés est $Inv(\sigma) = 18$ et $\varepsilon(\sigma) = (-1)^{18} = 1$, et donc σ est paire.

Théorème 1.8 Pour tout transposition τ, sa signature est $\varepsilon(\tau) = -1$.

Preuve *Soient $(i, j) \in [\![1,n]\!]^2$ tels que $i < j$, on considère la transposition*

$$\tau = \begin{pmatrix} 1 & \cdots & i & \cdots & k & \cdots & j & \cdots & n \\ 1 & \cdots & j & \cdots & k & \cdots & i & \cdots & n \end{pmatrix}$$

En deuxième ligne

- *il y a $j - i$ termes plus petits que j, écris après j.*
- *tout entier k tel que $i < k < j$, a i comme seul terme plus petit que lui et écris après lui.*

Alors, le nombre d'inversion pour τ est

$$Inv(\tau) = (j - i) + ((j - 1) - i) = 2(j - i) - 1.$$

Cet entier est impair et donc la transposition τ est impaire. ■

Proposition 1.13 Pour tout permutation σ, on a

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j} = \prod_{i>j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Théorème 1.9 L'application $\varepsilon : \sigma \mapsto \varepsilon(\sigma)$ est un morphisme de $(S_n, \circ)$ dans $(\{-1, 1\}, \times)$:

$$\forall \sigma_1, \sigma_2 \in S_n, \;\; \varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1) \times \varepsilon(\sigma_2)$$

Preuve *Nous avons*

$$\varepsilon(\sigma_1 \circ \sigma_2) = \frac{\prod_{i<j} \big(\sigma_1 \circ \sigma_2(i) - \sigma_1 \circ \sigma_2(j)\big)}{\prod_{i<j} \big(\sigma_2(i) - \sigma_2(j)\big)} \times \frac{\prod_{i<j} \big(\sigma_2(i) - \sigma_2(j)\big)}{\prod_{i<j} (i - j)}.$$

Comme σ_2 est une permutation de $\mathbb{N}_n$, alors on a

$$\frac{\prod_{i<j} \big(\sigma_1 \circ \sigma_2(i) - \sigma_1 \circ \sigma_2(j)\big)}{\prod_{i<j} \big(\sigma_2(i) - \sigma_2(j)\big)} = \varepsilon(\sigma_1).$$

Finalement, il vient que $\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1) \times \varepsilon(\sigma_2)$. ■

Théorème 1.10 Si une permutation σ est la composée de s transpositions, alors sa signature est

$$\varepsilon(\sigma) = (-1)^s.$$

Corollaire 1.3 Si σ est un cycle de longueur p, alors sa signature est

$$\varepsilon(\sigma) = (-1)^{p-1}.$$

On utilise pour prouver ce corollaire la décomposition

$$(a_1, a_2, \cdots, a_{p-1}, a_p) = (a_1, a_p) \circ (a_1, a_{p-1}) \circ \cdots \circ (a_1, a_2).$$

Définition 1.14 — Groupe alterné. Le groupe alterné $\mathscr{A}_n$ est le sous-ensemble de S_n formé des permutations paires de $\mathbb{N}_n$.

Proposition 1.14 Le groupe $\mathscr{A}_n$ est un sous-groupe de S_n de cardinal $\dfrac{n!}{2}$.

Preuve *C'est en effet le noyau du morphisme ε de $(S_n, \circ)$ dans $(\{-1, 1\}, \times)$.* ■

Exercice 1.13 *1- Déterminer la signature de la permutation suivante*

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

2- Déterminer $\sigma \circ \sigma'$ et $\sigma' \circ \sigma$ pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$ *et* $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$.

Exercice 1.14 *Décomposer en produit de cycles disjoints la permutation de S_7 suivante*

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

Calculer de plusieurs manière sa signature.

Exercice 1.15 *Soient τ_1 et τ_2 deux transpositions de $[\![1, n]\!]$. Montrer que*

$$\text{soit } \tau_1 \circ \tau_2 = Id, \quad \text{soit } (\tau_1 \circ \tau_2)^2 = Id, \quad \text{soit } (\tau_1 \circ \tau_2)^3 = Id.$$

Exercice 1.16 *On considère la permutation suivante*

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

1- Vérifier que

$$\sigma = (1,9,5,7)\circ(2,4,8)\circ(6,10).$$

2- En déduire un calcul de $\varepsilon(\sigma)$ et une décomposition de σ en produit de transpositions.

3- Procéder de la manière pour la permutation suivante

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

Exercice 1.17 *Utiliser la méthode du théorème d'existence de décomposition d'une permutation en produit de transpositions pour décomposer :*

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

Comparer avec l'exercice précédent.