Cours Algèbre 2 – II: Théorie des groupes

Andrei Teleman

Département de Mathématiques, Aix-Marseille Université

19 mars 2021

Table of Contents

Table of Contents

Définition 1.1

Soit M un ensemble. Une loi de composition interne (lci) sur M est une application $l : M \times M \to M$.

Définition 1.1

Soit M un ensemble. Une loi de composition interne (lci) sur M est une application $l : M \times M \to M$. Notations possibles :

$x \circ y := l(x, y)$, $x * y := l(x, y)$, $x \cdot y := l(x, y)$, $x + y := l(x, y)$ ...

Définition 1.1

Soit M un ensemble. Une loi de composition interne (lci) sur M est une application $l : M \times M \to M$. Notations possibles :

$$x \circ y := l(x,y)\,,\ x * y := l(x,y)\,,\ x \cdot y := l(x,y)\,,\ x + y := l(x,y)\ \ldots$$

Sur un ensemble fini on peut définir une lci à l'aide d'un tableau. Sur un ensemble à trois éléments $M = \{a, b, c\}$ une lci $\circ$ sera définie par un tableau de la forme

$\circ$	a	b	c
a	$a \circ a$	$a \circ b$	$a \circ c$
b	$b \circ a$	$b \circ b$	$b \circ c$
c	$c \circ a$	$c \circ b$	$c \circ c$

.

Exemple 1.1

Par exemple la lci définie par le tableau

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	b	c

(1)

est l'application $l : \{a, b, c\} \times \{a, b, c\} \to \{a, b, c\}$ donnée par

Exemple 1.1

Par exemple la lci définie par le tableau

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	b	c

(1)

est l'application $l : \{a, b, c\} \times \{a, b, c\} \to \{a, b, c\}$ donnée par

$$l(a, a) = a,\ l(a, b) = b,\ l(a, c) = c,\ l(b, a) = b,\ l(b, b) = c,$$

$$l(b, c) = a,\ l(c, a) = c,\ l(c, b) = b,\ l(c, c) = c.$$

Définition 1.2

Une loi de composition interne $\circ : M \times M \to M$ *est dite*

1. *commutative, si* $x \circ y = y \circ x$ *pour tous* $x, y \in M$,

Définition 1.2

Une loi de composition interne $\circ : M \times M \to M$ *est dite*

1. *commutative, si* $x \circ y = y \circ x$ *pour tous* $x, y \in M$,
2. *associative, si* $x \circ (y \circ z) = (x \circ y) \circ z$ *pour tous* $x, y, z \in M$.

Définition 1.2

Une loi de composition interne $\circ : M \times M \to M$ *est dite*

1. *commutative, si* $x \circ y = y \circ x$ *pour tous* $x, y \in M$,
2. *associative, si* $x \circ (y \circ z) = (x \circ y) \circ z$ *pour tous* $x, y, z \in M$.

Définition 1.3

Soit $(M, \circ)$ *un ensemble muni d'une loi de composition interne. Un élément* $e \in M$ *s'appelle élément neutre (pour la lci* $\circ$*) si* $e \circ x = x \circ e = x$ *pour tout* $x \in M$.

Définition 1.2

Une loi de composition interne $\circ : M \times M \to M$ *est dite*

1. *commutative, si* $x \circ y = y \circ x$ *pour tous* $x, y \in M$,
2. *associative, si* $x \circ (y \circ z) = (x \circ y) \circ z$ *pour tous* $x, y, z \in M$.

Définition 1.3

Soit $(M, \circ)$ *un ensemble muni d'une loi de composition interne. Un élément* $e \in M$ *s'appelle élément neutre (pour la lci* $\circ$*) si* $e \circ x = x \circ e = x$ *pour tout* $x \in M$.

Exercice 1.1

Est-ce que la lci $\{a, b, c\}$ définie par le tableau (1) est commutative ? Est-ce qu'elle est associative ? Est-ce qu'elle admet un élément neutre ? Si oui, lequel ?

Remarque 1.4

Si un élément neutre existe, il est unique.

Remarque 1.4

Si un élément neutre existe, il est unique.

Dém: En effet, soient e, e_1 deux éléments neutres pour la loi de composition interne $\circ$. Alors

$$e \circ e_1 = e_1 \ , \ e \circ e_1 = e \, ,$$

où d'abord on a utilisé le fait que e est élément neutre, puis le fait que e_1 est élément neutre. Donc $e = e_1$. ■

Remarque 1.4

Si un élément neutre existe, il est unique.

Dém: En effet, soient e, e_1 deux éléments neutres pour la loi de composition interne $\circ$. Alors

$$e \circ e_1 = e_1 \ , \ e \circ e_1 = e \, ,$$

où d'abord on a utilisé le fait que e est élément neutre, puis le fait que e_1 est élément neutre. Donc $e = e_1$. ■

Définition 1.5

Soit $(M, \circ)$ un ensemble muni d'une loi de composition interne, soit $e \in M$ un élément neutre pour $\circ$ et soit $a \in M$.

Remarque 1.4

Si un élément neutre existe, il est unique.

Dém: En effet, soient e, e_1 deux éléments neutres pour la loi de composition interne $\circ$. Alors

$$e \circ e_1 = e_1 \ , \ e \circ e_1 = e \, ,$$

où d'abord on a utilisé le fait que e est élément neutre, puis le fait que e_1 est élément neutre. Donc $e = e_1$. ■

Définition 1.5

Soit $(M, \circ)$ un ensemble muni d'une loi de composition interne, soit $e \in M$ un élément neutre pour $\circ$ et soit $a \in M$. Un élément symétrique de a est un élément $a' \in M$ tel que

$$a' \circ a = a \circ a' = e$$

Remarque 1.6

Supposons que $\circ$ admet un element neutre e et est associative. Soit $a \in M$. Si a admet un élément symétrique, alors il est unique.

Remarque 1.6

Supposons que $\circ$ admet un element neutre e et est associative. Soit $a \in M$. Si a admet un élément symétrique, alors il est unique.

Dém: Soient a' et a'' éléments symétriques de $a \in M$. Alors

$$a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''.$$

Remarque 1.6

Supposons que $\circ$ admet un element neutre e et est associative. Soit $a \in M$. Si a admet un élément symétrique, alors il est unique.

Dém: Soient a' et a'' éléments symétriques de $a \in M$. Alors

$$a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''.$$

Définition 1.7

Un groupe est un couple $(G, \circ)$, où $\circ$ est une lci sur G telle que :

1. *$\circ$ est associative.*

Remarque 1.6

Supposons que $\circ$ admet un element neutre e et est associative. Soit $a \in M$. Si a admet un élément symétrique, alors il est unique.

Dém: Soient a' et a'' éléments symétriques de $a \in M$. Alors

$$a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''.$$

Définition 1.7

Un groupe est un couple $(G, \circ)$, où $\circ$ est une lci sur G telle que :

1. *$\circ$ est associative.*
2. *$\circ$ admet un élément neutre $e \in G$.*

Remarque 1.6

Supposons que $\circ$ admet un element neutre e et est associative. Soit $a \in M$. Si a admet un élément symétrique, alors il est unique.

Dém: Soient a' et a'' éléments symétriques de $a \in M$. Alors

$$a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''.$$

Définition 1.7

Un groupe est un couple $(G, \circ)$, où $\circ$ est une lci sur G telle que :

1. *$\circ$ est associative.*
2. *$\circ$ admet un élément neutre $e \in G$.*
3. *Tout $a \in G$ admet un symétrique $a' \in G$ par rapport à $\circ$.*

Remarque 1.6

Supposons que $\circ$ admet un element neutre e et est associative. Soit $a \in M$. Si a admet un élément symétrique, alors il est unique.

Dém: Soient a' et a'' éléments symétriques de $a \in M$. Alors

$$a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''.$$

Définition 1.7

Un groupe est un couple $(G, \circ)$, où $\circ$ est une lci sur G telle que :

1. *$\circ$ est associative.*
2. *$\circ$ admet un élément neutre $e \in G$.*
3. *Tout $a \in G$ admet un symétrique $a' \in G$ par rapport à $\circ$.*

Si G est fini, $\mathrm{card}(G)$ s'appelle l'ordre du groupe, noté $|G|$.

Définition 1.8

Un groupe $(G, \circ)$ est dit commutatif (ou abélien) si $\circ$ est commutative, donc si $x \circ y = y \circ x$ pour tous les x, $y \in G$.

Définition 1.8

Un groupe $(G, \circ)$ est dit commutatif (ou abélien) si $\circ$ est commutative, donc si $x \circ y = y \circ x$ pour tous les x, $y \in G$.

Exemple 1.2

Un singleton $\{e\}$ admet une seule lci $\circ$ et $(\{e\}, \circ)$ est évidemment un groupe abélien. Un tel groupe s'appelle groupe trivial.

Définition 1.8

Un groupe $(G, \circ)$ est dit commutatif (ou abélien) si $\circ$ est commutative, donc si $x \circ y = y \circ x$ pour tous les x, $y \in G$.

Exemple 1.2

Un singleton $\{e\}$ admet une seule lci $\circ$ et $(\{e\}, \circ)$ est évidemment un groupe abélien. Un tel groupe s'appelle groupe trivial.

Exemple 1.3

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^n, +)$ sont des groupes abéliens.

Définition 1.8

Un groupe $(G, \circ)$ est dit commutatif (ou abélien) si $\circ$ est commutative, donc si $x \circ y = y \circ x$ pour tous les x, $y \in G$.

Exemple 1.2

Un singleton $\{e\}$ admet une seule lci $\circ$ et $(\{e\}, \circ)$ est évidemment un groupe abélien. Un tel groupe s'appelle groupe trivial.

Exemple 1.3

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^n, +)$ sont des groupes abéliens.

Exemple 1.4

$(\{\pm 1\}, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ sont des groupes abéliens.

Exemple 1.5

Soit $n \in \mathbb{N}^*$. Le couple $(\mathbb{Z}_n, +)$ est un groupe abélien. Son élément neutre est la classe $[0]_n = n\mathbb{Z}$ et l'élément symétrique d'une classe $[k]_n \in \mathbb{Z}_n$ par rapport à l'addition est la classe $[-k]_n$.

Exemple 1.5

Soit $n \in \mathbb{N}^*$. Le couple $(\mathbb{Z}_n, +)$ est un groupe abélien. Son élément neutre est la classe $[0]_n = n\mathbb{Z}$ et l'élément symétrique d'une classe $[k]_n \in \mathbb{Z}_n$ par rapport à l'addition est la classe $[-k]_n$.

Exemple 1.6

Soit $n \geqslant 2$. $(\mathbb{Z}_n, \cdot)$ admet un élément neutre, à savoir la classe $[1]_n$, mais *n'est pas un groupe*, parce que la classe $[0]_n \in \mathbb{Z}_n$ n'est pas inversible par rapport à la multiplication.

Exemple 1.5

Soit $n \in \mathbb{N}^*$. Le couple $(\mathbb{Z}_n, +)$ est un groupe abélien. Son élément neutre est la classe $[0]_n = n\mathbb{Z}$ et l'élément symétrique d'une classe $[k]_n \in \mathbb{Z}_n$ par rapport à l'addition est la classe $[-k]_n$.

Exemple 1.6

Soit $n \geqslant 2$. $(\mathbb{Z}_n, \cdot)$ admet un élément neutre, à savoir la classe $[1]_n$, mais *n'est pas un groupe*, parce que la classe $[0]_n \in \mathbb{Z}_n$ n'est pas inversible par rapport à la multiplication.

La multiplication définit une lci sur le sous-ensemble $\mathbb{Z}_n^\times \subset \mathbb{Z}_n$ et $(\mathbb{Z}_n^\times, \cdot)$ *est un groupe*. Le symétrique de $\xi \in \mathbb{Z}_n^\times$ est la classe $\eta \in \mathbb{Z}_n^\times$ qui satisfait $\xi\eta = [1]_n$. Une telle classe existe par la définition de $\mathbb{Z}_n^\times$.

Exemple 1.7

$(\mathrm{GL}(n,\mathbb{R}),\cdot)$ où $\mathrm{GL}(n,\mathbb{R}) := \{A \in M_{n,n}(\mathbb{R}) |\ \det(A) \neq 0\}$ est l'ensemble des matrices carrées de taille n inversibles, ensemble muni de la multiplication matricielle est un groupe, qui pour $n \geqslant 2$ est *non-abélien*. L'élément neutre de $\mathrm{GL}(n,\mathbb{R})$ est la matrice unité d'ordre n notée I_n.

Exemple 1.7

$(\mathrm{GL}(n,\mathbb{R}),\cdot)$ où $\mathrm{GL}(n,\mathbb{R}) := \{A \in M_{n,n}(\mathbb{R}) |\ \det(A) \neq 0\}$ est l'ensemble des matrices carrées de taille n inversibles, ensemble muni de la multiplication matricielle est un groupe, qui pour $n \geqslant 2$ est *non-abélien*. L'élément neutre de $\mathrm{GL}(n,\mathbb{R})$ est la matrice unité d'ordre n notée I_n.

Exemple 1.8 (Le groupe des permutations d'un ensemble)

Soit M un ensemble. On désigne par $\mathfrak{S}(M)$ l'ensemble des applications bijectives $f : M \to M$.

Exemple 1.7

$(\mathrm{GL}(n,\mathbb{R}),\cdot)$ où $\mathrm{GL}(n,\mathbb{R}) := \{A \in M_{n,n}(\mathbb{R}) |\ \det(A) \neq 0\}$ est l'ensemble des matrices carrées de taille n inversibles, ensemble muni de la multiplication matricielle est un groupe, qui pour $n \geqslant 2$ est *non-abélien*. L'élément neutre de $\mathrm{GL}(n,\mathbb{R})$ est la matrice unité d'ordre n notée I_n.

Exemple 1.8 (Le groupe des permutations d'un ensemble)

Soit M un ensemble. On désigne par $\mathfrak{S}(M)$ l'ensemble des applications bijectives $f : M \to M$.

Si on munit $\mathfrak{S}(M)$ de la composition des bijections, on obtient un groupe $(\mathfrak{S}(M),\circ)$ qui s'appelle *le groupe symétrique* ou *le groupe des permutations de* M.

Exemple 1.7

$(\mathrm{GL}(n,\mathbb{R}),\cdot)$ où $\mathrm{GL}(n,\mathbb{R}) := \{A \in M_{n,n}(\mathbb{R}) |\ \det(A) \neq 0\}$ est l'ensemble des matrices carrées de taille n inversibles, ensemble muni de la multiplication matricielle est un groupe, qui pour $n \geqslant 2$ est *non-abélien*. L'élément neutre de $\mathrm{GL}(n,\mathbb{R})$ est la matrice unité d'ordre n notée I_n.

Exemple 1.8 (Le groupe des permutations d'un ensemble)

Soit M un ensemble. On désigne par $\mathfrak{S}(M)$ l'ensemble des applications bijectives $f : M \to M$.

Si on munit $\mathfrak{S}(M)$ de la composition des bijections, on obtient un groupe $(\mathfrak{S}(M),\circ)$ qui s'appelle *le groupe symétrique* ou *le groupe des permutations de M*. L'élément neutre de ce groupe est id_M et l'élément symétrique de $f \in \mathfrak{S}(M)$ est l'application réciproque f^{-1}.

Si M est fini de cardinal n, alors $|\mathfrak{S}(M)| = n!$.

Si M est fini de cardinal n, alors $|\mathfrak{S}(M)| = n!$.

On désigne par $\mathfrak{S}_n$ le groupe des permutations de $\{1, 2, \ldots, n\}$. $\mathfrak{S}_n$ s'appelle le groupe symétrique d'indice n et un élément de $\mathfrak{S}_n$ s'appelle permutation de degré n.

Si M est fini de cardinal n, alors $|\mathfrak{S}(M)| = n!$.

On désigne par $\mathfrak{S}_n$ le groupe des permutations de $\{1, 2, \ldots, n\}$. $\mathfrak{S}_n$ s'appelle le groupe symétrique d'indice n et un élément de $\mathfrak{S}_n$ s'appelle permutation de degré n. On a donc

$$|\mathfrak{S}_n| = n! \,.$$

Si M est fini de cardinal n, alors $|\mathfrak{S}(M)| = n!$.

On désigne par $\mathfrak{S}_n$ le groupe des permutations de $\{1, 2, \ldots, n\}$. $\mathfrak{S}_n$ s'appelle le groupe symétrique d'indice n et un élément de $\mathfrak{S}_n$ s'appelle permutation de degré n. On a donc

$$|\mathfrak{S}_n| = n! \,.$$

Une permutation $\sigma \in \mathfrak{S}_n$ s'écrit sous la forme

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

où $i_s \in \{1, \ldots, n\}$ est l'image de $s \in \{1, 2, \ldots, n\}$ par la bijection considérée.

Si M est fini de cardinal n, alors $|\mathfrak{S}(M)| = n!$.

On désigne par $\mathfrak{S}_n$ le groupe des permutations de $\{1, 2, \ldots, n\}$. $\mathfrak{S}_n$ s'appelle le groupe symétrique d'indice n et un élément de $\mathfrak{S}_n$ s'appelle permutation de degré n. On a donc

$$|\mathfrak{S}_n| = n! \,.$$

Une permutation $\sigma \in \mathfrak{S}_n$ s'écrit sous la forme

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

où $i_s \in \{1, \ldots, n\}$ est l'image de $s \in \{1, 2, \ldots, n\}$ par la bijection considérée. Puisqu'il s'agit d'une application injective on a $i_s \neq i_t$ pour $t \neq s$.

Notons que

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

Notons que

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Notons que

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

$\mathfrak{S}_2$ est abélien, $\mathfrak{S}_n$ est non-abélien pour $n \geqslant 3$. Pourquoi ?

Notons que

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

$\mathfrak{S}_2$ est abélien, $\mathfrak{S}_n$ est non-abélien pour $n \geqslant 3$. Pourquoi ?

Dans la liste des éléments de $\mathfrak{S}_3$ le 2me, 3me et 4me élément sont des transpositions (ou 2-cycles), i.e. des permutations qui échangent deux éléments, laissant inchangés les autres.

Notons que

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

$\mathfrak{S}_2$ est abélien, $\mathfrak{S}_n$ est non-abélien pour $n \geqslant 3$. Pourquoi ?

Dans la liste des éléments de $\mathfrak{S}_3$ le 2me, 3me et 4me élément sont des transpositions (ou 2-cycles), i.e. des permutations qui échangent deux éléments, laissant inchangés les autres. Le 5me et le 6me élément sont des 3-cycles.

Exemple 1.9

Soit $(G_1, \circ)$, $(G_2, *)$ deux groupes. Leur produit direct est le groupe $(G_1 \times G_2, \cdot)$ où la loi de composition interne $\cdot$ sur le produit cartésien $G_1 \times G_2$ est donnée par la formule

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 \circ h_1, g_2 * h_2) .$$

Exemple 1.9

Soit $(G_1, \circ)$, $(G_2, *)$ deux groupes. Leur produit direct est le groupe $(G_1 \times G_2, \cdot)$ où la loi de composition interne $\cdot$ sur le produit cartésien $G_1 \times G_2$ est donnée par la formule

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 \circ h_1, g_2 * h_2) .$$

Montrer que $(G_1 \times G_2, \cdot)$ ainsi défini est bien un groupe.

Exemple 1.9

Soit $(G_1, \circ)$, $(G_2, *)$ deux groupes. Leur produit direct est le groupe $(G_1 \times G_2, \cdot)$ où la loi de composition interne $\cdot$ sur le produit cartésien $G_1 \times G_2$ est donnée par la formule

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 \circ h_1, g_2 * h_2)\,.$$

Montrer que $(G_1 \times G_2, \cdot)$ ainsi défini est bien un groupe.
De la même manière on définit la produit direct $\times_{i=1}^{k} G_i$ de k groupes $G_1, \ldots, G_k$.

Exemple 1.9

Soit $(G_1, \circ)$, $(G_2, *)$ deux groupes. Leur produit direct est le groupe $(G_1 \times G_2, \cdot)$ où la loi de composition interne $\cdot$ sur le produit cartésien $G_1 \times G_2$ est donnée par la formule

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 \circ h_1, g_2 * h_2)\,.$$

Montrer que $(G_1 \times G_2, \cdot)$ ainsi défini est bien un groupe.
De la même manière on définit la produit direct $\times_{i=1}^{k} G_i$ de k groupes $G_1, \ldots, G_k$.

La théorie de groupes a été introduite en mathématiques par Évariste Galois, un mathématicien français génial, qui est mort en 1832 à 20 ans, suite à un duel.

Soit $(G, \circ)$ un groupe.

Définition 1.9

Pour un élément $x \in G$ et $n \in \mathbb{Z}$ on pose :

$$x^n := \begin{cases} \underbrace{x \circ x \circ \ldots \circ x}_{n \text{ fois}} & \text{si} \quad n > 0 \\ e & \text{si} \quad n = 0 \\ (x')^{|n|} & \text{si} \quad n < 0 \ . \end{cases}$$

Soit $(G, \circ)$ un groupe.

Définition 1.9

Pour un élément $x \in G$ et $n \in \mathbb{Z}$ on pose :

$$x^n := \begin{cases} \underbrace{x \circ x \circ \ldots \circ x}_{n \text{ fois}} & \text{si} \quad n > 0 \\ e & \text{si} \quad n = 0 \\ (x')^{|n|} & \text{si} \quad n < 0 \ . \end{cases}$$

En particulier on a $x^{-1} = x'$, donc on pourra utiliser la notation x^{-1} au lieu de x'.

Proposition 1.10 (Règles de calcul dans un groupe)

Soit $(G, \circ)$ un groupe.

1. *Pour tous x, $y \in G$ on a $(x \circ y)' = y' \circ x'$.*

Proposition 1.10 (Règles de calcul dans un groupe)

Soit $(G, \circ)$ un groupe.

1. *Pour tous x, $y \in G$ on a $(x \circ y)' = y' \circ x'$.*
2. *Pour tous $x \in G$, $n \in \mathbb{Z}$ on a $(x^n)' = (x')^n = x^{-n}$.*

Proposition 1.10 (Règles de calcul dans un groupe)

Soit $(G, \circ)$ un groupe.

1. *Pour tous x, $y \in G$ on a $(x \circ y)' = y' \circ x'$.*
2. *Pour tous $x \in G$, $n \in \mathbb{Z}$ on a $(x^n)' = (x')^n = x^{-n}$.*
3. *Pour tous $x \in G$, m, $n \in \mathbb{Z}$ on a $x^n \circ x^m = x^{n+m}$.*

Proposition 1.10 (Règles de calcul dans un groupe)

Soit $(G, \circ)$ un groupe.

1. *Pour tous x, $y \in G$ on a $(x \circ y)' = y' \circ x'$.*
2. *Pour tous $x \in G$, $n \in \mathbb{Z}$ on a $(x^n)' = (x')^n = x^{-n}$.*
3. *Pour tous $x \in G$, m, $n \in \mathbb{Z}$ on a $x^n \circ x^m = x^{n+m}$.*
4. *Pour tous $x \in G$, m, $n \in \mathbb{Z}$ on a $(x^m)^n = x^{mn}$.*

Proposition 1.10 (Règles de calcul dans un groupe)

Soit $(G, \circ)$ un groupe.

1. *Pour tous x, $y \in G$ on a $(x \circ y)' = y' \circ x'$.*
2. *Pour tous $x \in G$, $n \in \mathbb{Z}$ on a $(x^n)' = (x')^n = x^{-n}$.*
3. *Pour tous $x \in G$, m, $n \in \mathbb{Z}$ on a $x^n \circ x^m = x^{n+m}$.*
4. *Pour tous $x \in G$, m, $n \in \mathbb{Z}$ on a $(x^m)^n = x^{mn}$.*

Dém: 1. Nous vérifions que $y' \circ x'$ satisfait aux propriétés qui caractérisent l'élément symétrique de $x \circ y$.

Proposition 1.10 (Règles de calcul dans un groupe)

Soit $(G, \circ)$ un groupe.

1. *Pour tous $x, y \in G$ on a $(x \circ y)' = y' \circ x'$.*
2. *Pour tous $x \in G$, $n \in \mathbb{Z}$ on a $(x^n)' = (x')^n = x^{-n}$.*
3. *Pour tous $x \in G$, $m, n \in \mathbb{Z}$ on a $x^n \circ x^m = x^{n+m}$.*
4. *Pour tous $x \in G$, $m, n \in \mathbb{Z}$ on a $(x^m)^n = x^{mn}$.*

Dém: 1. Nous vérifions que $y' \circ x'$ satisfait aux propriétés qui caractérisent l'élément symétrique de $x \circ y$. On a

$$(x \circ y) \circ (y' \circ x') = x \circ (y \circ y') \circ x' = x \circ e \circ x' = x \circ x' = e$$

Proposition 1.10 (Règles de calcul dans un groupe)

Soit $(G, \circ)$ un groupe.

1. *Pour tous x, $y \in G$ on a $(x \circ y)' = y' \circ x'$.*
2. *Pour tous $x \in G$, $n \in \mathbb{Z}$ on a $(x^n)' = (x')^n = x^{-n}$.*
3. *Pour tous $x \in G$, m, $n \in \mathbb{Z}$ on a $x^n \circ x^m = x^{n+m}$.*
4. *Pour tous $x \in G$, m, $n \in \mathbb{Z}$ on a $(x^m)^n = x^{mn}$.*

Dém: 1. Nous vérifions que $y' \circ x'$ satisfait aux propriétés qui caractérisent l'élément symétrique de $x \circ y$. On a

$$(x \circ y) \circ (y' \circ x') = x \circ (y \circ y') \circ x' = x \circ e \circ x' = x \circ x' = e$$

$$(y' \circ x') \circ (x \circ y) = y' \circ (x' \circ x) \circ y = y' \circ y = e\,.$$

Donc $y' \circ x'$ est bien l'élément symétrique de $x \circ y$.

2. On traite d'abord le cas $n \in \mathbb{N}$, puis le cas $n \in \mathbb{Z}_-$. Dans chaque cas on utilise la récurrence.

2. On traite d'abord le cas $n \in \mathbb{N}$, puis le cas $n \in \mathbb{Z}_-$. Dans chaque cas on utilise la récurrence.

3. Pour $n \in \mathbb{Z}$ fixé soit P_n la proposition : « Pout tout $m \in \mathbb{Z}$ on a $x^n \circ x^m = x^{n+m}$ ». On démontre par récurrence que P_n est vraie pour tout $n \in \mathbb{N}$, puis on démontre par récurrence que P_{-n} est vraie pour tout $n \in \mathbb{N}$.

2. On traite d'abord le cas $n \in \mathbb{N}$, puis le cas $n \in \mathbb{Z}_-$. Dans chaque cas on utilise la récurrence.

3. Pour $n \in \mathbb{Z}$ fixé soit P_n la proposition : « Pout tout $m \in \mathbb{Z}$ on a $x^n \circ x^m = x^{n+m}$ ». On démontre par récurrence que P_n est vraie pour tout $n \in \mathbb{N}$, puis on démontre par récurrence que P_{-n} est vraie pour tout $n \in \mathbb{N}$.

4. Pour $n \in \mathbb{Z}$ fixé soit P_n la proposition : « Pout tout $m \in \mathbb{Z}$ on a $(x^m)^n = x^{mn}$ ». On applique la méthode utilisée pour démontrer 3.

■

Remarque 1.11

Si la loi de composition interne d'un groupe est notée additivement (par $+$), alors on utilise la notation nx au lieu de x^n. On va poser alors

$$nx := \begin{cases} \underbrace{x + x + \ldots + x}_{n \text{ fois}} & \text{si} \quad n > 0 \\ e & \text{si} \quad n = 0 \\ |n|x' & \text{si} \quad n < 0 \ . \end{cases}$$

Remarque 1.11

Si la loi de composition interne d'un groupe est notée additivement (par $+$), alors on utilise la notation nx au lieu de x^n. On va poser alors

$$nx := \begin{cases} \underbrace{x + x + \ldots + x}_{n \text{ fois}} & \text{si} \quad n > 0 \\ e & \text{si} \quad n = 0 \\ |n|x' & \text{si} \quad n < 0 \ . \end{cases}$$

En particulier on aura $(-1)x = x'$ donc, pour une lci de groupe en notation additive, on pourra utiliser la notation $-x$ au lieu de x'.

Reformuler les règles de calcul dans un groupe $(G, +)$ en utilisant la notation additive nx. La notation additive $+$ est réservée aux lois de composition internes commutatives.

Définition 1.12

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes. Une application $f : G \to \tilde{G}$ est dite homomorphisme (morphisme) de groupes si

$$\forall (x, y) \in G \times G,\ f(x \circ y) = f(x) * f(y)\,.$$

Définition 1.12

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes. Une application $f : G \to \tilde{G}$ est dite homomorphisme (morphisme) de groupes si

$$\forall (x, y) \in G \times G,\ f(x \circ y) = f(x) * f(y)\,.$$

Un morphisme f est dit monomorphisme s'il est injectif, est dit épimorphisme s'il est surjectif et est dit isomorphisme s'il est bijectif.

Définition 1.12

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes. Une application $f : G \to \tilde{G}$ est dite homomorphisme (morphisme) de groupes si

$$\forall (x, y) \in G \times G,\ f(x \circ y) = f(x) * f(y)\,.$$

Un morphisme f est dit monomorphisme s'il est injectif, est dit épimorphisme s'il est surjectif et est dit isomorphisme s'il est bijectif. Deux groupes $(G, \circ)$, $(\tilde{G}, *)$ sont dits isomorphes s'il existe un isomorphisme $f : G \to \tilde{G}$.

Définition 1.12

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes. Une application $f : G \to \tilde{G}$ est dite homomorphisme (morphisme) de groupes si

$$\forall (x, y) \in G \times G,\ f(x \circ y) = f(x) * f(y)\,.$$

Un morphisme f est dit monomorphisme s'il est injectif, est dit épimorphisme s'il est surjectif et est dit isomorphisme s'il est bijectif. Deux groupes $(G, \circ)$, $(\tilde{G}, *)$ sont dits isomorphes s'il existe un isomorphisme $f : G \to \tilde{G}$.

Si f est un isomorphisme, l'application réciproque f^{-1} sera aussi un isomorphisme. Pourquoi ?

Définition 1.12

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes. Une application $f : G \to \tilde{G}$ est dite homomorphisme (morphisme) de groupes si

$$\forall (x, y) \in G \times G,\ f(x \circ y) = f(x) * f(y)\,.$$

Un morphisme f est dit monomorphisme s'il est injectif, est dit épimorphisme s'il est surjectif et est dit isomorphisme s'il est bijectif. Deux groupes $(G, \circ)$, $(\tilde{G}, *)$ sont dits isomorphes s'il existe un isomorphisme $f : G \to \tilde{G}$.

Si f est un isomorphisme, l'application réciproque f^{-1} sera aussi un isomorphisme. Pourquoi ?
Deux groupes isomorphes ont les mêmes propriétés algébriques.
Par exemple si l'un est abélien, l'autre sera aussi abélien.

Exemple 1.10

L'application $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est un isomorphisme $(\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$.

Exemple 1.10

L'application $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est un isomorphisme $(\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$.

Exemple 1.11

Soient $n_1, \ldots, n_k \in \mathbb{N}^*$ et soit $n := \prod_{i=1}^k n_i$. L'application

$$f : \mathbb{Z}_n \to \times_{i=1}^k \mathbb{Z}_{n_i}, \ f([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k}).$$

(qui intervient dans le théorème des restes chinois) est un morphisme de groupes *additifs*,

Exemple 1.10

L'application $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est un isomorphisme $(\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$.

Exemple 1.11

Soient $n_1, \ldots, n_k \in \mathbb{N}^*$ et soit $n := \prod_{i=1}^k n_i$. L'application

$$f : \mathbb{Z}_n \to \times_{i=1}^k \mathbb{Z}_{n_i}, \ f([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k}).$$

(qui intervient dans le théorème des restes chinois) est un morphisme de groupes *additifs*, qui induit un morphisme de groupes *multiplicatifs* $h : \mathbb{Z}_n^\times \to \times_{i=1}^k \mathbb{Z}_{n_i}^\times$.

Exemple 1.10

L'application $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est un isomorphisme $(\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$.

Exemple 1.11

Soient $n_1, \ldots, n_k \in \mathbb{N}^*$ et soit $n := \prod_{i=1}^k n_i$. L'application

$$f : \mathbb{Z}_n \to \times_{i=1}^k \mathbb{Z}_{n_i}, \ f([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k}).$$

(qui intervient dans le théorème des restes chinois) est un morphisme de groupes *additifs*, qui induit un morphisme de groupes *multiplicatifs* $h : \mathbb{Z}_n^\times \to \times_{i=1}^k \mathbb{Z}_{n_i}^\times$.

Si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, alors f et h sont des isomorphismes.

Toute composition de deux morphismes (monomorphismes, épimorphismes, isomorphismes) est aussi un morphisme (respectivement monomorphisme, épimorphisme, isomorphisme).

Toute composition de deux morphismes (monomorphismes, épimorphismes, isomorphismes) est aussi un morphisme (respectivement monomorphisme, épimorphisme, isomorphisme).

Démontrer ces affirmations.

Toute composition de deux morphismes (monomorphismes, épimorphismes, isomorphismes) est aussi un morphisme (respectivement monomorphisme, épimorphisme, isomorphisme).

Démontrer ces affirmations.

Remarque 1.13

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes et soient e, $\tilde{e}$ leurs éléments neutres respectivement. Soit $f : G \to \tilde{G}$ un homomorphisme de groupes. Alors

1. $f(e) = \tilde{e}$,

Toute composition de deux morphismes (monomorphismes, épimorphismes, isomorphismes) est aussi un morphisme (respectivement monomorphisme, épimorphisme, isomorphisme).

Démontrer ces affirmations.

Remarque 1.13

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes et soient e, $\tilde{e}$ leurs éléments neutres respectivement. Soit $f : G \to \tilde{G}$ un homomorphisme de groupes. Alors

1. $f(e) = \tilde{e}$,
2. *Pour tout $x \in G$ on a $f(x') = (f(x))'$.*

Toute composition de deux morphismes (monomorphismes, épimorphismes, isomorphismes) est aussi un morphisme (respectivement monomorphisme, épimorphisme, isomorphisme).

Démontrer ces affirmations.

Remarque 1.13

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes et soient e, $\tilde{e}$ leurs éléments neutres respectivement. Soit $f : G \to \tilde{G}$ un homomorphisme de groupes. Alors

1. $f(e) = \tilde{e}$,
2. *Pour tout $x \in G$ on a $f(x') = (f(x))'$.*
3. *Pour tout $x \in G$ et $k \in \mathbb{Z}$ on a $f(x^k) = f(x)^k$.*

Dém: 1. En effet, f étant un morphisme de groupes on a

$$f(e) = f(e \circ e) = f(e) * f(e)\,.$$

Dém: 1. En effet, f étant un morphisme de groupes on a

$$f(e) = f(e \circ e) = f(e) * f(e)\,.$$

En composant les deux membres par l'élément symétrique $f(e)'$ de $f(e)$ et en utilisant l'associativité de $*$ on obtient bien $f(e) = \tilde{e}$.

Dém: 1. En effet, f étant un morphisme de groupes on a

$$f(e) = f(e \circ e) = f(e) * f(e)\,.$$

En composant les deux membres par l'élément symétrique $f(e)'$ de $f(e)$ et en utilisant l'associativité de $*$ on obtient bien $f(e) = \tilde{e}$.

2. On a

$$f(x') * f(x) = f(x \circ x') = f(e) = \tilde{e}\ ,$$

donc (en composant à droite les deux membres par $f(x)'$), on obtient bien $f(x') = (f(x))'$.

Dém: 1. En effet, f étant un morphisme de groupes on a

$$f(e) = f(e \circ e) = f(e) * f(e)\,.$$

En composant les deux membres par l'élément symétrique $f(e)'$ de $f(e)$ et en utilisant l'associativité de $*$ on obtient bien $f(e) = \tilde{e}$.

2. On a

$$f(x') * f(x) = f(x \circ x') = f(e) = \tilde{e}\ ,$$

donc (en composant à droite les deux membres par $f(x)'$), on obtient bien $f(x') = (f(x))'$.

3. On considère deux cas :

(a) $k \in \mathbb{N}$,

(b) $-k \in \mathbb{N}^*$.

Dans chaque cas on utilise la récurrence. ■

Définition 1.14

Soit $(G, \circ)$ un groupe. Un sous-ensemble $H \subset G$ s'appelle sous-groupe si les deux conditions suivantes sont vérifiées :

(i) $H \neq \emptyset$,

Définition 1.14

Soit $(G, \circ)$ un groupe. Un sous-ensemble $H \subset G$ s'appelle sous-groupe si les deux conditions suivantes sont vérifiées :

(i) $H \neq \emptyset$,

(ii) *pour tous les x, $y \in H$ on a $x \circ y' \in H$.*

Définition 1.14

Soit $(G, \circ)$ un groupe. Un sous-ensemble $H \subset G$ s'appelle sous-groupe si les deux conditions suivantes sont vérifiées :

(i) $H \neq \emptyset$,

(ii) *pour tous les x, $y \in H$ on a $x \circ y' \in H$.*

Nous avons une manière équivalente de définir cette notion :

Proposition 1.15

$H \subset G$ est un sous-groupe si et seulement si les trois conditions suivantes sont vérifiées :

1. $e \in H$,

Définition 1.14

Soit $(G, \circ)$ un groupe. Un sous-ensemble $H \subset G$ s'appelle sous-groupe si les deux conditions suivantes sont vérifiées :

(i) $H \neq \emptyset$,

(ii) *pour tous les x, $y \in H$ on a $x \circ y' \in H$.*

Nous avons une manière équivalente de définir cette notion :

Proposition 1.15

$H \subset G$ est un sous-groupe si et seulement si les trois conditions suivantes sont vérifiées :

1. $e \in H$,
2. *pour tous les x, $y \in H$ on a $x \circ y \in H$,*

Définition 1.14

Soit $(G, \circ)$ un groupe. Un sous-ensemble $H \subset G$ s'appelle sous-groupe si les deux conditions suivantes sont vérifiées :

(i) $H \neq \emptyset$,

(ii) *pour tous les x, $y \in H$ on a $x \circ y' \in H$.*

Nous avons une manière équivalente de définir cette notion :

Proposition 1.15

$H \subset G$ est un sous-groupe si et seulement si les trois conditions suivantes sont vérifiées :

1. $e \in H$,
2. *pour tous les x, $y \in H$ on a $x \circ y \in H$,*
3. *pour tout $x \in H$ on a $x' \in H$.*

Dém: Exercice.

En utilisant la proposition précédente on obtient facilement :

Remarque 1.16

Soit $H \subset G$ un sous-groupe et soit $x \in H$. Alors pour tout $k \in \mathbb{Z}$ on a $x^k \in H$.

En utilisant la proposition précédente on obtient facilement :

Remarque 1.16

Soit $H \subset G$ un sous-groupe et soit $x \in H$. Alors pour tout $k \in \mathbb{Z}$ on a $x^k \in H$.

Si H est un sous-groupe, alors la restriction

$$\circ|_{H\times H} : H \times H \to H$$

de $\circ$ à $H \times H$ définit une lci sur H et, muni de cette lci, H devient lui-même un groupe (avec le même élément neutre e que celui de $(G, \circ)$).

En utilisant la proposition précédente on obtient facilement :

Remarque 1.16

Soit $H \subset G$ un sous-groupe et soit $x \in H$. Alors pour tout $k \in \mathbb{Z}$ on a $x^k \in H$.

Si H est un sous-groupe, alors la restriction

$$\circ_{|H\times H} : H \times H \to H$$

de $\circ$ à $H \times H$ définit une lci sur H et, muni de cette lci, H devient lui-même un groupe (avec le même élément neutre e que celui de $(G, \circ)$).

Pour $x \in H$ l'élément symétrique de x dans le groupe $(H, \circ_{|H\times H})$ coïncide avec son élément symétrique dans $(G, \circ)$.

Exemples 1.1

1. Soit $(G, *)$ un groupe. Alors $\{e\}$, G sont sous-groupes de $(G, *)$. $\{e\}$ s'appelle le sous-groupe trivial de $(G, *)$.

Exemples 1.1

1. Soit $(G, *)$ un groupe. Alors $\{e\}$, G sont sous-groupes de $(G, *)$. $\{e\}$ s'appelle le sous-groupe trivial de $(G, *)$.

2. Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z} \subset \mathbb{Z}$ est sous-groupe de $(\mathbb{Z}, +)$. On peut montrer que tout sous-groupe de $\mathbb{Z}$ est de cette forme.

Exemples 1.1

1. Soit $(G, *)$ un groupe. Alors $\{e\}$, G sont sous-groupes de $(G, *)$. $\{e\}$ s'appelle le sous-groupe trivial de $(G, *)$.

2. Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z} \subset \mathbb{Z}$ est sous-groupe de $(\mathbb{Z}, +)$. On peut montrer que tout sous-groupe de $\mathbb{Z}$ est de cette forme.

3. Les inclusion $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des inclusions de sous-groupes (par rapport à l'addition).

Exemples 1.1

1. Soit $(G, *)$ un groupe. Alors $\{e\}$, G sont sous-groupes de $(G, *)$. $\{e\}$ s'appelle le sous-groupe trivial de $(G, *)$.

2. Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z} \subset \mathbb{Z}$ est sous-groupe de $(\mathbb{Z}, +)$. On peut montrer que tout sous-groupe de $\mathbb{Z}$ est de cette forme.

3. Les inclusion $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des inclusions de sous-groupes (par rapport à l'addition).

4. Les inclusion $\{\pm 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$ sont des inclusions de sous-groupes (par rapport à la multiplication).

Exemples 1.1

1. Soit $(G, *)$ un groupe. Alors $\{e\}$, G sont sous-groupes de $(G, *)$. $\{e\}$ s'appelle le sous-groupe trivial de $(G, *)$.

2. Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z} \subset \mathbb{Z}$ est sous-groupe de $(\mathbb{Z}, +)$. On peut montrer que tout sous-groupe de $\mathbb{Z}$ est de cette forme.

3. Les inclusion $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des inclusions de sous-groupes (par rapport à l'addition).

4. Les inclusion $\{\pm 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$ sont des inclusions de sous-groupes (par rapport à la multiplication).

5. Soient $\mathrm{U} := \{z \in \mathbb{C} |\ |z| = 1\}$, $\mathrm{U}_n := \{z \in \mathbb{C} |\ z^n = 1\}$. Les inclusions $\mathrm{U}_n \subset \mathrm{U} \subset \mathbb{C}^*$ sont des inclusions de sous-groupes (par rapport à la multiplication).

Définition 1.17

Soit $(G, \circ)$ un groupe. Un sous-groupe $H \subset G$ est dit sous-groupe normal (ou distingué) si pour tout $x \in G$ et tout $h \in H$ on a $x \circ h \circ x' \in H$.

Définition 1.17

Soit $(G, \circ)$ un groupe. Un sous-groupe $H \subset G$ est dit sous-groupe normal (ou distingué) si pour tout $x \in G$ et tout $h \in H$ on a $x \circ h \circ x' \in H$.

La condition "pour tout $x \in G$ et tout $h \in H$ on a $x \circ h \circ x' \in H$" peut être reformulée : pour tout $x \in G$ on a

$$x \circ H \circ x' \subset H.$$

Ici on a utilisé la notation

$$x \circ H \circ y := \{x \circ h \circ y | \ h \in H\} \ .$$

Remarque 1.18

Si $H \subset G$ est un sous-groupe normal (distingué), alors pour tout $x \in G$ on a $x \circ H \circ x' = H$.

Remarque 1.18

Si $H \subset G$ est un sous-groupe normal (distingué), alors pour tout $x \in G$ on a $x \circ H \circ x' = H$.

Dém: Soit $x \in G$. Puisque H est normal on a

$$x \circ H \circ x' \subset H,$$

Remarque 1.18

Si $H \subset G$ est un sous-groupe normal (distingué), alors pour tout $x \in G$ on a $x \circ H \circ x' = H$.

Dém: Soit $x \in G$. Puisque H est normal on a

$$x \circ H \circ x' \subset H,$$

donc il suffit de montrer l'inclusion inverse

$$H \subset x \circ H \circ x'.$$

Remarque 1.18

Si $H \subset G$ est un sous-groupe normal (distingué), alors pour tout $x \in G$ on a $x \circ H \circ x' = H$.

Dém: Soit $x \in G$. Puisque H est normal on a

$$x \circ H \circ x' \subset H,$$

donc il suffit de montrer l'inclusion inverse

$$H \subset x \circ H \circ x'.$$

Mais cette inclusion est équivalente à $(x') \circ H \circ (x')' \subset H$ (qui est vraie, parce que H est normal et $x' \in G$). ■

Exemples 1.2

1. $\{e\}$ est G sont sous-groupes normaux de $(G, *)$.

Exemples 1.2

1. $\{e\}$ est G sont sous-groupes normaux de $(G, *)$.

2. Si $(G, *)$ est un groupe abélien, alors tout sous-groupe de $(G, *)$ est normal (à justifier).

Exemples 1.2

1. $\{e\}$ est G sont sous-groupes normaux de $(G, *)$.

2. Si $(G, *)$ est un groupe abélien, alors tout sous-groupe de $(G, *)$ est normal (à justifier).

3. Le sous-ensemble

$$\mathrm{SL}(n, \mathbb{R}) := \{A \in \mathrm{GL}(n, \mathbb{R}) |\ \det(A) = 1\}$$

est un sous-groupe normal de $(\mathrm{GL}(n, \mathbb{R}), \cdot)$.

Exemples 1.2

1. $\{e\}$ est G sont sous-groupes normaux de $(G, *)$.

2. Si $(G, *)$ est un groupe abélien, alors tout sous-groupe de $(G, *)$ est normal (à justifier).

3. Le sous-ensemble

$$\mathrm{SL}(n, \mathbb{R}) := \{A \in \mathrm{GL}(n, \mathbb{R}) |\ \det(A) = 1\}$$

est un sous-groupe normal de $(\mathrm{GL}(n, \mathbb{R}), \cdot)$. En effet, pour un couple $(B, A) \in \mathrm{GL}(n, \mathbb{R}) \times \mathrm{GL}(n, \mathbb{R})$ on a

$$\det(BAB^{-1}) = \det(B)\det(A)\det(B)^{-1} = \det(A),$$

donc $BAB^{-1} \in \mathrm{SL}(n, \mathbb{R})$ si $A \in \mathrm{SL}(n, \mathbb{R})$.

4. Soit $(\mathfrak{S}_n, \circ)$ le groupe symétrique de degré n et

$$\mathrm{A}_n := \{\sigma \in \mathfrak{S}_n | \ \varepsilon(\sigma) = 1\} \subset \mathfrak{S}_n$$

le sous-ensemble des permutations paires (de signature $+1$).

4. Soit $(\mathfrak{S}_n, \circ)$ le groupe symétrique de degré n et

$$\mathrm{A}_n := \{\sigma \in \mathfrak{S}_n | \ \varepsilon(\sigma) = 1\} \subset \mathfrak{S}_n$$

le sous-ensemble des permutations paires (de signature $+1$). A_n est un sous-groupe normal de $(\mathfrak{S}_n, \circ)$.

4. Soit $(\mathfrak{S}_n, \circ)$ le groupe symétrique de degré n et

$$\mathrm{A}_n := \{\sigma \in \mathfrak{S}_n | \ \varepsilon(\sigma) = 1\} \subset \mathfrak{S}_n$$

le sous-ensemble des permutations paires (de signature $+1$). A_n est un sous-groupe normal de $(\mathfrak{S}_n, \circ)$. En effet, pour un couple $(\sigma, \eta) \in \mathfrak{S}_n \times \mathfrak{S}_n$ on a $\varepsilon(\sigma \circ \eta \circ \sigma^{-1}) = \varepsilon(\eta)$, donc, en supposant $\eta \in \mathrm{A}_n$, on obtient $\sigma \circ \eta \circ \sigma^{-1} \in \mathrm{A}_n$.

4. Soit $(\mathfrak{S}_n, \circ)$ le groupe symétrique de degré n et

$$\mathrm{A}_n := \{\sigma \in \mathfrak{S}_n |\ \varepsilon(\sigma) = 1\} \subset \mathfrak{S}_n$$

le sous-ensemble des permutations paires (de signature $+1$). A_n est un sous-groupe normal de $(\mathfrak{S}_n, \circ)$. En effet, pour un couple $(\sigma, \eta) \in \mathfrak{S}_n \times \mathfrak{S}_n$ on a $\varepsilon(\sigma \circ \eta \circ \sigma^{-1}) = \varepsilon(\eta)$, donc, en supposant $\eta \in \mathrm{A}_n$, on obtient $\sigma \circ \eta \circ \sigma^{-1} \in \mathrm{A}_n$.

5. Le sous-ensemble $H := \left\{\mathrm{id}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}$ est un sous-groupe de $\mathfrak{S}_3$, mais ce sous-groupe n'est pas normal.

4. Soit $(\mathfrak{S}_n, \circ)$ le groupe symétrique de degré n et

$$\mathrm{A}_n := \{\sigma \in \mathfrak{S}_n |\ \varepsilon(\sigma) = 1\} \subset \mathfrak{S}_n$$

le sous-ensemble des permutations paires (de signature $+1$). A_n est un sous-groupe normal de $(\mathfrak{S}_n, \circ)$. En effet, pour un couple $(\sigma, \eta) \in \mathfrak{S}_n \times \mathfrak{S}_n$ on a $\varepsilon(\sigma \circ \eta \circ \sigma^{-1}) = \varepsilon(\eta)$, donc, en supposant $\eta \in \mathrm{A}_n$, on obtient $\sigma \circ \eta \circ \sigma^{-1} \in \mathrm{A}_n$.

5. Le sous-ensemble $H := \left\{\mathrm{id}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}$ est un sous-groupe de $\mathfrak{S}_3$, mais ce sous-groupe n'est pas normal. En effet, en posant $\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, on a $\sigma \circ \tau \circ \sigma^{-1} \notin H$.

6. Le centre d'un groupe $(G, \circ)$ est défini par

$$Z(G) := \{x \in G | \ \forall y \in G, \ x \circ y = y \circ x\}.$$

$Z(G)$ est un sous-groupe normal et abélien de G.

6. Le centre d'un groupe $(G, \circ)$ est défini par

$$Z(G) := \{x \in G | \ \forall y \in G, \ x \circ y = y \circ x\}.$$

$Z(G)$ est un sous-groupe normal et abélien de G. Il coïncide avec G si $(G, \circ)$ est abélien.

6. Le centre d'un groupe $(G, \circ)$ est défini par

$$Z(G) := \{x \in G | \ \forall y \in G, \ x \circ y = y \circ x\}.$$

$Z(G)$ est un sous-groupe normal et abélien de G. Il coïncide avec G si $(G, \circ)$ est abélien. Quel est le centre de $\mathfrak{S}_3$?

6. Le centre d'un groupe $(G, \circ)$ est défini par

$$Z(G) := \{x \in G |\ \forall y \in G,\ x \circ y = y \circ x\}.$$

$Z(G)$ est un sous-groupe normal et abélien de G. Il coïncide avec G si $(G, \circ)$ est abélien. Quel est le centre de $\mathfrak{S}_3$?

Définition 1.19

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes avec éléments neutres $e \in G$, $\tilde{e} \in \tilde{G}$, $f : G \to \tilde{G}$ un morphisme de groupes. On pose

$$\ker(f) := \{x \in G |\ f(x) = \tilde{e}\} = f^{-1}(\{\tilde{e}\}),$$

6. Le centre d'un groupe $(G, \circ)$ est défini par

$$Z(G) := \{x \in G |\ \forall y \in G,\ x \circ y = y \circ x\}.$$

$Z(G)$ est un sous-groupe normal et abélien de G. Il coïncide avec G si $(G, \circ)$ est abélien. Quel est le centre de $\mathfrak{S}_3$?

Définition 1.19

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes avec éléments neutres $e \in G$, $\tilde{e} \in \tilde{G}$, $f : G \to \tilde{G}$ un morphisme de groupes. On pose

$$\ker(f) := \{x \in G |\ f(x) = \tilde{e}\} = f^{-1}(\{\tilde{e}\}),$$

$$\mathrm{im}(f) := \{y \in \tilde{G} |\ \exists x \in G, y = f(x)\} = \{f(x) |\ x \in G\}.$$

Remarque 1.20

Soient $(G, \circ)$, $(\tilde{G}, *)$ *deux groupes avec éléments neutres* $e \in G$, $\tilde{e} \in \tilde{G}$ *et* $f : G \to \tilde{G}$ *un homomorphisme de groupes.*

1. $\mathrm{im}(f)$ *est un sous-groupe de* $\tilde{G}$.

Remarque 1.20

Soient $(G, \circ)$, $(\tilde{G}, *)$ *deux groupes avec éléments neutres* $e \in G$, $\tilde{e} \in \tilde{G}$ *et* $f : G \to \tilde{G}$ *un homomorphisme de groupes.*

1. $\mathrm{im}(f)$ *est un sous-groupe de* $\tilde{G}$.
2. $\ker(f)$ *est un sous-groupe normal de* G.

Remarque 1.20

Soient $(G, \circ)$, $(\tilde{G}, *)$ *deux groupes avec éléments neutres* $e \in G$, $\tilde{e} \in \tilde{G}$ *et* $f : G \to \tilde{G}$ *un homomorphisme de groupes.*

1. $\mathrm{im}(f)$ *est un sous-groupe de* $\tilde{G}$.
2. $\ker(f)$ *est un sous-groupe normal de* G.
3. *Le sous-groupe* $\mathrm{im}(f) \subset \tilde{G}$ *est abélien si* G *est abélien.*

Remarque 1.20

Soient $(G, \circ)$, $(\tilde{G}, *)$ *deux groupes avec éléments neutres* $e \in G$, $\tilde{e} \in \tilde{G}$ *et* $f : G \to \tilde{G}$ *un homomorphisme de groupes.*

1. $\mathrm{im}(f)$ *est un sous-groupe de* $\tilde{G}$.
2. $\ker(f)$ *est un sous-groupe normal de* G.
3. *Le sous-groupe* $\mathrm{im}(f) \subset \tilde{G}$ *est abélien si* G *est abélien.*
4. f *est un monomorphisme si et seulement si* $\ker(f) = \{e\}$.

Remarque 1.20

Soient $(G, \circ)$, $(\tilde{G}, *)$ *deux groupes avec éléments neutres* $e \in G$, $\tilde{e} \in \tilde{G}$ *et* $f : G \to \tilde{G}$ *un homomorphisme de groupes.*

1. $\mathrm{im}(f)$ *est un sous-groupe de* $\tilde{G}$.
2. $\ker(f)$ *est un sous-groupe normal de* G.
3. *Le sous-groupe* $\mathrm{im}(f) \subset \tilde{G}$ *est abélien si* G *est abélien.*
4. f *est un monomorphisme si et seulement si* $\ker(f) = \{e\}$.
5. f *est un épimorphisme si et seulement si* $\mathrm{im}(f) = \tilde{G}$.

Remarque 1.20

Soient $(G, \circ)$, $(\tilde{G}, *)$ *deux groupes avec éléments neutres* $e \in G$, $\tilde{e} \in \tilde{G}$ *et* $f : G \to \tilde{G}$ *un homomorphisme de groupes.*

1. $\mathrm{im}(f)$ *est un sous-groupe de* $\tilde{G}$.
2. $\ker(f)$ *est un sous-groupe normal de* G.
3. *Le sous-groupe* $\mathrm{im}(f) \subset \tilde{G}$ *est abélien si* G *est abélien.*
4. f *est un monomorphisme si et seulement si* $\ker(f) = \{e\}$.
5. f *est un épimorphisme si et seulement si* $\mathrm{im}(f) = \tilde{G}$.

Dém: Exercice. ■

Exercice 1.2

Soient $f : G \to G'$, $g : G' \to G''$ homomorphismes de groupes. Montrer que $\ker(f) \subset \ker(g \circ f)$, $\mathrm{im}(g \circ f) \subset \mathrm{im}(g)$.

Exercice 1.2

Soient $f : G \to G'$, $g : G' \to G''$ homomorphismes de groupes. Montrer que $\ker(f) \subset \ker(g \circ f)$, $\mathrm{im}(g \circ f) \subset \mathrm{im}(g)$.

Remarque 1.21

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes et soit $f : G \to \tilde{G}$ un homomorphisme de groupes . Alors

1. *Pour tout sous-groupe $H \subset G$ l'image $f(H) := \{f(x) | \ x \in H\}$ est un sous-groupe de $(\tilde{G}, *)$.*

Exercice 1.2

Soient $f : G \to G'$, $g : G' \to G''$ homomorphismes de groupes. Montrer que $\ker(f) \subset \ker(g \circ f)$, $\mathrm{im}(g \circ f) \subset \mathrm{im}(g)$.

Remarque 1.21

Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes et soit $f : G \to \tilde{G}$ un homomorphisme de groupes . Alors

1. *Pour tout sous-groupe $H \subset G$ l'image $f(H) := \{f(x) | \ x \in H\}$ est un sous-groupe de $(\tilde{G}, *)$.*
2. *Pour tout sous-groupe $\tilde{H} \subset \tilde{G}$ l'image réciproque $f^{-1}(\tilde{H}) := \{x \in G | \ f(x) \in \tilde{H}\}$ est un sous-groupe de $(G, \circ)$. Ce sous-groupe est normal si $\tilde{H}$ est normal.*

En prenant $H = G$ (respectivement $\tilde{H} = \{\tilde{e}\}$) on obtient comme cas particuliers les sous-groupes $\mathrm{im}(f) \subset \tilde{G}$ (respectivement $\ker(f) \subset G$) définis ci-dessus.

En prenant $H = G$ (respectivement $\tilde{H} = \{\tilde{e}\}$) on obtient comme cas particuliers les sous-groupes $\mathrm{im}(f) \subset \tilde{G}$ (respectivement $\ker(f) \subset G$) définis ci-dessus.

Exercice 1.3

Soient $f : G \to \tilde{G}$ un morphisme et $H \subset G$ un sous-groupe. Si H est normal et f est surjective alors $f(H)$ est normal .

Table of Contents

Soit $(G, \circ)$ un groupe, e son élément neutre.

Définition 2.1

Soit $x \in G$. On dit que x est un élément de torsion ou un élément d'ordre fini s'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$.

Soit $(G, \circ)$ un groupe, e son élément neutre.

Définition 2.1

Soit $x \in G$. On dit que x est un élément de torsion ou un élément d'ordre fini s'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$. Si c'est le cas, alors on définit l'ordre de x par

$$\mathrm{ord}(x) := \min\{k \in \mathbb{N}^* | \ x^k = e\}\,.$$

Soit $(G, \circ)$ un groupe, e son élément neutre.

Définition 2.1

Soit $x \in G$. On dit que x est un élément de torsion ou un élément d'ordre fini s'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$. Si c'est le cas, alors on définit l'ordre de x par

$$\mathrm{ord}(x) := \min\{k \in \mathbb{N}^* | \ x^k = e\}.$$

Si l'ensemble $\{k \in \mathbb{N}^* | \ x^k = e\}$ est vide, on va dire que x est un élément d'ordre infini.

Exemples 2.1

1. L'ordre de i dans le groupe $(\mathbb{C}^*, \cdot)$ est 4.

Exemples 2.1

1. L'ordre de i dans le groupe $(\mathbb{C}^*, \cdot)$ est 4.
2. Le nombre complexe $2i$ est un élément d'ordre infini dans le groupe $(\mathbb{C}^*, \cdot)$.

Exemples 2.1

1. L'ordre de i dans le groupe $(\mathbb{C}^*, \cdot)$ est 4.
2. Le nombre complexe $2i$ est un élément d'ordre infini dans le groupe $(\mathbb{C}^*, \cdot)$.
3. La permutation $(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in \mathfrak{S}_3$ est un 3-cycle, donc un élément d'ordre 3 dans $(\mathfrak{S}_3, \circ)$.

Exemples 2.1

1. L'ordre de i dans le groupe $(\mathbb{C}^*, \cdot)$ est 4.
2. Le nombre complexe $2i$ est un élément d'ordre infini dans le groupe $(\mathbb{C}^*, \cdot)$.
3. La permutation $(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in \mathfrak{S}_3$ est un 3-cycle, donc un élément d'ordre 3 dans $(\mathfrak{S}_3, \circ)$.

Définition 2.2

Soit $x \in G$. Le sous-groupe cyclique (monogène) engendré par x est défini par :

$$\langle x \rangle := \{x^k |\ k \in \mathbb{Z}\} = \{y \in G |\ \exists k \in \mathbb{Z},\ y = x^k\}.$$

Remarque 2.3

Soit $x \in G$. Alors

1. *$\langle x \rangle$ est bien un sous-groupe de $(G, \circ)$. Ce sous-groupe est abélien.*

Remarque 2.3

Soit $x \in G$. Alors

1. *$\langle x \rangle$ est bien un sous-groupe de $(G, \circ)$. Ce sous-groupe est abélien.*
2. *$\langle x \rangle$ est le plus petit sous-groupe (au sens de l'inclusion) qui contient x. Plus précisément, pour tout sous-groupe $H \subset G$ tel que $x \in H$, on a $\langle x \rangle \subset H$.*

Dém: Exercice. ■

Remarque 2.3

Soit $x \in G$. Alors

1. *$\langle x \rangle$ est bien un sous-groupe de $(G, \circ)$. Ce sous-groupe est abélien.*
2. *$\langle x \rangle$ est le plus petit sous-groupe (au sens de l'inclusion) qui contient x. Plus précisément, pour tout sous-groupe $H \subset G$ tel que $x \in H$, on a $\langle x \rangle \subset H$.*

Dém: Exercice. ■

Définition équivalente du sous-groupe $\langle x \rangle$: L'application

$$F_x : \mathbb{Z} \to G, \ F_x(k) := x^k .$$

est un morphisme $(\mathbb{Z}, +) \to (G, \circ)$. On a $\langle x \rangle = \mathrm{im}(F_x)$.

Proposition 2.4

Soit $x \in G$ un élément d'ordre fini n. Alors

1. $\ker(F_x) = n\mathbb{Z}$.

Proposition 2.4

Soit $x \in G$ un élément d'ordre fini n. Alors

1. $\ker(F_x) = n\mathbb{Z}$.
2. *F_x est compatible avec la relation d'équivalence $\underset{n}{\equiv}$ sur $\mathbb{Z}$. En particulier F_x induit une application*

$$f_x : \mathbb{Z}_n \to G,\ f_x([k]_n) = F_x(k) = x^k.$$

Proposition 2.4

Soit $x \in G$ un élément d'ordre fini n. Alors

1. $\ker(F_x) = n\mathbb{Z}$.
2. *F_x est compatible avec la relation d'équivalence $\underset{n}{\equiv}$ sur $\mathbb{Z}$. En particulier F_x induit une application*

$$f_x : \mathbb{Z}_n \to G, \ f_x([k]_n) = F_x(k) = x^k.$$

3. *f_x est un monomorphisme $(\mathbb{Z}_n, +) \to (G, \circ)$ et son image est $\langle x \rangle$, donc f_x induit un isomorphisme $g_x : \mathbb{Z}_n \xrightarrow{\simeq} \langle x \rangle$.*

Proposition 2.4

Soit $x \in G$ un élément d'ordre fini n. Alors

1. $\ker(F_x) = n\mathbb{Z}$.
2. *F_x est compatible avec la relation d'équivalence $\underset{n}{\equiv}$ sur $\mathbb{Z}$. En particulier F_x induit une application*

$$f_x : \mathbb{Z}_n \to G, \ f_x([k]_n) = F_x(k) = x^k.$$

3. *f_x est un monomorphisme $(\mathbb{Z}_n, +) \to (G, \circ)$ et son image est $\langle x \rangle$, donc f_x induit un isomorphisme $g_x : \mathbb{Z}_n \xrightarrow{\simeq} \langle x \rangle$.*
4. *Les éléments $e, \ldots, x^{n-1}$ sont distincts deux à deux, $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$ et $|\langle x \rangle| = n$.*

La proposition nous précise explicitement le sous-ensemble $\langle x \rangle \subset G$ et affirme que le groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}_n$.

La proposition nous précise explicitement le sous-ensemble $\langle x \rangle \subset G$ et affirme que le groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}_n$.

Dém: (1) : Soit $k \in \mathbb{Z}$. En appliquant le TDE on obtient :

$$k = qn + r, \text{ avec } q, \ r \in \mathbb{Z}, \ 0 \leqslant r \leqslant n-1.$$

$$x^k = x^{nq+r} = x^{nq} \circ x^r = (x^n)^q \circ x^r = e^q \circ x^r = e \circ x^r = x^r \, .$$

La proposition nous précise explicitement le sous-ensemble $\langle x \rangle \subset G$ et affirme que le groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}_n$.

Dém: (1) : Soit $k \in \mathbb{Z}$. En appliquant le TDE on obtient :

$$k = qn + r, \text{ avec } q, \ r \in \mathbb{Z}, \ 0 \leqslant r \leqslant n-1.$$

$$x^k = x^{nq+r} = x^{nq} \circ x^r = (x^n)^q \circ x^r = e^q \circ x^r = e \circ x^r = x^r \, .$$

$$k \in \ker(F_x) \Leftrightarrow x^k = e \Leftrightarrow x^r = e \Leftrightarrow r = 0.$$

La proposition nous précise explicitement le sous-ensemble $\langle x \rangle \subset G$ et affirme que le groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}_n$.

Dém: (1) : Soit $k \in \mathbb{Z}$. En appliquant le TDE on obtient :

$$k = qn + r, \text{ avec } q,\ r \in \mathbb{Z},\ 0 \leqslant r \leqslant n-1.$$

$$x^k = x^{nq+r} = x^{nq} \circ x^r = (x^n)^q \circ x^r = e^q \circ x^r = e \circ x^r = x^r\ .$$

$$k \in \ker(F_x) \Leftrightarrow x^k = e \Leftrightarrow x^r = e \Leftrightarrow r = 0.$$

À justifier l'implication $x^r = e \Rightarrow r = 0$:

La proposition nous précise explicitement le sous-ensemble $\langle x \rangle \subset G$ et affirme que le groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}_n$.

Dém: (1) : Soit $k \in \mathbb{Z}$. En appliquant le TDE on obtient :

$$k = qn + r, \text{ avec } q,\ r \in \mathbb{Z},\ 0 \leqslant r \leqslant n-1.$$

$$x^k = x^{nq+r} = x^{nq} \circ x^r = (x^n)^q \circ x^r = e^q \circ x^r = e \circ x^r = x^r\,.$$

$$k \in \ker(F_x) \Leftrightarrow x^k = e \Leftrightarrow x^r = e \Leftrightarrow r = 0.$$

À justifier l'implication $x^r = e \Rightarrow r = 0$:

Si $r > 0$, r serait un élément de $\mathbb{N}^*$ inférieur à n tel que $x^r = e$, contredit la définition de $n = \mathrm{ord}(x)$.

La proposition nous précise explicitement le sous-ensemble $\langle x \rangle \subset G$ et affirme que le groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}_n$.

Dém: (1) : Soit $k \in \mathbb{Z}$. En appliquant le TDE on obtient :

$$k = qn + r, \text{ avec } q,\ r \in \mathbb{Z},\ 0 \leqslant r \leqslant n-1.$$

$$x^k = x^{nq+r} = x^{nq} \circ x^r = (x^n)^q \circ x^r = e^q \circ x^r = e \circ x^r = x^r\,.$$

$$k \in \ker(F_x) \Leftrightarrow x^k = e \Leftrightarrow x^r = e \Leftrightarrow r = 0.$$

À justifier l'implication $x^r = e \Rightarrow r = 0$:

Si $r > 0$, r serait un élément de $\mathbb{N}^*$ inférieur à n tel que $x^r = e$, contredit la définition de $n = \mathrm{ord}(x)$.

Donc $k \in \ker(F_x) \Leftrightarrow (r = 0) \Leftrightarrow k \in n\mathbb{Z}$, donc $\ker(F_x) = n\mathbb{Z}$.

(2) M. q. F_x est compatible avec $\underset{n}{\equiv}$. Nous avons :

$$u \underset{n}{\equiv} v \Leftrightarrow n\big|(v-u) \Leftrightarrow v-u \in n\mathbb{Z} = \ker(F_x)$$

$$\Leftrightarrow F_x(v-u) = e \Leftrightarrow F_x(v) \circ F_x(u)' = e \Leftrightarrow F_x(u) = F_x(v).$$

(2) M. q. F_x est compatible avec $\underset{n}{\equiv}$. Nous avons :

$$u \underset{n}{\equiv} v \Leftrightarrow n\big|(v-u) \Leftrightarrow v-u \in n\mathbb{Z} = \ker(F_x)$$

$$\Leftrightarrow F_x(v-u) = e \Leftrightarrow F_x(v) \circ F_x(u)' = e \Leftrightarrow F_x(u) = F_x(v).$$

(3) Soit $f_x : \mathbb{Z}_n \to G$ l'application induite par F_x.

(2) M. q. F_x est compatible avec $\underset{n}{\equiv}$. Nous avons :

$$u \underset{n}{\equiv} v \Leftrightarrow n|(v-u) \Leftrightarrow v-u \in n\mathbb{Z} = \ker(F_x)$$

$$\Leftrightarrow F_x(v-u) = e \Leftrightarrow F_x(v) \circ F_x(u)' = e \Leftrightarrow F_x(u) = F_x(v).$$

(3) Soit $f_x : \mathbb{Z}_n \to G$ l'application induite par F_x.

M. q. f_x est injective. Soient $[u]_n, [v]_n \in \mathbb{Z}_n$.

$$f_x([u]_n) = f_x([v]_n) \Leftrightarrow F_x(u) = F_x(v) \Leftrightarrow u \underset{n}{\equiv} v \Leftrightarrow [u]_n = [v]_n.$$

(2) M. q. F_x est compatible avec $\underset{n}{\equiv}$. Nous avons :

$$u \underset{n}{\equiv} v \Leftrightarrow n|(v-u) \Leftrightarrow v-u \in n\mathbb{Z} = \ker(F_x)$$

$$\Leftrightarrow F_x(v-u) = e \Leftrightarrow F_x(v) \circ F_x(u)' = e \Leftrightarrow F_x(u) = F_x(v).$$

(3) Soit $f_x : \mathbb{Z}_n \to G$ l'application induite par F_x.

M. q. f_x est injective. Soient $[u]_n, [v]_n \in \mathbb{Z}_n$.

$$f_x([u]_n) = f_x([v]_n) \Leftrightarrow F_x(u) = F_x(v) \Leftrightarrow u \underset{n}{\equiv} v \Leftrightarrow [u]_n = [v]_n.$$

M. q. f_x est morphisme de groupes :

$$f_x([u]_n + [v]_n) = f_x([u+v]_n) = F_x(u+v) = F_x(u) \circ F_x(v)$$

$$= f_x([u]_n) \circ f_x([v]_n).$$

Nous avons obtenu un monomorphisme $f_x : \mathbb{Z}_n \to G$ dont l'image est $\langle x \rangle$.

Nous avons obtenu un monomorphisme $f_x : \mathbb{Z}_n \to G$ dont l'image est $\langle x \rangle$.
Par restriction au but (corestriction), on obtient un isomorphisme $g_x : \mathbb{Z}_n \to \langle x \rangle$.

Nous avons obtenu un monomorphisme $f_x : \mathbb{Z}_n \to G$ dont l'image est $\langle x \rangle$.
Par restriction au but (corestriction), on obtient un isomorphisme $g_x : \mathbb{Z}_n \to \langle x \rangle$.

(4) Conséquence directe de (3).

Nous avons obtenu un monomorphisme $f_x : \mathbb{Z}_n \to G$ dont l'image est $\langle x \rangle$.
Par restriction au but (corestriction), on obtient un isomorphisme $g_x : \mathbb{Z}_n \to \langle x \rangle$.

(4) Conséquence directe de (3).

Remarque 2.5

Soit $x \in G$ un élément d'ordre infini. Alors $\ker(F_x) = \{0\}$, donc $F_x : \mathbb{Z} \to G$ est un monomorphisme. Par restriction au but on obtient un isomorphisme $g_x : \mathbb{Z} \xrightarrow{\simeq} \langle x \rangle$.

Nous avons obtenu un monomorphisme $f_x : \mathbb{Z}_n \to G$ dont l'image est $\langle x \rangle$.
Par restriction au but (corestriction), on obtient un isomorphisme $g_x : \mathbb{Z}_n \to \langle x \rangle$.

(4) Conséquence directe de (3).

Remarque 2.5

Soit $x \in G$ un élément d'ordre infini. Alors $\ker(F_x) = \{0\}$, donc $F_x : \mathbb{Z} \to G$ est un monomorphisme. Par restriction au but on obtient un isomorphisme $g_x : \mathbb{Z} \xrightarrow{\simeq} \langle x \rangle$.

Conclusion : Le sous-groupe cyclique $\langle x \rangle$ engendré par x est isomorphe à $\mathbb{Z}_n$ si x est d'ordre fini n et est isomorphe à $\mathbb{Z}$ si x est d'ordre infini.

Définition 2.6

Un groupe $(G, \circ)$ est dit groupe cyclique (ou monogène) s'il existe $x \in G$ tel que $G = \langle x \rangle$. Si c'est le cas, on dira que x est un générateur de G ou que G est engendré par x.

Définition 2.6

Un groupe $(G, \circ)$ est dit groupe cyclique (ou monogène) s'il existe $x \in G$ tel que $G = \langle x \rangle$. Si c'est le cas, on dira que x est un générateur de G ou que G est engendré par x.

Définition équivalente : $(G, \circ)$ est un groupe cyclique de générateur x si le morphisme $F_x : \mathbb{Z} \to G$ est un épimorphisme.

Définition 2.6

Un groupe $(G, \circ)$ est dit groupe cyclique (ou monogène) s'il existe $x \in G$ tel que $G = \langle x \rangle$. Si c'est le cas, on dira que x est un générateur de G ou que G est engendré par x.

Définition équivalente : $(G, \circ)$ est un groupe cyclique de générateur x si le morphisme $F_x : \mathbb{Z} \to G$ est un épimorphisme.

Exemple 2.1

Soit $n \in \mathbb{N}^*$. Le groupe $(\mathrm{U}_n, \cdot)$ est cyclique engendré par $e^{\frac{2\pi i}{n}}$.

Définition 2.6

Un groupe $(G, \circ)$ est dit groupe cyclique (ou monogène) s'il existe $x \in G$ tel que $G = \langle x \rangle$. Si c'est le cas, on dira que x est un générateur de G ou que G est engendré par x.

Définition équivalente : $(G, \circ)$ est un groupe cyclique de générateur x si le morphisme $F_x : \mathbb{Z} \to G$ est un épimorphisme.

Exemple 2.1

Soit $n \in \mathbb{N}^*$. Le groupe $(\mathrm{U}_n, \cdot)$ est cyclique engendré par $e^{\frac{2\pi i}{n}}$.

Remarque 2.7

Tout groupe cyclique fini d'ordre n est isomorphe à $\mathbb{Z}_n$. Tout groupe cyclique infini est isomorphe à $\mathbb{Z}$.

Pour un groupe muni d'une lci en notation additive les notations utilisées ci-dessus changent :

Remarque 2.8

Soient $(G, +)$ un groupe en notation additive et $x \in G$. Alors :

1. *Le morphisme $F_x : \mathbb{Z} \to G$ associée à x s'écrit $F_x(k) = kx$.*

Pour un groupe muni d'une lci en notation additive les notations utilisées ci-dessus changent :

Remarque 2.8

Soient $(G, +)$ un groupe en notation additive et $x \in G$. Alors :

1. *Le morphisme $F_x : \mathbb{Z} \to G$ associée à x s'écrit $F_x(k) = kx$.*
2. *x est d'ordre fini (de torsion) s'il existe $k \in \mathbb{N}^*$ t. q. $kx = e$.*

Pour un groupe muni d'une lci en notation additive les notations utilisées ci-dessus changent :

Remarque 2.8

Soient $(G,+)$ un groupe en notation additive et $x \in G$. Alors :

1. *Le morphisme $F_x : \mathbb{Z} \to G$ associée à x s'écrit $F_x(k) = kx$.*
2. *x est d'ordre fini (de torsion) s'il existe $k \in \mathbb{N}^*$ t. q. $kx = e$.*
3. *Si x est d'ordre fini, alors $\mathrm{ord}(x) := \min\{k \in \mathbb{N}^* |\ kx = e\}$.*
4. *Le sous-groupe cyclique engendré par x est*

$$\langle x \rangle = \{kx |\ k \in \mathbb{Z}\} = \{y \in G |\ \exists k \in \mathbb{Z},\ y = kx\}.$$

Pour un groupe muni d'une lci en notation additive les notations utilisées ci-dessus changent :

Remarque 2.8

Soient $(G,+)$ un groupe en notation additive et $x \in G$. Alors :

1. *Le morphisme $F_x : \mathbb{Z} \to G$ associée à x s'écrit $F_x(k) = kx$.*
2. *x est d'ordre fini (de torsion) s'il existe $k \in \mathbb{N}^*$ t. q. $kx = e$.*
3. *Si x est d'ordre fini, alors $\operatorname{ord}(x) := \min\{k \in \mathbb{N}^* | \ kx = e\}$.*
4. *Le sous-groupe cyclique engendré par x est*

$$\langle x \rangle = \{kx | \ k \in \mathbb{Z}\} = \{y \in G | \ \exists k \in \mathbb{Z}, \ y = kx\}.$$

5. *Si $\operatorname{ord}(x) = n$, alors*

$$\langle x \rangle = \{e, x, \ldots, (n-1)x\}.$$

Exemples 2.2

1. $(\mathbb{Z}_n, +)$ est un groupe cyclique d'ordre n engendré par $[1]_n$.

Exemples 2.2

1. $(\mathbb{Z}_n, +)$ est un groupe cyclique d'ordre n engendré par $[1]_n$.
2. $(\mathbb{Z}, +)$ est un groupe cyclique infini engendré par 1.

Exemples 2.2

1. $(\mathbb{Z}_n, +)$ est un groupe cyclique d'ordre n engendré par $[1]_n$.
2. $(\mathbb{Z}, +)$ est un groupe cyclique infini engendré par 1.
3. Soit $n \in \mathbb{N}^*$. $(n\mathbb{Z}, +)$ est un groupe cyclique infini engendré par n.
4. En général le groupe produit $(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, +)$ (où $n_1, \ldots, n_k \in \mathbb{N}^*$) n'est pas cyclique. Par exemple dans $\mathbb{Z}_2 \times \mathbb{Z}_2$ tout élément est d'ordre $\leqslant 2$.

Exemples 2.2

1. $(\mathbb{Z}_n, +)$ est un groupe cyclique d'ordre n engendré par $[1]_n$.
2. $(\mathbb{Z}, +)$ est un groupe cyclique infini engendré par 1.
3. Soit $n \in \mathbb{N}^*$. $(n\mathbb{Z}, +)$ est un groupe cyclique infini engendré par n.
4. En général le groupe produit $(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, +)$ (où $n_1, \ldots, n_k \in \mathbb{N}^*$) n'est pas cyclique. Par exemple dans $\mathbb{Z}_2 \times \mathbb{Z}_2$ tout élément est d'ordre $\leqslant 2$.
   Si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, le théorème des restes chinois fournit un isomorphisme $f : \mathbb{Z}_n \to \times_{i=1}^{k} \mathbb{Z}_{n_i}$ où $n = \prod_{i=1}^{n} n_i$.

Exemples 2.2

1. $(\mathbb{Z}_n, +)$ est un groupe cyclique d'ordre n engendré par $[1]_n$.
2. $(\mathbb{Z}, +)$ est un groupe cyclique infini engendré par 1.
3. Soit $n \in \mathbb{N}^*$. $(n\mathbb{Z}, +)$ est un groupe cyclique infini engendré par n.
4. En général le groupe produit $(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, +)$ (où $n_1, \ldots, n_k \in \mathbb{N}^*$) n'est pas cyclique. Par exemple dans $\mathbb{Z}_2 \times \mathbb{Z}_2$ tout élément est d'ordre $\leqslant 2$.
   Si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, le théorème des restes chinois fournit un isomorphisme $f : \mathbb{Z}_n \to \times_{i=1}^{k} \mathbb{Z}_{n_i}$ où $n = \prod_{i=1}^{n} n_i$. Puisque $(\mathbb{Z}_n, +)$ est cyclique engendré par $[1]_n$, il en résulte que dans ce cas $(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, +)$ est cyclique engendré par $f([1]_n) = ([1]_{n_1}, \ldots, [1]_{n_k})$.

Table of Contents

Soient $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe. On va utiliser la notation simplifiée

$$xy := x \circ y.$$

Soient $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe. On va utiliser la notation simplifiée

$$xy := x \circ y.$$

Définition 3.1

Nous associons à H deux relations R_H, ${}_HR$ sur G :

1. $x \, R_H \, y$ *si* $x'y \in H$.

Soient $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe. On va utiliser la notation simplifiée

$$xy := x \circ y.$$

Définition 3.1

Nous associons à H deux relations R_H, ${}_HR$ sur G :

1. $x \, R_H \, y$ *si* $x'y \in H$.
2. $x \, {}_HR \, y$ *si* $xy' \in H$.

Soient $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe. On va utiliser la notation simplifiée

$$xy := x \circ y.$$

Définition 3.1

Nous associons à H deux relations R_H, ${}_HR$ sur G :

1. $x \, R_H \, y$ *si* $x'y \in H$.
2. $x \, {}_HR \, y$ *si* $xy' \in H$.

La proposition suivante montre que R_H, ${}_HR$ sont des relations d'équivalence et précise la classe d'équivalence d'un élément $x \in G$ par rapport à chacune de ces relations.

Proposition 3.2

1. *R_H, ${}_HR$ sont des relations d'équivalence sur G.*

Proposition 3.2

1. *R_H, ${}_HR$ sont des relations d'équivalence sur G.*
2. *La classe d'équivalence $[x]_H$ de x par rapport à R_H est*

$$[x]_H = xH := \{xh |\ h \in H\} .$$

Proposition 3.2

1. *R_H, ${}_HR$ sont des relations d'équivalence sur G.*
2. *La classe d'équivalence $[x]_H$ de x par rapport à R_H est*

$$[x]_H = xH := \{xh |\ h \in H\} .$$

3. *La classe d'équivalence ${}_H[x]$ de x par rapport à ${}_HR$ est*

$${}_H[x] = Hx := \{hx |\ h \in H\} .$$

Proposition 3.2

1. R_H, ${}_HR$ *sont des relations d'équivalence sur* G.
2. *La classe d'équivalence* $[x]_H$ *de* x *par rapport à* R_H *est*

$$[x]_H = xH := \{xh |\ h \in H\} .$$

3. *La classe d'équivalence* ${}_H[x]$ *de* x *par rapport à* ${}_HR$ *est*

$${}_H[x] = Hx := \{hx |\ h \in H\} .$$

Dém: Exercice ■

Proposition 3.2

1. R_H, ${}_HR$ *sont des relations d'équivalence sur* G.
2. *La classe d'équivalence* $[x]_H$ *de* x *par rapport à* R_H *est*

$$[x]_H = xH := \{xh |\ h \in H\} .$$

3. *La classe d'équivalence* ${}_H[x]$ *de* x *par rapport à* ${}_HR$ *est*

$${}_H[x] = Hx := \{hx |\ h \in H\} .$$

Dém: Exercice ■

Remarquer que la classe de l'élément neutre e (par rapport à R_H ou ${}_HR$) est H.

Définition 3.3

R_H ($_HR$) s'appelle la relation d'équivalence à gauche (à droite) suivant H.

Définition 3.3

R_H ($_HR$) s'appelle la relation d'équivalence à gauche (à droite) suivant H.
Les classes d'équivalence par rapport à R_H ($_HR$) s'appellent classes d'équivalence à gauche (à droite) suivant H.

Définition 3.3

R_H ($_HR$) s'appelle la relation d'équivalence à gauche (à droite) suivant H.
Les classes d'équivalence par rapport à R_H ($_HR$) s'appellent classes d'équivalence à gauche (à droite) suivant H.

La terminologie "à gauche","à droite" est justifiée par la :

Définition 3.3

R_H ($_HR$) s'appelle la relation d'équivalence à gauche (à droite) suivant H.
Les classes d'équivalence par rapport à R_H ($_HR$) s'appellent classes d'équivalence à gauche (à droite) suivant H.

La terminologie "à gauche","à droite" est justifiée par la :

Remarque 3.4

Soit $u \in G$. Alors

1. *$x\ R_H\ y$ si et seulement si $(ux)\ R_H\ (uy)$. Donc R_H est "compatible" à gauche avec la lci de G.*

Définition 3.3

R_H ($_HR$) s'appelle la relation d'équivalence à gauche (à droite) suivant H.
Les classes d'équivalence par rapport à R_H ($_HR$) s'appellent classes d'équivalence à gauche (à droite) suivant H.

La terminologie "à gauche","à droite" est justifiée par la :

Remarque 3.4

Soit $u \in G$. Alors

1. *$x\ R_H\ y$ si et seulement si $(ux)\ R_H\ (uy)$. Donc R_H est "compatible" à gauche avec la lci de G.*
2. *$x\ {}_HR\ y$ si et seulement si $(xu)\ {}_HR\ (yu)$. Donc ${}_HR$ est compatible à droite avec la lci de G.*

Rappel : Deux ensembles A, B *ont le même cardinal* s'il existe une bijection $f : A \to B$.

Rappel : Deux ensembles A, B *ont le même cardinal* s'il existe une bijection $f : A \to B$.

Proposition 3.5

Soit $x \in G$. Les applications $l_x : H \to xH$, $r_x : H \to Hx$ définies par

$$l_x(h) = xh, \ \ r_x(h) = hx$$

sont bijectives.

Rappel : Deux ensembles A, B *ont le même cardinal* s'il existe une bijection $f : A \to B$.

Proposition 3.5

Soit $x \in G$. Les applications $l_x : H \to xH$, $r_x : H \to Hx$ définies par

$$l_x(h) = xh, \ \ r_x(h) = hx$$

sont bijectives. En particulier toutes les classes d'équivalence à gauche (ou à droite) suivant H ont le même cardinal.

Rappel : Deux ensembles A, B *ont le même cardinal* s'il existe une bijection $f : A \to B$.

Proposition 3.5

Soit $x \in G$. Les applications $l_x : H \to xH$, $r_x : H \to Hx$ définies par

$$l_x(h) = xh, \ \ r_x(h) = hx$$

sont bijectives. En particulier toutes les classes d'équivalence à gauche (ou à droite) suivant H ont le même cardinal.

Dém: l_x injective : $l_x(h_1) = l_x(h_2) \Rightarrow xh_1 = xh_2 \Rightarrow h_1 = h_2$.
(On a multiplié les deux membres à gauche par x'.)

Rappel : Deux ensembles A, B *ont le même cardinal* s'il existe une bijection $f : A \to B$.

Proposition 3.5

Soit $x \in G$. Les applications $l_x : H \to xH$, $r_x : H \to Hx$ définies par

$$l_x(h) = xh, \ \ r_x(h) = hx$$

sont bijectives. En particulier toutes les classes d'équivalence à gauche (ou à droite) suivant H ont le même cardinal.

Dém: l_x injective : $l_x(h_1) = l_x(h_2) \Rightarrow xh_1 = xh_2 \Rightarrow h_1 = h_2$.
(On a multiplié les deux membres à gauche par x'.)

l_x surjective : Soit $y \in xH$. Par la définition de xH, il existe $h \in H$ tel que $y = xh = l_x(h)$.

Rappel : Deux ensembles A, B *ont le même cardinal* s'il existe une bijection $f : A \to B$.

Proposition 3.5

Soit $x \in G$. Les applications $l_x : H \to xH$, $r_x : H \to Hx$ définies par

$$l_x(h) = xh, \ \ r_x(h) = hx$$

sont bijectives. En particulier toutes les classes d'équivalence à gauche (ou à droite) suivant H ont le même cardinal.

Dém: l_x injective : $l_x(h_1) = l_x(h_2) \Rightarrow xh_1 = xh_2 \Rightarrow h_1 = h_2$.
(On a multiplié les deux membres à gauche par x'.)

l_x surjective : Soit $y \in xH$. Par la définition de xH, il existe $h \in H$ tel que $y = xh = l_x(h)$.

La bijectivité de r_x : exercice. ■

Notations utilisées dans la littérature :

$$G/H := G/R_H,\ H\backslash G := G/{}_H R\,.$$

Notations utilisées dans la littérature :

$$G/H := G/R_H,\ H\backslash G := G/{}_H R\,.$$

Remarque 3.6

Soit $H \subset G$ un sous-groupe. Les ensembles quotient G/R_H, $G/{}_H R$ ont le même cardinal.

Dém: L'application $\iota : G \to G$ donnée par $x \mapsto x^{-1}$ est une bijection, qui induit une bijection $\bar{\iota} : G/R_H \to G/{}_H R$ donnée explicitement par $\bar{\iota}(xH) = Hx^{-1}$.

Notations utilisées dans la littérature :

$$G/H := G/R_H,\ H\backslash G := G/{}_H R\,.$$

Remarque 3.6

Soit $H \subset G$ un sous-groupe. Les ensembles quotient G/R_H, $G/{}_H R$ ont le même cardinal.

Dém: L'application $\iota : G \to G$ donnée par $x \mapsto x^{-1}$ est une bijection, qui induit une bijection $\bar{\iota} : G/R_H \to G/{}_H R$ donnée explicitement par $\bar{\iota}(xH) = Hx^{-1}$.

Démontrer que $\bar{\iota}$ est bien définie et bijective. ■

Notations utilisées dans la littérature :

$$G/H := G/R_H,\ H\backslash G := G/{}_H R\,.$$

Remarque 3.6

Soit $H \subset G$ un sous-groupe. Les ensembles quotient G/R_H, $G/{}_H R$ ont le même cardinal.

Dém: L'application $\iota : G \to G$ donnée par $x \mapsto x^{-1}$ est une bijection, qui induit une bijection $\bar{\iota} : G/R_H \to G/{}_H R$ donnée explicitement par $\bar{\iota}(xH) = Hx^{-1}$.

Démontrer que $\bar{\iota}$ est bien définie et bijective. ■

La remarque ci-dessus est vraie en toute généralité, sans supposer que G, H, $|G/R_H|$, ou $|G/{}_H R|$ soit fini.

Définition 3.7

Soit $H \subset G$ un sous-groupe. Supposons que le quotient G/R_H (ou, de manière équivalente, $G/{}_HR$) est fini. L'indice de H dans G est défini par

$$|G : H| := |G/R_H| = |G/{}_HR|.$$

Définition 3.7

Soit $H \subset G$ un sous-groupe. Supposons que le quotient G/R_H (ou, de manière équivalente, $G/{}_HR$) est fini. L'indice de H dans G est défini par

$$|G : H| := |G/R_H| = |G/{}_HR|.$$

Théorème 3.8 (le théorème de Lagrange)

Soit $(G, \circ)$ un groupe fini, et soit $H \subset G$ un sous-groupe. Alors

$$|G| = |H| \cdot |G : H|.$$

On va utiliser un lemme élémentaire :

Lemme 3.9 (Le Lemme des bergers)

Soient $k, l \in \mathbb{N}^*$ et M un ensemble qui possède une partition en k sous-ensembles, chacun de cardinal l. Alors $|M| = kl$.

On va utiliser un lemme élémentaire :

Lemme 3.9 (Le Lemme des bergers)

Soient $k, l \in \mathbb{N}^*$ et M un ensemble qui possède une partition en k sous-ensembles, chacun de cardinal l. Alors $|M| = kl$.

Dém: (du théorème de Lagrange) On applique le lemme des bergers à la partition de G définie par les classes d'équivalence par rapport à R_H (ou à ${}_HR$).

On va utiliser un lemme élémentaire :

Lemme 3.9 (Le Lemme des bergers)

Soient $k, l \in \mathbb{N}^*$ et M un ensemble qui possède une partition en k sous-ensembles, chacun de cardinal l. Alors $|M| = kl$.

Dém: (du théorème de Lagrange) On applique le lemme des bergers à la partition de G définie par les classes d'équivalence par rapport à R_H (ou à ${}_HR$).

Nous savons que toutes ces classes ont le même cardinal qui coïncide avec $|H|$.

On va utiliser un lemme élémentaire :

Lemme 3.9 (Le Lemme des bergers)

Soient $k, l \in \mathbb{N}^*$ et M un ensemble qui possède une partition en k sous-ensembles, chacun de cardinal l. Alors $|M| = kl$.

Dém: (du théorème de Lagrange) On applique le lemme des bergers à la partition de G définie par les classes d'équivalence par rapport à R_H (ou à ${}_HR$).

Nous savons que toutes ces classes ont le même cardinal qui coïncide avec $|H|$.

Le nombre des classes d'équivalence par rapport à R_H est $|G/R_H|$. Mais $|G/R_H| = |G : H|$ par la définition de $|G : H|$. ■

Remarque 3.10

Le théorème de Lagrange est vrai même en toute généralité, même si G est infini. Pour cette généralisation on a besoin de la généralisation du produit pour les nombres cardinaux infinis.

Remarque 3.10

Le théorème de Lagrange est vrai même en toute généralité, même si G est infini. Pour cette généralisation on a besoin de la généralisation du produit pour les nombres cardinaux infinis.

Corollaire 3.11

Soit $(G, \circ)$ un groupe fini, $H \subset G$ un sous-groupe. Alors $|H|$ est un diviseur de $|G|$.

Remarque 3.10

Le théorème de Lagrange est vrai même en toute généralité, même si G est infini. Pour cette généralisation on a besoin de la généralisation du produit pour les nombres cardinaux infinis.

Corollaire 3.11

Soit $(G, \circ)$ un groupe fini, $H \subset G$ un sous-groupe. Alors $|H|$ est un diviseur de $|G|$.

Dans la littérature on appelle souvent ce corollaire " le théorème de Lagrange".

Corollaire 3.12

Soient $(G, \circ)$ un groupe fini et $x \in G$. Alors

1. $\mathrm{ord}(x)$ *est un diviseur de* $|G|$.

Corollaire 3.12

Soient $(G, \circ)$ un groupe fini et $x \in G$. Alors

1. $\mathrm{ord}(x)$ *est un diviseur de* $|G|$.
2. *Pour tout* $x \in G$ *on a* $x^{|G|} = e$.

Corollaire 3.12

Soient $(G, \circ)$ un groupe fini et $x \in G$. Alors

1. $\mathrm{ord}(x)$ *est un diviseur de* $|G|$.
2. *Pour tout* $x \in G$ *on a* $x^{|G|} = e$.

Dém: 1. On a $\mathrm{ord}(x) = |\langle x \rangle|$, donc $\mathrm{ord}(x)$ est un diviseur de $|G|$ d'après le corollaire 3.11.

Corollaire 3.12

Soient $(G, \circ)$ un groupe fini et $x \in G$. Alors

1. $\mathrm{ord}(x)$ *est un diviseur de* $|G|$.
2. *Pour tout* $x \in G$ *on a* $x^{|G|} = e$.

Dém: 1. On a $\mathrm{ord}(x) = |\langle x \rangle|$, donc $\mathrm{ord}(x)$ est un diviseur de $|G|$ d'après le corollaire 3.11.

2. Soit $k := \mathrm{ord}(x)$. Puisque $k||G|$ il existe $l \in \mathbb{N}$ tel que $|G| = kl$. Alors

$$x^{|G|} = x^{kl} = (x^k)^l = e^l = e.$$

■

Corollaire 3.13

Soit $(G, \circ)$ un groupe fini dont l'ordre $|G|$ est un nombre premier p. Alors G est un groupe cyclique d'ordre p, en particulier il est isomorphe à $(\mathbb{Z}_p, +)$.

Corollaire 3.13

Soit $(G, \circ)$ un groupe fini dont l'ordre $|G|$ est un nombre premier p. Alors G est un groupe cyclique d'ordre p, en particulier il est isomorphe à $(\mathbb{Z}_p, +)$.

Dém: Puisque $p \geqslant 2$ il existe $x \in G \backslash \{e\}$. On a $\mathrm{ord}(x) \geqslant 2$.

Corollaire 3.13

Soit $(G, \circ)$ un groupe fini dont l'ordre $|G|$ est un nombre premier p. Alors G est un groupe cyclique d'ordre p, en particulier il est isomorphe à $(\mathbb{Z}_p, +)$.

Dém: Puisque $p \geqslant 2$ il existe $x \in G \backslash \{e\}$. On a $\mathrm{ord}(x) \geqslant 2$.

D'après le corollaire 3.12 $\mathrm{ord}(x)|p$. Puisque p est un nombre premier, il en résulte $\mathrm{ord}(x) = p$, donc $|\langle x \rangle| = p = |G|$.

Corollaire 3.13

Soit $(G, \circ)$ un groupe fini dont l'ordre $|G|$ est un nombre premier p. Alors G est un groupe cyclique d'ordre p, en particulier il est isomorphe à $(\mathbb{Z}_p, +)$.

Dém: Puisque $p \geqslant 2$ il existe $x \in G \backslash \{e\}$. On a $\mathrm{ord}(x) \geqslant 2$.

D'après le corollaire 3.12 $\mathrm{ord}(x)|p$. Puisque p est un nombre premier, il en résulte $\mathrm{ord}(x) = p$, donc $|\langle x \rangle| = p = |G|$.

Puisque $\langle x \rangle$ est un sous-groupe de G, il en résulte $\langle x \rangle = G$.

Corollaire 3.13

Soit $(G, \circ)$ un groupe fini dont l'ordre $|G|$ est un nombre premier p. Alors G est un groupe cyclique d'ordre p, en particulier il est isomorphe à $(\mathbb{Z}_p, +)$.

Dém: Puisque $p \geqslant 2$ il existe $x \in G \backslash \{e\}$. On a $\mathrm{ord}(x) \geqslant 2$.

D'après le corollaire 3.12 $\mathrm{ord}(x)|p$. Puisque p est un nombre premier, il en résulte $\mathrm{ord}(x) = p$, donc $|\langle x \rangle| = p = |G|$.

Puisque $\langle x \rangle$ est un sous-groupe de G, il en résulte $\langle x \rangle = G$.

Donc G est un groupe cyclique d'ordre p. ■

Corollaire 3.14 (Le petit théorème de Fermat)

Si p est un nombre premier et $a \in \mathbb{Z}$ n'est pas divisible par p, alors

$$a^{p-1} \equiv 1 \ (mod)\ p\ .$$

Corollaire 3.14 (Le petit théorème de Fermat)

Si p est un nombre premier et $a \in \mathbb{Z}$ n'est pas divisible par p, alors

$$a^{p-1} \equiv 1 \ (mod)\ p\ .$$

Dém: Puisque a n'est pas divisible par p et p est premier, on $\mathrm{pgcd}(a, p) = 1$, donc $[a]_p \in \mathbb{Z}_p^{\times}$.

Corollaire 3.14 (Le petit théorème de Fermat)

Si p est un nombre premier et $a \in \mathbb{Z}$ n'est pas divisible par p, alors

$$a^{p-1} \equiv 1 \ (mod)\ p\ .$$

Dém: Puisque a n'est pas divisible par p et p est premier, on $\mathrm{pgcd}(a,p) = 1$, donc $[a]_p \in \mathbb{Z}_p^\times$.

Puisque p est un nombre premier, on a $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash \{[0]_p\}$, donc l'ordre du groupe $(\mathbb{Z}_p^\times, \cdot)$ est $p-1$.

Corollaire 3.14 (Le petit théorème de Fermat)

Si p est un nombre premier et $a \in \mathbb{Z}$ n'est pas divisible par p, alors

$$a^{p-1} \equiv 1 \ (mod)\ p\ .$$

Dém: Puisque a n'est pas divisible par p et p est premier, on $\mathrm{pgcd}(a,p) = 1$, donc $[a]_p \in \mathbb{Z}_p^\times$.

Puisque p est un nombre premier, on a $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash \{[0]_p\}$, donc l'ordre du groupe $(\mathbb{Z}_p^\times, \cdot)$ est $p-1$.

On applique le corollaire 3.12 au groupe $\mathbb{Z}_p^\times$ et à l'élément $[a]_p$ de ce groupe. ■

L'indicatrice d'Euler est l'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ définie par

$$\varphi(n) := |\mathbb{Z}_n^\times| = \left|\{k \in \{1, \ldots, n\},\ \mathrm{pgcd}(k, n) = 1\}\right| .$$

L'indicatrice d'Euler est l'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ définie par

$$\varphi(n) := |\mathbb{Z}_n^\times| = \left|\{k \in \{1, \ldots, n\},\ \operatorname{pgcd}(k, n) = 1\}\right| .$$

Corollaire 3.15 (le théorème de Euler)

Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ premier avec n. Alors

$$a^{\varphi(n)} \underset{n}{\equiv} 1 .$$

Dém: Exercice. Utiliser la même méthode que pour la démonstration du corollaire 3.14. Remarquer d'abord que $|\mathbb{Z}_n^\times| = \varphi(n)$. ■

On va voir : Si H est distingué, alors $R_H = {}_H R$ et le quotient $G/R_H = G/{}_H R$ a une structure naturelle de groupe.

On va voir : Si H est distingué, alors $R_H = {}_HR$ et le quotient $G/R_H = G/{}_HR$ a une structure naturelle de groupe.

Proposition 3.16

Soient $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe et R_H, ${}_HR$ les relations d'équivalence suivant H. Si H est distingué, alors

1. $R_H = {}_HR$,

On va voir : Si H est distingué, alors $R_H = {}_HR$ et le quotient $G/R_H = G/{}_HR$ a une structure naturelle de groupe.

Proposition 3.16

Soient $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe et R_H, ${}_HR$ les relations d'équivalence suivant H. Si H est distingué, alors

1. $R_H = {}_HR$,
2. *La formule $[x]_H \cdot [y]_H := [x \circ y]_H$ définit une structure de groupe sur le quotient $G/H := G/R_H = G/{}_HR$.*

On va voir : Si H est distingué, alors $R_H = {}_HR$ et le quotient $G/R_H = G/{}_HR$ a une structure naturelle de groupe.

Proposition 3.16

Soient $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe et R_H, ${}_HR$ les relations d'équivalence suivant H. Si H est distingué, alors

1. $R_H = {}_HR$,
2. *La formule $[x]_H \cdot [y]_H := [x \circ y]_H$ définit une structure de groupe sur le quotient $G/H := G/R_H = G/{}_HR$.*

Dém: 1. : On a $x\ R_H\ y \Rightarrow x'y \in H \Rightarrow \exists h \in H$ tel que $x'y = h$.

On va voir : Si H est distingué, alors $R_H = {}_HR$ et le quotient $G/R_H = G/{}_HR$ a une structure naturelle de groupe.

Proposition 3.16

Soient $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe et R_H, ${}_HR$ les relations d'équivalence suivant H. Si H est distingué, alors

1. $R_H = {}_HR$,
2. *La formule $[x]_H \cdot [y]_H := [x \circ y]_H$ définit une structure de groupe sur le quotient $G/H := G/R_H = G/{}_HR$.*

Dém: 1. : On a $x\ R_H\ y \Rightarrow x'y \in H \Rightarrow \exists h \in H$ tel que $x'y = h$.

Mais $x'y = h \Rightarrow y = xh \Rightarrow xy' = xh'x' \in H$ parce que $h' \in H$ et H est distingué. On a obtenu $xy' \in H$, donc $x\ {}_HR\ y$.

On va voir : Si H est distingué, alors $R_H = {}_HR$ et le quotient $G/R_H = G/{}_HR$ a une structure naturelle de groupe.

Proposition 3.16

Soient $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe et R_H, ${}_HR$ les relations d'équivalence suivant H. Si H est distingué, alors

1. $R_H = {}_HR$,
2. *La formule $[x]_H \cdot [y]_H := [x \circ y]_H$ définit une structure de groupe sur le quotient $G/H := G/R_H = G/{}_HR$.*

Dém: 1. : On a $x\ R_H\ y \Rightarrow x'y \in H \Rightarrow \exists h \in H$ tel que $x'y = h$.

Mais $x'y = h \Rightarrow y = xh \Rightarrow xy' = xh'x' \in H$ parce que $h' \in H$ et H est distingué. On a obtenu $xy' \in H$, donc $x\ {}_HR\ y$.

L'implication $x\ {}_HR\ y \Rightarrow x\ R_H\ y$ est proposée comme exercice.

2. À démontrer d'abord : la définition de $\cdot$ est cohérente, i.e. $[xy]_H$ dépend seulement des classes $[x]_H$, $[y]_H$.

2. À démontrer d'abord : la définition de $\cdot$ est cohérente, i.e. $[xy]_H$ dépend seulement des classes $[x]_H$, $[y]_H$.

Soient $\tilde{x}$, $\tilde{y} \in G$ tels que $\tilde{x}\ R_H\ x$ et $\tilde{y}\ R_H\ y$. On a donc $\tilde{x}'x \in H$, $\tilde{y}'y \in H$. Soient h, $\chi \in H$ tels que $\tilde{x}'x = h$, $\tilde{y}'y = \chi$. Alors

2. À démontrer d'abord : la définition de $\cdot$ est cohérente, i.e. $[xy]_H$ dépend seulement des classes $[x]_H$, $[y]_H$.

Soient $\tilde{x}$, $\tilde{y} \in G$ tels que $\tilde{x}\ R_H\ x$ et $\tilde{y}\ R_H\ y$. On a donc $\tilde{x}'x \in H$, $\tilde{y}'y \in H$. Soient h, $\chi \in H$ tels que $\tilde{x}'x = h$, $\tilde{y}'y = \chi$. Alors

$$(\tilde{x}\tilde{y})'(xy) = \tilde{y}'\tilde{x}'xy = (\chi y')(hx')(xy) = \chi(y'hy) \in H\ ,$$

parce que $\chi \in H$ et (H étant distingué) $y'hy \in H$.

2. À démontrer d'abord : la définition de $\cdot$ est cohérente, i.e. $[xy]_H$ dépend seulement des classes $[x]_H$, $[y]_H$.

Soient $\tilde{x}$, $\tilde{y} \in G$ tels que $\tilde{x}\ R_H\ x$ et $\tilde{y}\ R_H\ y$. On a donc $\tilde{x}'x \in H$, $\tilde{y}'y \in H$. Soient h, $\chi \in H$ tels que $\tilde{x}'x = h$, $\tilde{y}'y = \chi$. Alors

$$(\tilde{x}\tilde{y})'(xy) = \tilde{y}'\tilde{x}'xy = (\chi y')(hx')(xy) = \chi(y'hy) \in H\ ,$$

parce que $\chi \in H$ et (H étant distingué) $y'hy \in H$.

D'où $(\tilde{x}\tilde{y})\ R_H\ (xy)$, donc la classe $[x \circ y]_{R_H}$ dépend seulement des classes $[x]_H$, $[y]_H$.

2. À démontrer d'abord : la définition de $\cdot$ est cohérente, i.e. $[xy]_H$ dépend seulement des classes $[x]_H$, $[y]_H$.

Soient $\tilde{x}$, $\tilde{y} \in G$ tels que $\tilde{x}\ R_H\ x$ et $\tilde{y}\ R_H\ y$. On a donc $\tilde{x}'x \in H$, $\tilde{y}'y \in H$. Soient h, $\chi \in H$ tels que $\tilde{x}'x = h$, $\tilde{y}'y = \chi$. Alors

$$(\tilde{x}\tilde{y})'(xy) = \tilde{y}'\tilde{x}'xy = (\chi y')(hx')(xy) = \chi(y'hy) \in H\ ,$$

parce que $\chi \in H$ et (H étant distingué) $y'hy \in H$.

D'où $(\tilde{x}\tilde{y})\ R_H\ (xy)$, donc la classe $[x \circ y]_{R_H}$ dépend seulement des classes $[x]_H$, $[y]_H$.

Facile : la lci $\cdot$ sur G/R_H vérifie les axiomes du groupe :
– L'associativité de $\cdot$ résulte de l'associativité de $\circ$.
– La classe $[e]_H = H$ est élément neutre pour la lci $\cdot$.
– La classe $[x']_H$ est un élém. symétrique de $[x]_H$ par rapp. à $\cdot$ ■

Pour un sous-groupe distingué H la relation R_H s'appelle la relation d'équivalence (de congruence) suivant H. Aucune précision "à gauche" ou "à droite" n'est nécessaire.

Pour un sous-groupe distingué H la relation R_H s'appelle la relation d'équivalence (de congruence) suivant H. Aucune précision "à gauche" ou "à droite" n'est nécessaire. Si H est sous-entendu, on va noter $[x] := [x]_H$.

Pour un sous-groupe distingué H la relation R_H s'appelle la relation d'équivalence (de congruence) suivant H. Aucune précision "à gauche" ou "à droite" n'est nécessaire. Si H est sous-entendu, on va noter $[x] := [x]_H$.

Définition 3.17

Soit $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe distingué. Le groupe quotient de G par H est le groupe $(G/H, \cdot)$, où $G/H := G/R_H$ et $\cdot$ est la lci définie par

$$[x] \cdot [y] := [x \circ y].$$

Pour un sous-groupe distingué H la relation R_H s'appelle la relation d'équivalence (de congruence) suivant H. Aucune précision "à gauche" ou "à droite" n'est nécessaire. Si H est sous-entendu, on va noter $[x] := [x]_H$.

Définition 3.17

Soit $(G, \circ)$ un groupe, $H \subset G$ un sous-groupe distingué. Le groupe quotient de G par H est le groupe $(G/H, \cdot)$, où $G/H := G/R_H$ et $\cdot$ est la lci définie par

$$[x] \cdot [y] := [x \circ y].$$

L'épimorphisme canonique associé à H est l'épimorphisme $p_H : G \to G/H$ défini par $p_H(x) := [x]$.

Remarque 3.18

L'application p_H est un épimorphisme avec $\ker(p_H) = H$.

Dém: Exercice. ■

Remarque 3.18

L'application p_H est un épimorphisme avec $\ker(p_H) = H$.

Dém: Exercice. ■

Exemple 3.1

Dans un groupe abélien tout sous-groupe est distingué. En particulier $n\mathbb{Z}$ est un sous-groupe distingué de $\mathbb{Z}$.

Remarque 3.18

L'application p_H est un épimorphisme avec $\ker(p_H) = H$.

Dém: Exercice. ■

Exemple 3.1

Dans un groupe abélien tout sous-groupe est distingué. En particulier $n\mathbb{Z}$ est un sous-groupe distingué de $\mathbb{Z}$. Le groupe $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ est précisément le quotient de $\mathbb{Z}$ par $n\mathbb{Z}$ au sens de la théorie générale des groupes quotients.

Théorème 3.19 (Propriété universelle du groupe quotient)

Soient $H \subset G$ un sous-groupe distingué de G, $p_H : G \to G/H$ l'épimorphisme canonique et $f : G \to \tilde{G}$ un morphisme. Alors

Théorème 3.19 (Propriété universelle du groupe quotient)

Soient $H \subset G$ un sous-groupe distingué de G, $p_H : G \to G/H$ l'épimorphisme canonique et $f : G \to \tilde{G}$ un morphisme. Alors

1. *Il existe un morphisme $\bar{f} : G/H \to \tilde{G}$ tel que $\bar{f} \circ p_H = f$ si et seulement si $H \subset \ker(f)$.*

$$\begin{array}{ccc} G & \xrightarrow{f} & \tilde{G} \\ {\scriptstyle p_H}\downarrow & \nearrow_{\bar{f}} & \\ G/H & & \end{array} \qquad (2)$$

Théorème 3.19 (Propriété universelle du groupe quotient)

Soient $H \subset G$ un sous-groupe distingué de G, $p_H : G \to G/H$ l'épimorphisme canonique et $f : G \to \tilde{G}$ un morphisme. Alors

1. *Il existe un morphisme $\bar{f} : G/H \to \tilde{G}$ tel que $\bar{f} \circ p_H = f$ si et seulement si $H \subset \ker(f)$.*

$$\begin{array}{ccc} G & \xrightarrow{f} & \tilde{G} \\ {\scriptstyle p_H}\downarrow & \nearrow_{\bar{f}} & \\ G/H & & \end{array} \qquad (2)$$

2. *Si cette condition est vérifiée, alors*
   1. *$\bar{f}$ est unique, $\ker(\bar{f}) = \ker(f)/H$ et $\mathrm{im}(\bar{f}) = \mathrm{im}(f)$,*

Théorème 3.19 (Propriété universelle du groupe quotient)

Soient $H \subset G$ un sous-groupe distingué de G, $p_H : G \to G/H$ l'épimorphisme canonique et $f : G \to \tilde{G}$ un morphisme. Alors

1. *Il existe un morphisme $\bar{f} : G/H \to \tilde{G}$ tel que $\bar{f} \circ p_H = f$ si et seulement si $H \subset \ker(f)$.*

$$\begin{array}{ccc} G & \xrightarrow{f} & \tilde{G} \\ {\scriptstyle p_H}\downarrow & \nearrow_{\bar{f}} & \\ G/H & & \end{array} \qquad (2)$$

2. *Si cette condition est vérifiée, alors*
   1. *$\bar{f}$ est unique, $\ker(\bar{f}) = \ker(f)/H$ et $\operatorname{im}(\bar{f}) = \operatorname{im}(f)$,*
   2. *$\bar{f}$ est un monomorphisme si et seulement si $H = \ker(f)$,*

Théorème 3.19 (Propriété universelle du groupe quotient)

Soient $H \subset G$ un sous-groupe distingué de G, $p_H : G \to G/H$ l'épimorphisme canonique et $f : G \to \tilde{G}$ un morphisme. Alors

1. *Il existe un morphisme $\bar{f} : G/H \to \tilde{G}$ tel que $\bar{f} \circ p_H = f$ si et seulement si $H \subset \ker(f)$.*

$$\begin{array}{ccc} G & \xrightarrow{f} & \tilde{G} \\ {\scriptstyle p_H}\downarrow & \nearrow_{\bar{f}} & \\ G/H & & \end{array} \qquad (2)$$

2. *Si cette condition est vérifiée, alors*
   1. *$\bar{f}$ est unique, $\ker(\bar{f}) = \ker(f)/H$ et $\operatorname{im}(\bar{f}) = \operatorname{im}(f)$,*
   2. *$\bar{f}$ est un monomorphisme si et seulement si $H = \ker(f)$,*
   3. *$\bar{f}$ est un épimorphisme si et seulement si f est un épimorphisme.*

Dém: 1. Supposons : $\exists\ \bar{f} : G/H \to \tilde{G}$ morphisme tel que $\bar{f} \circ p_H = f$.

Dém: 1. Supposons : $\exists\ \bar{f} : G/H \to \tilde{G}$ morphisme tel que $\bar{f} \circ p_H = f$.

Il en résulte $H = \ker(p_H) \subset \ker(\bar{f} \circ p_H) = \ker(f)$.

Dém: 1. Supposons : $\exists\ \bar{f} : G/H \to \tilde{G}$ morphisme tel que $\bar{f} \circ p_H = f$.

Il en résulte $H = \ker(p_H) \subset \ker(\bar{f} \circ p_H) = \ker(f)$.

Réciproquement, si $H \subset \ker(f)$ alors f est compatible avec R_H, donc il existe une application $\bar{f} : G/H \to \tilde{G}$ avec la propriété $\bar{f} \circ p_H = f$.

Dém: 1. Supposons : $\exists\ \bar{f} : G/H \to \tilde{G}$ morphisme tel que $\bar{f} \circ p_H = f$.

Il en résulte $H = \ker(p_H) \subset \ker(\bar{f} \circ p_H) = \ker(f)$.

Réciproquement, si $H \subset \ker(f)$ alors f est compatible avec R_H, donc il existe une application $\bar{f} : G/H \to \tilde{G}$ avec la propriété $\bar{f} \circ p_H = f$. Cette application est un morphisme, parce que f est un morphisme.

Dém: 1. Supposons : $\exists\ \bar{f} : G/H \to \tilde{G}$ morphisme tel que $\bar{f} \circ p_H = f$.

Il en résulte $H = \ker(p_H) \subset \ker(\bar{f} \circ p_H) = \ker(f)$.

Réciproquement, si $H \subset \ker(f)$ alors f est compatible avec R_H, donc il existe une application $\bar{f} : G/H \to \tilde{G}$ avec la propriété $\bar{f} \circ p_H = f$. Cette application est un morphisme, parce que f est un morphisme.

2.(a) La condition $\bar{f} \circ p_H = f$ est équivalente à

$$\forall x \in G\ \bar{f}([x]) = f(x)\,,$$

donc pour $\bar{f}$ nous avons une seule possibilité.

Pour la 2me affirmation, soit $\tilde{e}$ l'élément neutre de $\tilde{G}$. H est un sous-groupe distingué de $\ker(f)$, donc le groupe quotient $\ker(f)/H$ est défini.

Pour la 2me affirmation, soit $\tilde{e}$ l'élément neutre de $\tilde{G}$. H est un sous-groupe distingué de $\ker(f)$, donc le groupe quotient $\ker(f)/H$ est défini.

On a

$$\ker(\bar{f}) = \left\{[x] \in G/H |\ \bar{f}([x]) = \tilde{e}\right\} = \{[x] \in G/H |\ f(x) = \tilde{e}\}$$

$$= \{[x] \in G/H |\ x \in \ker(f)\} = \ker(f)/H\ .$$

Pour la 2me affirmation, soit $\tilde{e}$ l'élément neutre de $\tilde{G}$. H est un sous-groupe distingué de $\ker(f)$, donc le groupe quotient $\ker(f)/H$ est défini.

On a

$$\ker(\bar{f}) = \left\{[x] \in G/H |\ \bar{f}([x]) = \tilde{e}\right\} = \{[x] \in G/H |\ f(x) = \tilde{e}\}$$

$$= \{[x] \in G/H |\ x \in \ker(f)\} = \ker(f)/H\ .$$

Pour la 3me affirmation : $\mathrm{im}(f) = \mathrm{im}(\bar{f} \circ p_H) = \mathrm{im}(\bar{f})$. Pour la 2me égalité on a utilisé la surjectivité de p_H.

Pour la 2me affirmation, soit $\tilde{e}$ l'élément neutre de $\tilde{G}$. H est un sous-groupe distingué de $\ker(f)$, donc le groupe quotient $\ker(f)/H$ est défini.

On a

$$\ker(\bar{f}) = \left\{[x] \in G/H |\ \bar{f}([x]) = \tilde{e}\right\} = \{[x] \in G/H |\ f(x) = \tilde{e}\}$$

$$= \{[x] \in G/H |\ x \in \ker(f)\} = \ker(f)/H\ .$$

Pour la 3me affirmation : $\mathrm{im}(f) = \mathrm{im}(\bar{f} \circ p_H) = \mathrm{im}(\bar{f})$. Pour la 2me égalité on a utilisé la surjectivité de p_H.

2.(b) $\bar{f}$ est un monomorphisme si et seulement si $\ker(\bar{f})$ est trivial, donc si et seulement si le quotient $\ker(f)/H$ est trivial, donc si et seulement si $\ker(f) = H$.

Pour la 2me affirmation, soit $\tilde{e}$ l'élément neutre de $\tilde{G}$. H est un sous-groupe distingué de $\ker(f)$, donc le groupe quotient $\ker(f)/H$ est défini.

On a

$$\ker(\bar{f}) = \left\{[x] \in G/H |\ \bar{f}([x]) = \tilde{e}\right\} = \{[x] \in G/H |\ f(x) = \tilde{e}\}$$

$$= \{[x] \in G/H |\ x \in \ker(f)\} = \ker(f)/H\ .$$

Pour la 3me affirmation : $\mathrm{im}(f) = \mathrm{im}(\bar{f} \circ p_H) = \mathrm{im}(\bar{f})$. Pour la 2me égalité on a utilisé la surjectivité de p_H.

2.(b) $\bar{f}$ est un monomorphisme si et seulement si $\ker(\bar{f})$ est trivial, donc si et seulement si le quotient $\ker(f)/H$ est trivial, donc si et seulement si $\ker(f) = H$.

2.(c) Utiliser la troisième affirmation de 2(a). ■

Exemple 3.2

Soient m, $n \in \mathbb{N}^*$ et $p : \mathbb{Z} \to \mathbb{Z}_m$, $q : \mathbb{Z} \to \mathbb{Z}_n$ les épimorphismes canoniques. Dans la propriété universelle on va prendre $G = \mathbb{Z}$, $H = m\mathbb{Z}$, $\tilde{G} = \mathbb{Z}_n$, $f = q$. Supposons $n|m$.

Exemple 3.2

Soient m, $n \in \mathbb{N}^*$ et $p : \mathbb{Z} \to \mathbb{Z}_m$, $q : \mathbb{Z} \to \mathbb{Z}_n$ les épimorphismes canoniques. Dans la propriété universelle on va prendre $G = \mathbb{Z}$, $H = m\mathbb{Z}$, $\tilde{G} = \mathbb{Z}_n$, $f = q$. Supposons $n|m$.

Alors $m\mathbb{Z} = \ker(p) \subset \ker(q) = n\mathbb{Z}$ et d'après le théorème il existe un unique morphisme $\bar{q} : \mathbb{Z}_m \to \mathbb{Z}_n$ tel que $\bar{q} \circ p = q$, i.e. tel que

$$\forall x \in \mathbb{Z},\ \bar{q}([x]_m) = [x]_n\,.$$

Exemple 3.2

Soient m, $n \in \mathbb{N}^*$ et $p : \mathbb{Z} \to \mathbb{Z}_m$, $q : \mathbb{Z} \to \mathbb{Z}_n$ les épimorphismes canoniques. Dans la propriété universelle on va prendre $G = \mathbb{Z}$, $H = m\mathbb{Z}$, $\tilde{G} = \mathbb{Z}_n$, $f = q$. Supposons $n|m$.

Alors $m\mathbb{Z} = \ker(p) \subset \ker(q) = n\mathbb{Z}$ et d'après le théorème il existe un unique morphisme $\bar{q} : \mathbb{Z}_m \to \mathbb{Z}_n$ tel que $\bar{q} \circ p = q$, i.e. tel que

$$\forall x \in \mathbb{Z},\ \bar{q}([x]_m) = [x]_n\,.$$

Le même théorème nous donne

$$\ker(\bar{q}) = \ker q/\ker p = n\mathbb{Z}/m\mathbb{Z}\,,$$

et $\bar{q}$ est un épimorphisme, parce que q est un épimorphisme.

Théorème 3.20 (Le premier théorème d'isomorphisme)

Soient $(G, \cdot)$, $(\tilde{G}, *)$ groupes et $f : G \to \tilde{G}$ un homomorphisme.

Théorème 3.20 (Le premier théorème d'isomorphisme)

Soient $(G, \cdot)$, $(\tilde{G}, *)$ groupes et $f : G \to \tilde{G}$ un homomorphisme. Alors la formule $\varphi([x]) := f(x)$ définit un isomorphisme

$$\varphi : G/\ker(f) \xrightarrow{\cong} \operatorname{im}(f) .$$

Théorème 3.20 (Le premier théorème d'isomorphisme)

Soient $(G, \cdot)$, $(\tilde{G}, *)$ groupes et $f : G \to \tilde{G}$ un homomorphisme. Alors la formule $\varphi([x]) := f(x)$ définit un isomorphisme

$$\varphi : G/\ker(f) \xrightarrow{\cong} \operatorname{im}(f) .$$

Dém: Dans la propriété universelle choisissons $H := \ker(f)$.

Théorème 3.20 (Le premier théorème d'isomorphisme)

Soient $(G,\cdot)$, $(\tilde{G},*)$ groupes et $f : G \to \tilde{G}$ un homomorphisme. Alors la formule $\varphi([x]) := f(x)$ définit un isomorphisme

$$\varphi : G/\ker(f) \xrightarrow{\simeq} \operatorname{im}(f)\,.$$

Dém: Dans la propriété universelle choisissons $H := \ker(f)$.

D'après la propriété universelle f définit un monomorphisme $\bar{f} : G/\ker(f) \to \tilde{G}$ qui a la même image que f.

Théorème 3.20 (Le premier théorème d'isomorphisme)

Soient $(G,\cdot)$, $(\tilde{G},*)$ groupes et $f : G \to \tilde{G}$ un homomorphisme. Alors la formule $\varphi([x]) := f(x)$ définit un isomorphisme

$$\varphi : G/\ker(f) \xrightarrow{\simeq} \operatorname{im}(f).$$

Dém: Dans la propriété universelle choisissons $H := \ker(f)$.

D'après la propriété universelle f définit un monomorphisme $\bar{f} : G/\ker(f) \to \tilde{G}$ qui a la même image que f.

Par restriction "au but" on obtient un isomorphisme $\varphi : G/\ker(f) \xrightarrow{\simeq} \operatorname{im}(f)$ avec la propriété requise. ■

Exemple 3.3

Soit $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ le morphisme défini par $f(t) = e^{2\pi i t}$. On a

$$\ker(f) = \mathbb{Z},\ \operatorname{im}(f) = \mathrm{U} := \{z \in \mathbb{C}^* |\ |z| = 1\},$$

donc, d'après le 1er théorème d'isomorphisme, f induit un isomorphisme $\varphi : \mathbb{R}/\mathbb{Z} \xrightarrow{\simeq} \mathrm{U}$.

Exemple 3.3

Soit $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ le morphisme défini par $f(t) = e^{2\pi it}$. On a

$$\ker(f) = \mathbb{Z},\ \mathrm{im}(f) = \mathrm{U} := \{z \in \mathbb{C}^* |\ |z| = 1\},$$

donc, d'après le 1er théorème d'isomorphisme, f induit un isomorphisme $\varphi : \mathbb{R}/\mathbb{Z} \xrightarrow{\simeq} \mathrm{U}$.

Exemple 3.4

Soit $f : (\mathbb{Z}, +) \to (\mathbb{R}^*, \cdot)$ le morphisme défini par $f(k) = (-1)^k$. On a

$$\ker(f) = 2\mathbb{Z},\ \mathrm{im}(f) = \{\pm 1\},$$

donc f induit un isomorphisme $\varphi : \mathbb{Z}/2\mathbb{Z} \xrightarrow{\simeq} \{\pm 1\}$.

Table of Contents

Rappel : Soit M un ensemble fini, $n := |M|$ son cardinal.

Rappel : Soit M un ensemble fini, $n := |M|$ son cardinal.
Une permutation de M est une bijection $M \to M$.

Rappel : Soit M un ensemble fini, $n := |M|$ son cardinal.
Une permutation de M est une bijection $M \to M$.
Le groupe symétrique de M : $(\mathfrak{S}(M), \circ)$, où

$$\mathfrak{S}(M) := \{f : M \to M | \ f \text{ bijective } \}.$$

Rappel : Soit M un ensemble fini, $n := |M|$ son cardinal.
Une permutation de M est une bijection $M \to M$.
Le groupe symétrique de M : $(\mathfrak{S}(M), \circ)$, où

$$\mathfrak{S}(M) := \{f : M \to M | \ f \text{ bijective } \}.$$

et $\circ$ désigne la composition des bijections. Pour $M = \{1, \ldots, n\}$ on obtient le groupe symétrique de degré n : $(\mathfrak{S}_n, \circ)$.

Rappel : Soit M un ensemble fini, $n := |M|$ son cardinal.
Une permutation de M est une bijection $M \to M$.
Le groupe symétrique de M : $(\mathfrak{S}(M), \circ)$, où

$$\mathfrak{S}(M) := \{f : M \to M |\ f \text{ bijective } \}.$$

et $\circ$ désigne la composition des bijections. Pour $M = \{1, \ldots, n\}$ on obtient le groupe symétrique de degré n : $(\mathfrak{S}_n, \circ)$.

Exercice 4.1

Soit $b : \{1, \ldots, n\} \to M$ bijection. L'application

$$\phi_b : \mathfrak{S}(M) \xrightarrow{\simeq} \mathfrak{S}_n,\ \phi_b(\sigma) := b^{-1} \circ \sigma \circ b$$

est un isomorphisme, donc $(\mathfrak{S}(M), \circ)$ est isomorphe à $(\mathfrak{S}_n, \circ)$.

Il en résulte :

1. On a $|\mathfrak{S}(M)| = n!$.

Il en résulte :

1. On a $|\mathfrak{S}(M)| = n!$.
2. $(\mathfrak{S}(M), \circ)$ est non-abélien si $n \geqslant 3$.

Il en résulte :

1. On a $|\mathfrak{S}(M)| = n!$.
2. $(\mathfrak{S}(M), \circ)$ est non-abélien si $n \geqslant 3$.

On va étudier le groupe $(\mathfrak{S}(M), \circ)$.

Il en résulte :

1. On a $|\mathfrak{S}(M)| = n!$.
2. $(\mathfrak{S}(M), \circ)$ est non-abélien si $n \geqslant 3$.

On va étudier le groupe $(\mathfrak{S}(M), \circ)$.

Un *arrangement* de k éléments dans M est une famille $(m_1, \ldots, m_k)$ d'éléments de M, distincts deux à deux.

Il en résulte :

1. On a $|\mathfrak{S}(M)| = n!$.
2. $(\mathfrak{S}(M), \circ)$ est non-abélien si $n \geqslant 3$.

On va étudier le groupe $(\mathfrak{S}(M), \circ)$.

Un *arrangement* de k éléments dans M est une famille $(m_1, \ldots, m_k)$ d'éléments de M, distincts deux à deux.

$\mathcal{A}^k(M) :=$ l'ensemble des arrangements de k éléments dans M.
Son cardinal est :

$$A_n^k := |\mathcal{A}^k(M)| = \frac{n!}{(n-k)!}.$$

Définition 4.1

Soit $\sigma \in \mathfrak{S}(M)$.

1. *Un élément $m \in M$ s'appelle point fixe de σ si $\sigma(m) = m$. L'ensemble des points fixes de σ sera noté M^σ.*

Définition 4.1

Soit $\sigma \in \mathfrak{S}(M)$.

1. *Un élément $m \in M$ s'appelle point fixe de σ si $\sigma(m) = m$. L'ensemble des points fixes de σ sera noté M^σ.*
2. *Le support de σ est le sous-ensemble*

$$\mathrm{supp}(\sigma) := \{m \in M |\ \sigma(m) \neq m\} \subset M\,.$$

Donc le support de σ est le complémentaire dans M du sous-ensemble M^σ des points fixes de σ.

Définition 4.1

Soit $\sigma \in \mathfrak{S}(M)$.

1. *Un élément $m \in M$ s'appelle point fixe de σ si $\sigma(m) = m$. L'ensemble des points fixes de σ sera noté M^σ.*
2. *Le support de σ est le sous-ensemble*

$$\mathrm{supp}(\sigma) := \{m \in M | \ \sigma(m) \neq m\} \subset M\,.$$

   Donc le support de σ est le complémentaire dans M du sous-ensemble M^σ des points fixes de σ.
3. *Un sous-ensemble $N \subset M$ est dit sous-ensemble invariant (partie invariante) par σ si $\sigma(N) = N$.*

Remarque 4.2

Soit M un ensemble fini et $\sigma \in \mathfrak{S}(M)$.

Remarque 4.2

Soit M un ensemble fini et $\sigma \in \mathfrak{S}(M)$.

1. *Si $N \subset M$ est une partie invariante par σ, alors la restriction de σ à N définit une permutation de N.*

Remarque 4.2

Soit M un ensemble fini et $\sigma \in \mathfrak{S}(M)$.

1. *Si $N \subset M$ est une partie invariante par σ, alors la restriction de σ à N définit une permutation de N.*
2. *M^σ et $\mathrm{supp}(\sigma)$ sont des parties invariantes par σ.*

Remarque 4.2

Soit M un ensemble fini et $\sigma \in \mathfrak{S}(M)$.

1. *Si $N \subset M$ est une partie invariante par σ, alors la restriction de σ à N définit une permutation de N.*
2. *M^σ et $\mathrm{supp}(\sigma)$ sont des parties invariantes par σ.*

Remarque 4.3

Si $\alpha, \beta \in \mathfrak{S}(M)$ sont deux permutations à supports disjoints, alors $\alpha \circ \beta = \beta \circ \alpha$. Donc deux permutations à supports disjoints commutent.

Remarque 4.2

Soit M un ensemble fini et $\sigma \in \mathfrak{S}(M)$.

1. *Si $N \subset M$ est une partie invariante par σ, alors la restriction de σ à N définit une permutation de N.*
2. *M^σ et $\mathrm{supp}(\sigma)$ sont des parties invariantes par σ.*

Remarque 4.3

Si $\alpha, \beta \in \mathfrak{S}(M)$ sont deux permutations à supports disjoints, alors $\alpha \circ \beta = \beta \circ \alpha$. Donc deux permutations à supports disjoints commutent.

Dém: Soit $x \in M$. Discussion selon plusieurs cas. Par exemple si $x \in \mathrm{supp}(\alpha)$, alors $x \notin \mathrm{supp}(\beta)$ et $(\alpha \circ \beta)(x) = (\beta \circ \alpha)(x) = \alpha(x)$.

■

Définition 4.4

Soit $k \in \mathbb{N}^*$, $2 \leqslant k \leqslant n$. Une permutation $\alpha \in \mathfrak{S}(M)$ s'appelle cycle de longueur k, ou k-cycle, s'il existe un arrangement $(m_1, m_2 \ldots, m_{k-1}, m_k)$ de k éléments dans M tel que

$$\alpha(m_1) = m_2, \ \ldots, \ \alpha(m_{k-1}) = m_k, \ \alpha(m_k) = m_1, \ \text{et}$$

$$\alpha(m) = m \ \text{pour} \ m \notin \{m_1, \ldots, m_k\}.$$

Si c'est le cas, on va écrire $\alpha = (m_1 m_2 \ldots m_k)$. Un 2-cycle s'appelle transposition. Un n-cycle s'appelle permutation circulaire de M.

Remarque 4.5

1. *Soit* $\alpha = (m_1 m_2 \dots m_{k-1} m_k)$ *un* k*-cycle. Alors* $\alpha^{-1} = (m_k m_{k-1} \dots m_2 m_1)$.

Remarque 4.5

1. *Soit* $\alpha = (m_1 m_2 \dots m_{k-1} m_k)$ *un* k*-cycle. Alors* $\alpha^{-1} = (m_k m_{k-1} \dots m_2 m_1)$.
2. *Si* α *est un* k*-cycle alors* $\mathrm{ord}(\alpha) = k$.

Remarque 4.5

1. *Soit* $\alpha = (m_1 m_2 \dots m_{k-1} m_k)$ *un* k*-cycle. Alors* $\alpha^{-1} = (m_k m_{k-1} \dots m_2 m_1)$.
2. *Si* α *est un* k*-cycle alors* $\mathrm{ord}(\alpha) = k$.
3. *La correspondance entre arrangements de* k *éléments et* k*-cycles de* M *n'est pas bijective. On a évidemment*

$$(m_1 m_2 \dots m_{k-1} m_k) = (m_2 m_3 \dots m_k m_1) \cdots = (m_k m_1 \dots m_{k-2} m_{k-1})$$

donc à chaque k*-cycle correspondent* k *arrangements.*

Remarque 4.5

1. *Soit* $\alpha = (m_1 m_2 \dots m_{k-1} m_k)$ *un k-cycle. Alors* $\alpha^{-1} = (m_k m_{k-1} \dots m_2 m_1)$.
2. *Si* α *est un k-cycle alors* $\mathrm{ord}(\alpha) = k$.
3. *La correspondance entre arrangements de k éléments et k-cycles de M n'est pas bijective. On a évidemment*

$$(m_1 m_2 \dots m_{k-1} m_k) = (m_2 m_3 \dots m_k m_1) \cdots = (m_k m_1 \dots m_{k-2} m_{k-1})$$

donc à chaque k-cycle correspondent k arrangements.

4. *Le nombre de k-cycles dans* $\mathfrak{S}(M)$ *est* $\frac{1}{k} A_n^k = (k-1)! C_n^k$, *en particulier*

dans $\mathfrak{S}(M)$ il y a $C_n^2 = \frac{n(n-1)}{2}$ transpositions et $(n-1)!$ permutations circulaires.

dans $\mathfrak{S}(M)$ il y a $C_n^2 = \frac{n(n-1)}{2}$ transpositions et $(n-1)!$ permutations circulaires.

5. Un k-cycle (avec $k \geqslant 2$) s'écrit comme produit de $(k-1)$ transpositions. En effet on a

$$(m_1 m_2 \dots m_{k-1} m_k) = (m_1 m_k)(m_1 m_{k-1}) \dots (m_1 m_3)(m_1 m_2)\,.$$

dans $\mathfrak{S}(M)$ il y a $C_n^2 = \frac{n(n-1)}{2}$ transpositions et $(n-1)!$ permutations circulaires.

5. Un k-cycle (avec $k \geqslant 2$) s'écrit comme produit de $(k-1)$ transpositions. En effet on a

$$(m_1 m_2 \dots m_{k-1} m_k) = (m_1 m_k)(m_1 m_{k-1}) \dots (m_1 m_3)(m_1 m_2)\,.$$

6. Si $n = 3$ alors $\mathfrak{S}(M)$ contient : id_M, trois 2-cycles et deux 3-cycles.

dans $\mathfrak{S}(M)$ il y a $C_n^2 = \frac{n(n-1)}{2}$ transpositions et $(n-1)!$ permutations circulaires.

5. Un k-cycle (avec $k \geqslant 2$) s'écrit comme produit de $(k-1)$ transpositions. En effet on a

$$(m_1 m_2 \dots m_{k-1} m_k) = (m_1 m_k)(m_1 m_{k-1}) \dots (m_1 m_3)(m_1 m_2)\,.$$

6. Si $n = 3$ alors $\mathfrak{S}(M)$ contient : id_M, trois 2-cycles et deux 3-cycles.
Si $n = 4$: $\mathfrak{S}(M)$ contient : id_M, six 2-cycles, huit 3-cycles et six 4-cycles.

dans $\mathfrak{S}(M)$ il y a $C_n^2 = \frac{n(n-1)}{2}$ transpositions et $(n-1)!$ permutations circulaires.

5. Un k-cycle (avec $k \geqslant 2$) s'écrit comme produit de $(k-1)$ transpositions. En effet on a

$$(m_1 m_2 \dots m_{k-1} m_k) = (m_1 m_k)(m_1 m_{k-1}) \dots (m_1 m_3)(m_1 m_2)\,.$$

6. Si $n = 3$ alors $\mathfrak{S}(M)$ contient : id_M, trois 2-cycles et deux 3-cycles.
Si $n = 4$: $\mathfrak{S}(M)$ contient : id_M, six 2-cycles, huit 3-cycles et six 4-cycles.
Mais $|\mathfrak{S}(M)| = 24$, donc $\mathfrak{S}(M)\backslash\{\mathrm{id}_M\}$ contient trois permutations qui ne sont pas des cycles.

Remarque 4.6

Le support d'un cycle $\alpha = (m_1 m_2 \dots m_k)$ *est* $\{m_1, m_2, \dots, m_k\}$.

Remarque 4.6

Le support d'un cycle $\alpha = (m_1 m_2 \dots m_k)$ est $\{m_1, m_2, \dots, m_k\}$. La restriction de α à ce sous-ensemble est une permutation circulaire.

Remarque 4.6

Le support d'un cycle $\alpha = (m_1 m_2 \dots m_k)$ est $\{m_1, m_2, \dots, m_k\}$.
La restriction de α à ce sous-ensemble est une permutation circulaire.
La donnée d'un k-cycle dans $\mathfrak{S}(M)$ est équivalente à la donnée d'un sous-ensemble $N \subset M$ de cardinal k et d'une permutation circulaire de N.

Remarque 4.6

Le support d'un cycle $\alpha = (m_1 m_2 \dots m_k)$ est $\{m_1, m_2, \dots, m_k\}$.
La restriction de α à ce sous-ensemble est une permutation circulaire.
La donnée d'un k-cycle dans $\mathfrak{S}(M)$ est équivalente à la donnée d'un sous-ensemble $N \subset M$ de cardinal k et d'une permutation circulaire de N.

Définition 4.7

Soient $\alpha = (m_1 m_2 \dots m_{k-1} m_k)$, $\beta = (p_1 p_2 \dots p_{l-1} p_l) \in \mathfrak{S}(M)$ deux cycles. On dit que α, β sont des cycles disjoints si leur supports sont disjoints, donc si

$$\{m_1, m_2, \dots, m_{k-1}, m_k\} \cap \{p_1, p_2, \dots p_{l-1}, p_l\} = \varnothing.$$

Proposition 4.8

Soient $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathfrak{S}(M)$ des cycles disjoints deux à deux et soit $\sigma = \alpha_1\alpha_2 \ldots \alpha_s$ leur produit.

Proposition 4.8

Soient $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathfrak{S}(M)$ des cycles disjoints deux à deux et soit $\sigma = \alpha_1\alpha_2 \ldots \alpha_s$ leur produit. Alors

1. *On a*

$$\mathrm{supp}(\sigma) = \bigcup_{j=1}^{s} \mathrm{supp}(\alpha_i),$$

et les sous-ensembles $\mathrm{supp}(\alpha_i)$ $(1 \leqslant i \leqslant s)$ donnent une partition de $\mathrm{supp}(\sigma)$ en parties invariantes par σ.

Proposition 4.8

Soient $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathfrak{S}(M)$ des cycles disjoints deux à deux et soit $\sigma = \alpha_1\alpha_2 \ldots \alpha_s$ leur produit. Alors

1. *On a*
$$\mathrm{supp}(\sigma) = \bigcup_{j=1}^{s} \mathrm{supp}(\alpha_i),$$
et les sous-ensembles $\mathrm{supp}(\alpha_i)$ $(1 \leqslant i \leqslant s)$ donnent une partition de $\mathrm{supp}(\sigma)$ en parties invariantes par σ.
2. *Soit k_i la longueur de α_i. Alors $\mathrm{ord}(\sigma) = \mathrm{ppcm}(k_1, \ldots, k_s)$.*

Proposition 4.8

Soient $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathfrak{S}(M)$ des cycles disjoints deux à deux et soit $\sigma = \alpha_1\alpha_2 \ldots \alpha_s$ leur produit. Alors

1. *On a*
$$\mathrm{supp}(\sigma) = \bigcup_{j=1}^{s} \mathrm{supp}(\alpha_i),$$
et les sous-ensembles $\mathrm{supp}(\alpha_i)$ $(1 \leqslant i \leqslant s)$ donnent une partition de $\mathrm{supp}(\sigma)$ en parties invariantes par σ.
2. *Soit k_i la longueur de α_i. Alors $\mathrm{ord}(\sigma) = \mathrm{ppcm}(k_1, \ldots, k_s)$.*

Dém: (1) : Exercice.

Proposition 4.8

Soient $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathfrak{S}(M)$ des cycles disjoints deux à deux et soit $\sigma = \alpha_1\alpha_2 \ldots \alpha_s$ leur produit. Alors

1. *On a*
$$\mathrm{supp}(\sigma) = \bigcup_{j=1}^{s} \mathrm{supp}(\alpha_i),$$
et les sous-ensembles $\mathrm{supp}(\alpha_i)$ $(1 \leqslant i \leqslant s)$ donnent une partition de $\mathrm{supp}(\sigma)$ en parties invariantes par σ.
2. *Soit k_i la longueur de α_i. Alors $\mathrm{ord}(\sigma) = \mathrm{ppcm}(k_1, \ldots, k_s)$.*

Dém: (1) : Exercice.
(2) : Soient $M_i := \mathrm{supp}(\alpha_i)$, a_i la permutation circulaire définie par α_i sur M_i.

Puisque les α_i commutent, on a $\sigma^l = \alpha_1^l \alpha_2^l \dots \alpha_s^l$.

Puisque les α_i commutent, on a $\sigma^l = \alpha_1^l \alpha_2^l \dots \alpha_s^l$.

La permutation de M_i induite par σ^l est a_i^l.

Puisque les α_i commutent, on a $\sigma^l = \alpha_1^l \alpha_2^l \dots \alpha_s^l$.

La permutation de M_i induite par σ^l est a_i^l.

Il en résulte : $\sigma^l = \mathrm{id}_M \Leftrightarrow a_i^l = \mathrm{id}_{M_i}$ pour $1 \leqslant i \leqslant s$.

Puisque les α_i commutent, on a $\sigma^l = \alpha_1^l \alpha_2^l \dots \alpha_s^l$.

La permutation de M_i induite par σ^l est a_i^l.

Il en résulte : $\sigma^l = \mathrm{id}_M \Leftrightarrow a_i^l = \mathrm{id}_{M_i}$ pour $1 \leqslant i \leqslant s$.

Mais $\mathrm{ord}(a_i) = k_i$, donc

$$\sigma^l = \mathrm{id}_M \Leftrightarrow k_i \mid l \text{ pour } 1 \leqslant i \leqslant s \Leftrightarrow \mathrm{ppcm}(k_1, \dots, k_s) \mid l. \qquad \blacksquare$$

Puisque les α_i commutent, on a $\sigma^l = \alpha_1^l \alpha_2^l \dots \alpha_s^l$.

La permutation de M_i induite par σ^l est a_i^l.

Il en résulte : $\sigma^l = \mathrm{id}_M \Leftrightarrow a_i^l = \mathrm{id}_{M_i}$ pour $1 \leqslant i \leqslant s$.

Mais $\mathrm{ord}(a_i) = k_i$, donc

$$\sigma^l = \mathrm{id}_M \Leftrightarrow k_i \mid l \text{ pour } 1 \leqslant i \leqslant s \Leftrightarrow \mathrm{ppcm}(k_1, \dots, k_s) \mid l. \qquad \blacksquare$$

Théorème 4.9 (décomposition en produit de cycles disjoints)

Toute permutation $\sigma \in \mathfrak{S}(M) \backslash \{\mathrm{id}_M\}$ s'écrit comme produit de cycles disjoints deux à deux. Cette décomposition est unique à ordre près.

Dém: Récurrence par rapport à $n = |M|$. Voir le poly du cours. $\blacksquare$

Remarque 4.10

La démonstration du théorème nous donne un algorithme explicite qui fournit une décomposition en cycles d'une permutation donnée.

Remarque 4.10

La démonstration du théorème nous donne un algorithme explicite qui fournit une décomposition en cycles d'une permutation donnée.

Exemple 4.1

Trouver une décomposition en produit de cycles disjoints de la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_6$.

Remarque 4.10

La démonstration du théorème nous donne un algorithme explicite qui fournit une décomposition en cycles d'une permutation donnée.

Exemple 4.1

Trouver une décomposition en produit de cycles disjoints de la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_6$.

Corollaire 4.11

Toute permutation $\sigma \in \mathfrak{S}(M)$ s'écrit comme produit de transpositions.

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

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

Par exemple : $(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 1)(2\ 3) = (2\ 3)(1\ 3)$.

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

Par exemple : $(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 1)(2\ 3) = (2\ 3)(1\ 3)$.
Même le nombre des facteurs n'est pas unique.

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

Par exemple : $(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 1)(2\ 3) = (2\ 3)(1\ 3)$.
Même le nombre des facteurs n'est pas unique.

Définition 4.12

Soit $\sigma \in \mathfrak{S}_n$. Une inversion pour σ est un couple $(i,j) \in \{1,\ldots,n\}^2$ tel que $i < j$ et $\sigma(i) > \sigma(j)$.

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

Par exemple : $(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 1)(2\ 3) = (2\ 3)(1\ 3)$.
Même le nombre des facteurs n'est pas unique.

Définition 4.12

Soit $\sigma \in \mathfrak{S}_n$. Une inversion pour σ est un couple $(i,j) \in \{1,\ldots,n\}^2$ tel que $i < j$ et $\sigma(i) > \sigma(j)$.
Le nombre d'inversions pour σ est désigné par $\iota(\sigma)$. La signature de σ est définie par $\varepsilon(\sigma) := (-1)^{\iota(\sigma)} \in \{-1,1\}$.

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

Par exemple : $(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 1)(2\ 3) = (2\ 3)(1\ 3)$.
Même le nombre des facteurs n'est pas unique.

Définition 4.12

Soit $\sigma \in \mathfrak{S}_n$. Une inversion pour σ est un couple $(i,j) \in \{1,\dots,n\}^2$ tel que $i < j$ et $\sigma(i) > \sigma(j)$.
Le nombre d'inversions pour σ est désigné par $\iota(\sigma)$. La signature de σ est définie par $\varepsilon(\sigma) := (-1)^{\iota(\sigma)} \in \{-1,1\}$.

Exercice 4.2

Démontrer :

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma_j - \sigma_i}{j - i}\,.$$

Lemme 4.13

Soit τ une transposition. Alors $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

Lemme 4.13

Soit τ une transposition. Alors $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

Dém: Exercice. Étudier le cas particulier $\tau = (1\,2)$. ■

Lemme 4.13

Soit τ une transposition. Alors $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

Dém: Exercice. Étudier le cas particulier $\tau = (1\,2)$. ■

Proposition 4.14

Soit $\sigma \in \mathfrak{S}_n$ et $\sigma = \tau_1 \dots \tau_p$ une décomposition de σ en produit de transpositions. Alors $\varepsilon(\sigma) = (-1)^p$.

Lemme 4.13

Soit τ une transposition. Alors $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

Dém: Exercice. Étudier le cas particulier $\tau = (1\,2)$. ■

Proposition 4.14

Soit $\sigma \in \mathfrak{S}_n$ et $\sigma = \tau_1 \dots \tau_p$ une décomposition de σ en produit de transpositions. Alors $\varepsilon(\sigma) = (-1)^p$.

Donc la parité du nombre de facteurs dans une décomposition de σ en produit de transpositions dépend seulement de σ.

Lemme 4.13

Soit τ une transposition. Alors $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

Dém: Exercice. Étudier le cas particulier $\tau = (1\,2)$. ■

Proposition 4.14

Soit $\sigma \in \mathfrak{S}_n$ et $\sigma = \tau_1 \dots \tau_p$ une décomposition de σ en produit de transpositions. Alors $\varepsilon(\sigma) = (-1)^p$.

Donc la parité du nombre de facteurs dans une décomposition de σ en produit de transpositions dépend seulement de σ.

Cette proposition suggère une définition équivalente de la signature. Cette définition équivalente s'applique dans la cadre plus général des permutations d'un ensemble fini M.

Exemple 4.2

Soit $\alpha \in \mathfrak{S}_n$ un k-cycle. Alors $\varepsilon(\alpha) = (-1)^{k-1}$.

Exemple 4.2

Soit $\alpha \in \mathfrak{S}_n$ un k-cycle. Alors $\varepsilon(\alpha) = (-1)^{k-1}$.

Proposition 4.15

Munissons l'ensemble $\{-1, +1\}$ de la structure de groupe définie par la multiplication. L'application $\varepsilon : \mathfrak{S}_n \to \{-1, +1\}$ donnée par $\sigma \mapsto \varepsilon(\sigma)$ est un morphisme de groupes.

Exemple 4.2

Soit $\alpha \in \mathfrak{S}_n$ un k-cycle. Alors $\varepsilon(\alpha) = (-1)^{k-1}$.

Proposition 4.15

Munissons l'ensemble $\{-1, +1\}$ de la structure de groupe définie par la multiplication. L'application $\varepsilon : \mathfrak{S}_n \to \{-1, +1\}$ donnée par $\sigma \mapsto \varepsilon(\sigma)$ est un morphisme de groupes. Cet morphisme est un épimorphisme pour $n \geqslant 2$.

Dém: Exercice. Utiliser la proposition 4.14. Pour démontrer la surjectivité de ε, il suffit de remarquer que $\varepsilon(\tau) = -1$ pour toute transposition $\tau \in \mathfrak{S}_n$. ■

Pour $n \geqslant 2$ le noyau $\ker(\varepsilon)$ est un sous-groupe distingué de $\mathfrak{S}_n$, qui s'appelle le groupe alterné de degré n et est noté A_n.

Pour $n \geqslant 2$ le noyau $\ker(\varepsilon)$ est un sous-groupe distingué de $\mathfrak{S}_n$, qui s'appelle le groupe alterné de degré n et est noté A_n.

L'ordre de ce groupe est $\frac{n!}{2}$. En effet, d'après le théorème de Lagrange on a

$$n! = |A_n|[\mathfrak{S}_n : A_n].$$

Pour $n \geqslant 2$ le noyau $\ker(\varepsilon)$ est un sous-groupe distingué de $\mathfrak{S}_n$, qui s'appelle le groupe alterné de degré n et est noté A_n.

L'ordre de ce groupe est $\frac{n!}{2}$. En effet, d'après le théorème de Lagrange on a

$$n! = |A_n|[\mathfrak{S}_n : A_n].$$

Puisque A_n est un sous-groupe normal, l'indice $[\mathfrak{S}_n : A_n]$ s'identifie à l'ordre $|\mathfrak{S}_n/A_n|$ du groupe quotient $\mathfrak{S}_n/A_n$.

Pour $n \geqslant 2$ le noyau $\ker(\varepsilon)$ est un sous-groupe distingué de $\mathfrak{S}_n$, qui s'appelle le groupe alterné de degré n et est noté A_n.

L'ordre de ce groupe est $\frac{n!}{2}$. En effet, d'après le théorème de Lagrange on a

$$n! = |A_n|[\mathfrak{S}_n : A_n].$$

Puisque A_n est un sous-groupe normal, l'indice $[\mathfrak{S}_n : A_n]$ s'identifie à l'ordre $|\mathfrak{S}_n/A_n|$ du groupe quotient $\mathfrak{S}_n/A_n$.

Mais d'après le 1-er théorème d'isomorphisme on a un isomorphisme $\mathfrak{S}_n/A_n \simeq \varepsilon(\mathfrak{S}_n) = \{-1, 1\}$. Donc $[\mathfrak{S}_n : A_n] = 2$.