

MAT141 - Éléments d'algèbre
Donné par Jean-Philippe Burelle

Julien Houle

Automne 2025

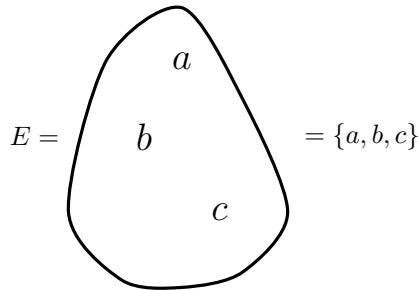
Table des matières

1	Ensembles	1
	Manières de définir une fonction	1
6	Groupes	8
	Propriétés élémentaires des groupes	9
	Produit cartésien de groupes	10
	Isomorphismes de groupes	11
	Puissances d'éléments de groupes	13
	Sous-groupes	16
2	Applications et équivalences	19
	2.4 Relations d'équivalence	19
	Ordre et groupes cycliques	22
6	Groupes (suite)	24
	6.13 Groupes symétriques S_n	24
8	Homomorphismes	29
	Équivalence modulo H et théorème de Lagrange	32
	8.6 Groupes quotients	34

Chapitre 1 Ensembles

Cours 1

Idée : ensemble = patate.



Notation. $E \subseteq F \Leftrightarrow \forall x \in E, x \in F$.

Remarque. $E \subseteq E$.

Notation. La cardinalité d'un ensemble, $|E|$, est le nombre d'éléments d'un ensemble.

Définition. Définition d'un ensemble par *compréhension*

Exemple. $E = \{n \in \mathbb{Z} | 1 \leq n \leq 20\}$.

Notation. $E = F \Leftrightarrow E \subseteq F$ et $F \subseteq E$.

Définition. Produit cartésien : $E \times F = \{(x, y) | x \in E, y \in F\}$.

Définition. Fonction/Application

$f : A \rightarrow B$, A et B des ensembles, associe à *chaque* $x \in A$ un *unique* élément $f(x) \in B$.

Cours 2

Rappel.

- Ensemble collection d'objets
- \in “élément” d'un ensemble
- sous-ensemble (\subseteq) $E \subseteq F$ si $x \in E$ implique $x \in F$
- $E = F$ si, et seulement si, $E \subseteq F$ et $F \subseteq E$
- \cup union
- \cap intersection
- $E \times F$ produit cartésien (paires (x, y))
- $f : E \rightarrow F$ fonction ou application, associe à chaque $x \in E$ un unique $f(x) \in F$, image de x par f
- $\mathbf{1}_E$: $E \rightarrow E$ est définie comme $\mathbf{1}_E(x) = x$

Manières de définir une fonction

- énumérer $f(x)$ pour chaque $x \in E$
- donner une formule
une formule ne définit pas toujours une fonction, elle doit être valide pour chaque x de l'ensemble de départ.
- en mots (décrire la valeur pour chaque $x \in E$)

- mélange de formule et mots

Définition. Une fonction $f : E \rightarrow F$ est *inversible* s'il existe une fonction $\underbrace{g : F \rightarrow E}_{*}$ telle que $\underbrace{g(f(x)) = x}_{**}$ pour tout $x \in E$ et $\underbrace{f(g(y)) = y}_{***}$ pour tout $y \in F$.

Exemple. $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x + 1$ est inversible d'inverse $g(y) = y - 1$

Démonstration.

On vérifie que

$$\begin{array}{ll} g(f(x)) = x & g(f(x)) = g(x + 1) \\ & = (x + 1) - 1 \\ & = x \\ f(g(y)) = y & f(g(y)) = f(y - 1) \\ & = (y - 1) + 1 \\ & = y \end{array}$$

□

Proposition. Si f admet un inverse, celui-ci est unique.

Démonstration.

Supposons que g_1 et g_2 sont tous deux inverses de f et montrons qu'elles sont égales.

(Pour démontrer que deux fonctions sont égales, il suffit de montrer que $g_1(y) = g_2(y)$ pour tout $y \in F$)

Soit $y \in F$.

On a

$$\begin{aligned} g_1(y) &\stackrel{***}{=} g_1(\underbrace{f(g_2(y))}_{*}) \\ &\stackrel{**}{=} g_2(y) \end{aligned}$$

□

Définition. Si $f : E \rightarrow F$ et $g : F \rightarrow G$, alors la *composée* de f et g est la fonction $g \circ f : E \rightarrow G$ définie par la formule $g \circ f(x) = g(f(x))$.

Définition (Redéfinition de l'inverse).

$$\begin{aligned} g \circ f &= \mathbf{1}_E \\ f \circ g &= \mathbf{1}_F \end{aligned}$$

Exemple.

$$A = \{a, b, c\}$$

$$B = \{d, e, f\}$$

$$f : A \rightarrow B, a \mapsto d, b \mapsto e, c \mapsto f$$

$$g : B \rightarrow A, d \mapsto a, e \mapsto b, f \mapsto c$$

$$g \circ f : A \rightarrow A, g \circ f(x) = x, g \circ f = \mathbf{1}_A.$$

De la même manière, $f \circ g = \mathbf{1}_B$.

Ainsi, g est l'inverse de f .

Notation. On note $g = f^{-1}$ l'inverse de f .

Rappel. Pour trouver l'inverse d'une fonction $f : \mathbb{R} \rightarrow \mathbb{R}$ donnée par une formule $f(x) = y$, on isole x en fonction de y .

Exemple.

$$\begin{aligned} f(x) &= 3x - 8 \\ y &= 3x - 8 \\ y + 8 &= 3x \\ \frac{y + 8}{3} &= x \\ g(y) &= \frac{y + 8}{3} \end{aligned}$$

Dans un devoir, on commence par la formule de l'inverse et on vérifie $g(f(x)) = x$ et $f(g(y)) = y$.

Définition. On dit que $f : E \rightarrow F$ est une fonction *injective* si $f(x_1) = f(x_2)$ implique $x_1 = x_2$.

Définition. On dit que $f : E \rightarrow F$ est une fonction *surjective* si pour tout $y \in F$, $\exists x \in E$ t.q. $f(x) = y$.

Définition. On dit que $f : E \rightarrow F$ est une fonction *bijective* si elle est injective **et** surjective.

Exemple.

•

$$f : \mathbb{R} \rightarrow \mathbb{R}^{\geq 0}, f(x) = |x|$$

f n'est pas injective, car $f(1) = |1| = 1$ et $f(-1) = |-1| = 1$, mais $1 \neq -1$.

f est surjective, car soit $y \in \mathbb{R}^{\geq 0}$, alors pour $x = y$, on a $f(x) = f(y) = |y| = y$.

•

$$\begin{array}{rcl} f : & \mathbb{N} & \rightarrow \mathbb{N} \\ & x & \mapsto x + 1 \end{array}$$

f est injective :

Soient $x_1, x_2 \in \mathbb{N}$.

On suppose $f(x_1) = f(x_2)$.

$$x_1 + 1 = x_2 + 1$$

$$x_1 = x_2$$

f n'est pas surjective

$y = 0 \in \mathbb{N}$ n'est pas égal à $f(x)$ pour $x \in \mathbb{N}$. Si il existait x avec $f(x) = 0$, $x + 1 = 0$, $x = -1$, $x \notin \mathbb{N}$.

•

$$\begin{array}{rcl} f : & \mathbb{R} & \rightarrow \mathbb{R} \\ & x & \mapsto 2x + 3 \end{array}$$

f est injective :

Soient $x_1, x_2 \in \mathbb{R}$.

supposons $f(x_1) = f(x_2)$, $2x_1 + 3 = 2x_2 + 3$, $2x_1 = 2x_2$, $x_1 = x_2$.

f est surjective :

Soit $y \in \mathbb{R}$.

On cherche x t.q. $f(x) = y$.

Posons $x = \frac{y - 3}{2} \in \mathbb{R}$.

Alors, $f(x) = f\left(\frac{y - 3}{2}\right) = 2 \cdot \frac{y - 3}{2} + 3 = y - 3 + 3 = y$.

Ainsi, f est bijective.

•

$$f : A \rightarrow B; A = \{1, 48, 57\}, B = \{a, b, c\}$$

$$1 \mapsto a, 48 \mapsto a, 57 \mapsto b$$

f n'est pas injective, car $1 \mapsto a$ et $48 \mapsto a$ avec $1 \neq 48$.

f n'est pas surjective, car aucun élément de $x \in A$ mappe c .

Remarque. La fonction $f' : A \rightarrow B'$ avec $B' = \{a, b\}$ est surjective.

Cours 3

Rappel. A, B deux ensembles

- $f : A \rightarrow B$ une fonction, associe à chaque $x \in A$ un unique $f(x) \in B$. $x \mapsto f(x)$.
- f est *inversible* s'il existe $g : B \rightarrow A$ t.q. $g(f(a)) = a$ pour tout $a \in A$ et $f(g(b)) = b$ pour tout $b \in B$.
- l'inverse est *unique*.
- La composition de $f : A \rightarrow B$ avec $g : B \rightarrow C$ est $g \circ f : A \rightarrow C$ avec $(g \circ f)(a) = g(f(a))$.
- f est injective si $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
- f est surjective si pour tout $b \in B$ il existe $a \in A$ t.q. $f(a) = b$.
- f est bijective si elle est injective et surjective.

Proposition. $f : A \rightarrow B$ est bijective si, et seulement si, elle est inversible.

Démonstration.

$\Leftarrow :$

Supposons que f est inversible.

Alors, il existe un inverse $g : B \rightarrow A$.

(inj) :

Soient $x_1, x_2 \in A$.

On suppose que $f(x_1) = f(x_2)$.

Alors, $g(f(x_1)) = g(f(x_2))$.

Donc, $x_1 = x_2$.

(surj) :

Soit $y \in B$.

Posons $x = g(y) \in A$.

Alors, $f(x) = f(g(y)) = y$.

Ainsi, f est bijective.

$\Rightarrow :$

Supposons f est injective et surjective.

Lemme. Pour chaque $y \in B$, il existe un unique $x \in A$ t.q. $f(x) = y$.

Démonstration.

Existance : Comme f est surjective, x existe.

Unicité : Supposons $x_1, x_2 \in A$ t.q. $f(x_1) = f(x_2)$, alors $x_1 = x_2$ puisque f est injective. ■

On définit $g : B \rightarrow A$ par $g(y) = x$ où x est l'unique élément du lemme.

On vérifie :

Soit $x \in A$, alors $\underbrace{g(f(x))}_y = x$, par définition de g .

Soit $y \in B$, alors $f(\underbrace{g(y)}_{\text{l'unique } x \text{ t.q. } f(x) = y}) = y$.

□

Définition. Une *opération* (interne, binaire) sur un ensemble E est un fonction $m : E \times E \rightarrow E$.

Exemple. $E = \mathbb{Z}$,

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (n, m) &\longmapsto n + m \\ \cdot : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (n, m) &\longmapsto n \cdot m \\ d : \mathbb{Q} \times \mathbb{Q} &\longrightarrow \mathbb{Q} \\ (x, y) &\longmapsto \frac{x}{y} \end{aligned}$$

n'est pas une opération, car $(1, 0) \mapsto \frac{1}{0}$ qui n'est pas défini. (d n'est pas une fonction.)

Cependant,

$$\begin{aligned} d : \mathbb{Q}_* \times \mathbb{Q}_* &\longrightarrow \mathbb{Q}_* \\ (x, y) &\longmapsto \frac{x}{y} \end{aligned}$$

est une opération.

A un ensemble

$E = \{f : A \rightarrow A\}$, où f est une fonction.

$$\begin{aligned} c : E \times E &\longrightarrow E \\ (f, g) &\longmapsto f \circ g \end{aligned}$$

La composition est une opération.

Notation. On note la plupart du temps une opération par un symbole entre les entrées.

Exemple. $m(x, y) := x * y$, ou $x + y$, ou $x \circ y$, ou xy .

Définition.

Un élément neutre pour une opération $*$ est un élément $e \in E$ t.q. pour tout $x \in E$, $e * x = x$ et $x * e = x$.

Cours 4

Rappel.

- $f : E \rightarrow F$ est bijective $\Leftrightarrow f$ est inversible.
- L'inverse est unique ($g = f^{-1}$)
- Opération : $m : E \times E \rightarrow E$, ou $* : E \times E \rightarrow E$

$$(x, y) \mapsto z$$
- Élément neutre : $e \in E$ t.q. $e * x = x$ et $x * e = x$.
- f est injective si tout $y \in F$ a au plus un antécédent
- f est surjective si tout $y \in F$ a au moins un antécédent
- f est bijective si tout $y \in F$ a exactement un antécédent
- x est antécédent de y si $f(x) = y$

Exemple.

Sur \mathbb{N} ,

- 0 est neutre pour $+$.

$$\begin{aligned} 0 + n &= n \\ n + 0 &= n \end{aligned}$$

- 1 est neutre pour \times .

$$\begin{aligned} 1 \times n &= n \\ n \times 1 &= n \end{aligned}$$

Sur \mathbb{Z} , $-$ est une opération mais elle n'a pas d'élément neutre.

En effet,

Supposons que $e \in \mathbb{Z}$ est neutre, alors $e - n = n$ pour tout n .

Pour $n = 0$, $e - 0 = 0$, donc $e = 0$.

Pour $n = 1$, $e - 1 = 1$, donc $-1 = 1$.

- Sur l'ensemble $E = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$, la multiplication matricielle \times est une opération.
La matrice $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est neutre pour \times .
- Sur $E = \{f : A \rightarrow A\}$, la fonction $\mathbb{1}_A$ est neutre pour la composition de fonctions.

Démonstration.

On doit montrer $\mathbb{1}_A \circ f = f$ et $f \circ \mathbb{1}_A = f$ pour tout $f \in E$.

(1) Soit $x \in A$, alors

$$\begin{aligned} (\mathbb{1}_A \circ f)(x) &= \mathbb{1}_A(f(x)) \\ &= f(x) \end{aligned}$$

Donc, $\mathbb{1}_A \circ f = f$.

(2) Soit $x \in A$, alors

$$\begin{aligned} (f \circ \mathbb{1}_A)(x) &= f(\mathbb{1}_A(x)) \\ &= f(x) \end{aligned}$$

Donc, $f \circ \mathbb{1}_A = f$.

□

On peut décrire une opération sur un ensemble fini avec sa table “de multiplication”.

Exemple. $A = \{0, 1\}$

$f_1 : \begin{matrix} 0 & \mapsto & 0 \\ 1 & \mapsto & 0 \end{matrix}, f_2 : \begin{matrix} 0 & \mapsto & 0 \\ 1 & \mapsto & 1 \end{matrix}, f_3 : \begin{matrix} 0 & \mapsto & 1 \\ 1 & \mapsto & 0 \end{matrix}, f_4 : \begin{matrix} 0 & \mapsto & 1 \\ 1 & \mapsto & 1 \end{matrix}$ On a $f_2 = \mathbb{1}_A$.

○	f_1	f_2	f_3	f_4
f_1	f_1	f_1	f_1	f_1
f_2	f_1	f_2	f_3	f_4
f_3	f_4	f_3	f_2	f_1
f_4	f_4	f_4	f_4	f_4

Définition.

Une opération $*$ sur E est *associative* si pour tout $x, y, z \in E$, on a $(x * y) * z = x * (y * z)$.

Proposition.

Si $$ admet un élément neutre, alors celui-ci est unique.*

Démonstration.

Supposons que e et e' sont neutres pour $*$.

On a

$$\begin{aligned} e * e' &= e' && \text{car } e \text{ est neutre} \\ e * e' &= e && \text{car } e' \text{ est neutre} \end{aligned}$$

Donc, $e = e'$.

□

Définition.

Soit E un ensemble, $*$ une opération sur E et $e \in E$ un neutre pour $*$. On dit que $a, b \in E$ sont *inverses* si $a * b = e$ et $b * a = e$.

Dans ce cas, on dit que a et b sont inversibles.

Exemple.

Dans \mathbb{Z} avec $+$, 3 et -3 sont inverses. En effet, on a $3 + (-3) = 0$ et $(-3) + 3 = 0$ avec 0 l'élément neutre de $+$.

Exemple.

Dans \mathbb{Z} avec \times , le neutre est 1, mais seuls 1 et -1 sont inversibles. En effet, on a $1 \times 1 = 1$ et $(-1) \times (-1) = 1$.

Remarque.

L'élément neutre est son propre inverse. En effet, $e * e = e$, pour tout $*$ qui admet e comme élément neutre.

Proposition.

Si $$ est associative et admet un élément neutre e , alors les inverses sont uniques s'ils existent.*

Démonstration.

Soit $a \in E$.

Supposons b, b' sont inverses de a .

Alors,

$$\begin{aligned} b &= b * e \\ \text{car } b' \text{ est inverse de } a &= b * (a * b') \\ \text{associativité} &= (b * a) * b' \\ \text{car } b \text{ est inverse de } a &= e * b' \\ &= b' \end{aligned}$$

□

Notation.

Comme l'inverse de a est unique, on le note a^{-1} .

Exemple.

Dans $E = \{f : A \rightarrow A\}$, avec l'opération \circ , les fonctions bijectives sont exactement celles qui sont inversibles pour \circ .

Proposition.

La composition de fonctions est associative.

Démonstration.

Soient $f : A \rightarrow B$, $g : B \rightarrow C$ et $h : C \rightarrow D$.

Soit $a \in A$.

$$\begin{aligned} ((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) \\ &= h(g(f(a))) \\ &= h((g \circ f)(a)) \\ &= (h \circ (g \circ f))(a) \\ \Rightarrow (h \circ g) \circ f &= h \circ (g \circ f) \end{aligned}$$

□

Chapitre 6 Groupes

Définition.

Un *groupe* est un ensemble G muni d'une opération $*$ t.q.

- (A) $*$ est associative
- (N) $*$ admet un neutre
- (I) tout $g \in G$ admet un inverse

Exemple.

- (1) $(\mathbb{Z}, +)$ est un groupe.

Neutre : 0

Inverse de n : $-n$

- (2) $(\mathbb{Q}, +)$ et $(\mathbb{R}, +)$ sont des groupes.

- (3) (\mathbb{Z}, \times) n'est pas un groupe, car, par exemple, 2 n'est pas inversible.

- (4) (\mathbb{Q}, \times) n'est pas un groupe, car 0 n'est pas inversible.

- (5) (\mathbb{Q}_*, \times) et (\mathbb{R}_*, \times) sont des groupes.

Neutre : 1

Inverse de x : $\frac{1}{x}$

Remarque. (1), (2) et (5) sont *commutatifs*.

Remarque. $(\mathbb{N}, +)$ n'est pas un groupe.

Définition. Si l'opération d'un groupe est commutative, on note le groupe comme *abélien* (ou commutatif).

- (6) $GL(n, \mathbb{R})$ est un groupe pour la multiplication matricielle.

$GL(n, \mathbb{R}) = \{M | M \text{ est une matrice } n \times n \text{ réelle inversible}\}$.

GL : général linéaire

$$\text{Neutre : } \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}.$$

M^{-1} la matrice inverse est l'inverse.

Pour $n \geq 2$, $GL(n, \mathbb{R})$ n'est pas abélien.

- (7) A un ensemble quelconque

$S(A) = \{f : A \rightarrow A | f \text{ est bijective}\}$ est un groupe pour \circ .

Neutre : $\mathbb{1}_A$

Inverse de f : f^{-1}

Remarque.

Pour $A = \{0, 1\}$

$$f_1 : \begin{matrix} 0 & \mapsto & 0 \\ 1 & \mapsto & 0 \end{matrix}, f_2 : \begin{matrix} 0 & \mapsto & 0 \\ 1 & \mapsto & 1 \end{matrix}, f_3 : \begin{matrix} 0 & \mapsto & 1 \\ 1 & \mapsto & 0 \end{matrix}, f_4 : \begin{matrix} 0 & \mapsto & 1 \\ 1 & \mapsto & 1 \end{matrix}, S(A) = \{f_2, f_3\}.$$

Cours 5

Rappel.

- Groupe : $(G, *)$

G ensemble

* opération sur G

- (A) * est associative

$$\forall a, b, c \in G, (a * b) * c = a * (b * c)$$

- (N) * admet un élément neutre dans G

$$\exists e \in G \text{ t.q. } \forall a \in G, e * a = a = a * e$$

- (I) tout élément de G est inversible

$$\forall a \in G, \exists b \in G \text{ t.q. } a * b = e = b * a$$

- Le neutre et l'inverse sont uniques

Remarque.

“Le groupe \mathbb{R} ” implique l’opération + et “le groupe \mathbb{R}_* ” implique l’opération \times .

Propriétés élémentaires des groupes

- (1) $\forall a, b \in G, (a * b)^{-1} = b^{-1} * a^{-1}$.
- (2) $\forall a \in G, (a^{-1})^{-1} = a$
- (3) Si $a * b = a * c$, alors $b = c$
- (4) Si $b * a = c * a$, alors $b = c$

Démonstration.

- (1) On calcule

$$\begin{aligned} (a * b) * (b^{-1} * a^{-1}) &= a * (b * (b^{-1} * a^{-1})) & (b^{-1} * a^{-1}) * (a * b) &= b^{-1} * (a^{-1} * (a * b)) \\ &= a * ((b * b^{-1}) * a^{-1}) & &= b^{-1} * ((a^{-1} * a) * b) \\ &= a * (e * a^{-1}) & &= b^{-1} * (e * b) \\ &= a * a^{-1} & &= b^{-1} * b \\ &= e & &= e \end{aligned}$$

Donc, $(a * b)^{-1} = b^{-1} * a^{-1}$.

- (2) Comme $a^{-1} * a = e = a * a^{-1}$, a est l'inverse de a^{-1} , donc $(a^{-1})^{-1} = a$.

- (3) Supposons $a * b = a * c$. Alors

$$\begin{aligned} a^{-1} * (a * b) &= a^{-1} * (a * c) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c \\ e * b &= e * c \\ b &= c \end{aligned}$$

- (4) Supposons $b * a = c * a$. Alors

$$\begin{aligned} (b * a) * a^{-1} &= (c * a) * a^{-1} \\ b * (a * a^{-1}) &= c * (a * a^{-1}) \\ b * e &= c * e \\ b &= c \end{aligned}$$

□

Exemple.

$(\mathbb{Z}_3, +)$.

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$+$ est associative.

$\bar{0}$ est l'élément neutre.

$$(\bar{1})^{-1} = \bar{2}.$$

$$(\bar{2})^{-1} = \bar{1}.$$

$(\mathbb{Z}_3, +)$ est un groupe abélien.

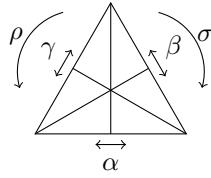
Remarque. La symétrie de la table par rapport à la diagonale implique la commutativité.

Exemple.

(\mathbb{D}_3, \circ) - groupe diédral d'ordre 3.

Groupe des symétries d'un triangle équilatéral.

$$\mathbb{D}_3 = \left\{ \begin{array}{l} \varepsilon \\ \text{identité} \\ \beta \\ \gamma \\ \alpha \\ \text{réflexion} \\ \sigma \\ \text{rotation} \end{array} \right\}.$$



\circ	ε	α	β	γ	ρ	σ
ε	ε	α	β	γ	ρ	σ
α	α	ε	ρ	σ	β	γ
β	β	σ	ε	ρ	γ	α
γ	γ	ρ	σ	ε	α	β
ρ	ρ	γ	α	β	σ	ε
σ	σ	β	γ	α	ε	ρ

(\mathbb{D}_3, \circ) n'est pas un groupe abélien.

Cours 6

Rappel.

- Groupe : $(G, *)$ avec A, N, I .

Abélien : C .

-

$$\begin{aligned} a * b &= a * c & \Rightarrow b &= c \\ b * a &= c * a & \Rightarrow b &= c \\ (a^{-1})^{-1} &= a \\ (a * b)^{-1} &= b^{-1} * a^{-1} \end{aligned}$$

-

Exemple.

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{Q}_*, \times), (\mathbb{R}_*, \times)$ sont des groupes abéliens ; $\mathbb{Z}_3, \mathbb{D}_3, GL(n, \mathbb{R})$ sont des groupes non abéliens.
 $S(E) = \{f : E \rightarrow E \mid f \text{ est bijective}\}$.

Remarque. E n'est pas l'ensemble utilisé dans la définition du groupe.

Produit cartésien de groupes

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

Proposition.

$G \times H$ est un groupe lorsque muni de l'opération $(a, b) \bullet (a', b') = (a * a', b \diamond b')$, avec $a, a' \in G$ et $b, b' \in H$.

Démonstration.

(N) $e \in G$ le neutre et $e' \in H$ le neutre, alors $(e, e') \in G \times H$

$$\begin{aligned}(a, b) \bullet (e, e') &= (a * e, b \diamond e') \\ &= (a, b) \\ (e, e') \bullet (a, b) &= (e * a, e' \diamond b) \\ &= (a, b)\end{aligned}$$

(e, e') est bien neutre.

(I) $(a, b) \in G \times H$, alors (a^{-1}, b^{-1}) est inverse de (a, b) .

En effet,

$$\begin{aligned}(a, b) \bullet (a^{-1}, b^{-1}) &= (a * a^{-1}, b \diamond b^{-1}) \\ &= (e, e') \\ (a^{-1}, b^{-1}) \bullet (a, b) &= (a^{-1} * a, b^{-1} \diamond b) \\ &= (e, e')\end{aligned}$$

(A) Soient $(a, b), (c, d), (e, f) \in G \times H$. On a

$$\begin{aligned}((a, b) \bullet (c, d)) \bullet (e, f) &= (a * c, b \diamond d) \bullet (e, f) \\ &= ((a * c) * e, (b \diamond d) \diamond f) \\ &= (a * (c * e), b \diamond (d \diamond f)) \\ &= (a, b) \bullet (c * e, d \diamond f) \\ &= (a, b) \bullet ((c, d) \bullet (e, f))\end{aligned}$$

□

Exemple.

- $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$
 $(x, y) + (x', y') = (x + x', y + y')$.
- $(\mathbb{Z}_2, +)$

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\mathbb{Z}_2 \times \mathbb{Z}_2$

+	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$

Isomorphismes de groupes

Définition. $(G, *)$ et (H, \diamond) deux groupes.

Un *isomorphisme* de G vers H est une application $f : G \rightarrow H$ t.q.

- (1) $\forall a, b \in G, f(a * b) = f(a) \diamond f(b)$.

Préservation des opérations

(2) f est bijective.

Exemple.

- $(\mathbb{R}, +)$ et (\mathbb{R}_*^+, \times)

$f : \mathbb{R} \rightarrow \mathbb{R}_*^+$ $x \mapsto e^x$ est un isomorphisme de groupes.

(1) Soient $x, y \in \mathbb{R}$.

$$\begin{aligned} f(x+y) &= e^{x+y} \\ &= e^x \times e^y \\ &= f(x) \times f(y) \end{aligned}$$

(2) $\ln : \mathbb{R}_*^+ \rightarrow \mathbb{R}$ est inverse de $f : \ln e^x = x, \forall x \in \mathbb{R}$ et $e^{\ln x} = x, \forall x \in \mathbb{R}_*^+$.

Proposition. Si $f : G \rightarrow H$ est un isomorphisme de groupes, alors $f(e_G) = e_H$, où e_G est l'élément neutre de G et e_H est l'élément neutre de H .

Démonstration. Stratégie : montrer que $f(e_G)$ est neutre pour H et utiliser l'unicité.

Soit $b \in H$.

Comme f est bijective, $\exists a \in G$ t.q. $f(a) = b$

$$\begin{array}{ll} f(e_G) \diamond b = f(e_G) \diamond f(a) & b \diamond f(e_G) = f(a) \diamond f(e_G) \\ = f(e_G * a) & = f(a * e_G) \\ = f(a) & = f(a) \\ = b & = b \end{array}$$

On a donc que $f(e_G) \in H$ est neutre pour \diamond , mais comme l'élément neutre est unique, $f(e_G) = e_H$. \square

Exemple. Pour $f : \mathbb{R} \rightarrow \mathbb{R}_*^+$ $x \mapsto e^x$, $f(0) = e^0 = 1$.

Proposition. Si $f : G \rightarrow H$ est un isomorphisme de groupes, alors $f(a^{-1}) = f(a)^{-1}$, pour tout $a \in G$.

Démonstration. Stratégie : montrer que $f(a^{-1})$ est inverse de $f(a)$ et utiliser l'unicité.

$$\begin{array}{ll} f(a^{-1}) \diamond f(a) = f(a^{-1} * a) & f(a) \diamond f(a^{-1}) = f(a * a^{-1}) \\ = f(e_G) & = f(e_G) \\ = e_H & = e_H \end{array}$$

On a donc que $f(a^{-1})$ est inverse de $f(a)$, mais comme l'inverse est unique, $f(a^{-1}) = f(a)^{-1}$. \square

Exemple. Pour $f : \mathbb{R} \rightarrow \mathbb{R}_*^+$ $x \mapsto e^x$, $f(-x) = e^{-x} = (e^x)^{-1} = f(x)^{-1} = \frac{1}{f(x)}$, où $-x$ est l'inverse de x pour $+$ et $\frac{1}{f(x)}$ est l'inverse de $f(x)$ pour \times .

Remarque. Si G, H sont des groupes finis et f est un isomorphisme, alors f “envoie la table de G à celle de H ”.

*	e_G	a_1	a_2	\dots	\diamond	e_H	$f(a_1)$	$f(a_2)$	\dots
e_G					$f(e_G)$				
a_1			$a_1 * a_2$		$f(a_1)$			$f(a_1) \diamond f(a_2)$	
a_2					$f(a_2)$				
\vdots					\vdots				

$G : \xrightarrow{f} H$

Avec $f(a_1 * a_2) = f(a_1) \diamond f(a_2)$.

Exemple.

$$\begin{array}{c} \begin{array}{c|c|c} + & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{1} \\ \hline \bar{1} & \bar{1} & \bar{0} \end{array} \quad H : \begin{array}{c|c|c} \circ & \varepsilon & \alpha \\ \hline \varepsilon & \varepsilon & \alpha \\ \hline \alpha & \alpha & \varepsilon \end{array} \quad C_2 : \begin{array}{c|c|c} \times & 1 & -1 \\ \hline 1 & 1 & -1 \\ \hline -1 & -1 & 1 \end{array} \end{array}$$

\mathbb{Z}_2 , H et C_2 sont isomorphes.

Il existe un isomorphisme entre chaque paire.

Proposition. Si $f : G \rightarrow H$ est un isomorphisme, alors $f^{-1} : H \rightarrow G$ est un isomorphisme.

Démonstration.

(1) Soient $b_1, b_2 \in H$.

$$\begin{aligned} f^{-1}(b_1 \diamond b_2) &= f^{-1}(f[f^{-1}(b_1)] \diamond f[f^{-1}(b_2)]) \\ &= f^{-1}(f[f^{-1}(b_1) * f^{-1}(b_2)]) \\ &= f^{-1}(b_1) * f^{-1}(b_2) \end{aligned}$$

(2) f^{-1} est bijective, car elle est inversible d'inverse f .

$$\begin{aligned} f \circ f^{-1} &= 1_H \\ f^{-1} \circ f &= 1_G \end{aligned}$$

□

Proposition (Transitivité).

Si $f : G \rightarrow H$ et $g : H \rightarrow K$ sont des isomorphismes, alors $g \circ f : G \rightarrow K$ est un isomorphisme.

Démonstration.

(1) Soient $a, b \in G$

$$\begin{aligned} (g \circ f)(a * b) &= g(f(a * b)) \\ &= g(f(a) \diamond f(b)) \\ &= g(f(a)) \oplus g(f(b)) \\ &= (g \circ f)(a) \oplus (g \circ f)(b) \end{aligned}$$

(2) $g \circ f$ est inversible d'inverse $f^{-1} \circ g^{-1}$.

□

Puissances d'éléments de groupes

Définition (par récurrence).

$a \in G, n \in \mathbb{N}$

- (1) $a^0 := e_G$
- (2) $a^n = a * a^{n-1}, \forall n \geq 1$

Exemple.

•

$$\begin{aligned} a^4 &= a * a^3 \\ &= a * a * a^2 \\ &= a * a * a * a^1 \\ &= a * a * a * a * a^0 \\ &= a * a * a * a * e \\ &= a * a * a * a \end{aligned}$$

- Dans $(\mathbb{Z}, +)$, $2^3 = 3 \cdot 2 = 2 + 2 + 2$.

Proposition. $a^{n+m} = a^n * a^m$, $\forall n, m \in \mathbb{N}$.

Démonstration. par récurrence sur n .

(1) $n = 0$:

$$\begin{aligned} a^{0+m} &= a^m \\ &= e * a^m \\ &= a^0 * a^m \end{aligned}$$

(2) supposons que $a^{n+m} = a^n * a^m$ pour un $n \geq 0$.

$$\begin{aligned} a^{(n+1)+m} &= a^{n+m+1} \\ &= a * a^{n+m} \\ \text{hyp rec} &= a * (a^n * a^m) \\ &= (a * a^n) * a^m \\ &= a^{n+1} * a^m \end{aligned}$$

□

Définition. Pour $n \in \mathbb{Z}$.

Si $n \geq 0$, on a déjà défini a^n .

Si $n < 0$, on définit $a^n = (a^{-1})^{-n}$.

Exemple. $a^{-3} = (a^{-1})^3 = a^{-1} * a^{-1} * a^{-1}$.

Proposition. $a^{n+m} = a^n * a^m$, $\forall n, m \in \mathbb{Z}$.

Proposition. $(a^n)^m = a^{nm}$, $\forall m, n \in \mathbb{N}$. Vraie aussi pour $m, n \in \mathbb{Z}$.

Démonstration. par récurrence sur m .

(1) $m = 0$:

$$\begin{aligned} (a^n)^0 &= e \\ a^{n \cdot 0} &= a^0 = e \end{aligned}$$

(2) supposons que $(a^n)^m = a^{nm}$ pour un certain $m \in \mathbb{N}$.

$$\begin{aligned} (a^n)^{m+1} &= (a^n)(a^n)^m \\ \text{hyp rec} &= (a^n)a^{nm} \\ &= a^{n+nm} \\ &= a^{n(m+1)} \end{aligned}$$

□

Cours 7

Rappel.

- Isomorphisme : $f : G \rightarrow H$ t.q.

- (1) $f(ab) = f(a)f(b)$
avec $a * b$ et $f(a) \diamond f(b)$ implicitement.
- (2) f est bijective
“même table”

- f, g isomorphismes $\Rightarrow f^{-1}, g \circ f$ isomorphismes.
 $1_G : G \rightarrow G$ est trivialement un isomorphisme.
- G est isomorphe à H s'il existe un isomorphisme $f : G \rightarrow H$.
- Puissances :
Soit $a \in G$ avec G un groupe.

- $a^0 = e$
- $a^{n+1} = aa^n$
- $a^{-n} = (a^{-1})^n$
- $a^{n+m} = a^n a^m$
- $(a^n)^m = a^{n \cdot m}$

- f isomorphisme
 - $f(e_G) = e_H$
 - $f(a^{-1}) = f(a)^{-1}$

Proposition. f isomorphisme $f : G \rightarrow H$.

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

Démonstration. par récurrence sur n .

$n \geq 0$ (1) $n = 0$

$$\begin{aligned} f(a^0) &= f(e_G) \\ &= e_H \\ &= f(a)^0 \end{aligned}$$

(2) supposons que $f(a^n) = f(a)^n$ pour un certain $n \in \mathbb{Z}$.

$$\begin{aligned} f(a^{n+1}) &= f(a \cdot a^n) \\ &= f(a)f(a^n) \\ &\stackrel{\text{hyp rec}}{=} f(a)f(a)^n \\ &= f(a)^{n+1} \end{aligned}$$

$n < 0$ alors, $-n > 0$ et

$$\begin{aligned} f(a^n) &= f((a^{-1})^{-n}) \\ &= f(a^{-1})^{-n} \\ &= (f(a)^{-1})^{-n} \\ &= f(a)^n \end{aligned}$$

□

Exemple. $H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R}) \mid x \in \mathbb{R} \right\}$, avec la multiplication de matrices.

Soient $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} \in H$

(A) : associatif, car la multiplication de matrices est associative.

(N) : $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$ est neutre

(I) : l'inverse de $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ est $\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}$

Ainsi, H est un groupe pour la multiplication matricielle.

On définit $f : \mathbb{R} \rightarrow H$

$$x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

Soient $x, y \in \mathbb{R}$.

$$(1) \quad f(x+y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = f(x) \cdot f(y)$$

(2) montrons que. f est bijective.

- f est injective

Soient $x, y \in \mathbb{R}$.

Supposons $f(x) = f(y)$

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$$

$$x = y$$

- f est surjective

Soit $Y = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in H$, avec $y \in \mathbb{R}$.

$Y = f(y)$.

□

Sous-groupes

Définition. $H \subseteq G$ est un *sous-groupe* de G si H est un groupe pour la même opération que G .

Exemple.

- $\{e\} \subseteq G$ est un sous-groupe.
- $G \subseteq G$ est un sous-groupe.
- $\{\dots, -4, -2, 0, 2, 4, \dots\} = 2\mathbb{Z} \subseteq (\mathbb{Z}, +)$
- Dans $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, $\{\bar{0}, \bar{2}\}$ est un sous-groupe.

+	$\bar{0}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{0}$

Ce groupe est isomorphe à \mathbb{Z}_2 et à $C_2 = (\{-1, 1\}, \times)$.

- $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +)$.
- $C_2 \subseteq \mathbb{Q}_* \subseteq \mathbb{R}_*$.
- $\mathbb{D}_3 = \{\varepsilon, \alpha, \beta, \gamma, \rho, \sigma\}$.
- $\{\varepsilon, \alpha\}$ et $\{\varepsilon, \rho, \sigma\}$ sont des sous-groupes de \mathbb{D}_3 .

Notation. On note l'ensemble $m\mathbb{Z} = \{m \cdot n \mid n \in \mathbb{Z}\}$.

Cours 8

Rappel.

- $a \in G$.
 - $a^n = \underbrace{a * a * \dots * a}_{n \text{ fois}}$
 - $a^n = a * a^{n-1}$
 - $a^0 = e$
 - $a^{-n} = (a^{-1})^n$

- Sous-groupe de $(G, *) : H \subseteq G$ qui est un groupe pour $*$.

Exemple. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ pour $+$.

Exemple.

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

est un sous-groupe de $GL(2, \mathbb{R})$.

Proposition. $H \subseteq G$ un sous-groupe.

- (1) Si G est abélien, alors H est abélien ;
- (2) Le neutre de H est le neutre de G ;
- (3) Si $a \in H$, son inverse $a^{-1} \in H$ est l'inverse de a dans G .

Démonstration.

- (1) G est abélien, alors $\forall a, b \in G, ab = ba$.

En particulier, $\forall a, b \in H, ab = ba$.

- (2) Le neutre de G e_G a la propriété que $\forall a \in G, e_G a = a = a e_G$.

Comme $H \subseteq G$, cette propriété est vraie pour H aussi.

Donc, $a e_G = a = e_G a$.

Ainsi, e_G est le neutre de H , par l'unicité de l'élément neutre.

- (3) $a \in H$, il existe un inverse $b \in G$ pour a t.q. $ab = ba = e$.

Comme H est un groupe, $\exists! a^{-1} \in H$.

De $ab = e$, on a $a^{-1}ab = a^{-1}e$, donc $b = a^{-1}$.

□

Théorème.

Un sous-ensemble non-vide $H \subseteq G$ est un sous-groupe si, et seulement si, pour tous $a, b \in H$, $ab^{-1} \in H$.

Démonstration.

(\Rightarrow) Supposons que H est un sous-groupe, donc $a, b \in H$, alors $b^{-1} \in H$.

De plus, H est fermé pour la multiplication, donc $ab^{-1} \in H$.

(\Leftarrow) (N) H est non-vide, donc $\exists a \in H$.

Par hypothèse, $aa^{-1} = e \in H$.

(I) On vient de montrer que $e \in H$.

Soit $b \in H$ quelconque. Par hypothèse, $eb^{-1} = b^{-1} \in H$.

(A) On sait que $\forall a, b, c \in G, (ab)c = a(bc)$.

En particulier, $\forall a, b, c \in H, (ab)c = a(bc)$.

Finalement, H est fermé pour l'opération de G , car $\forall a, b \in H, b^{-1} \in H$.

Donc, par hypothèse, $a(b^{-1})^{-1} = ab \in H$.

□

Exemple.

Soit $m \in \mathbb{Z}$.

Posons $H = m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, 2m, \dots\}$, muni de l'addition.

montrons que. H est un sous-groupe de $(\mathbb{Z}, +)$.

H est non-vide, car $m0 = 0 \in H$.

Soient $a, b \in H$.

Par définition de H , $\exists a', b' \in \mathbb{Z}$ t.q. $a = ma'$ et $b = mb'$.

Dans \mathbb{Z} , $b^{-1} = -mb'$.

On a $a + (-b) = ma' + (-mb') = m(a' - b') \in H$.

Donc, H est un sous-groupe de $(\mathbb{Z}, +)$.

□

Réciproquement, soit $H \subseteq \mathbb{Z}$ un sous-groupe de \mathbb{Z} quelconque. Alors $\exists m \in \mathbb{Z}$ t.q. $H = m\mathbb{Z}$.

Démonstration.

On sait que $0 \in H$.

Si $H = \{0\}$, alors $H = 0\mathbb{Z}$ et l'énoncé est vrai.

Sinon, H contient un autre élément $a \in H$, donc $-a \in H$.

En particulier, H contient au moins un entier positif.

Soit m le plus petit élément positif de H .

Soit $h \in H$ quelconque. On divise h par m , donc $h = qm + r$, où $q, r \in \mathbb{Z}$ et $0 \leq r < m$.

Si $r = 0$, $h = qm \in m\mathbb{Z}$.

Sinon, comme $h \in H$ et $m \in H$, $h - qm \in H$, mais $h - qm = r$, donc $r \in H$.

Comme $0 < r < m$, il y a une contradiction à la définition de m .

↳

Ainsi, $H \subseteq m\mathbb{Z}$. Mais clairement, $m\mathbb{Z} \subseteq H$, car $m \in H$ et $mn \in H$, donc $H = m\mathbb{Z}$.

□

Proposition.

Soit $f : G \rightarrow H$ un isomorphisme. Alors, $K \subseteq G$ est un sous-groupe de G si, et seulement si, $f(K)$ est un sous-groupe de H .

Notation. $f(K) = \{f(k) \mid k \in K\}$.

(\Rightarrow) Supposons que K est un sous-groupe de G .

On sait que $e \in K$, alors $f(e) = e \in f(K)$, donc $f(K)$ est non-vide.

Soient $a, b \in f(K)$. On veut montrer que $ab^{-1} \in f(K)$.

Alors, $a = f(k)$ et $b = f(k')$, avec $k, k' \in K$.

Donc, $ab^{-1} = f(k)f(k')^{-1} = f(k)f(k'^{-1}) = f(kk'^{-1})$.

Comme $kk'^{-1} \in K$, $ab^{-1} \in f(K)$.

(\Leftarrow) On effectue la même preuve avec f^{-1} qui est un isomorphisme en remarquant que $f^{-1}(f(k)) = k$.

Notation.

$G \xrightarrow{f} H$ avec f un isomorphisme est équivalent à $G \xrightarrow{\sim} H$.

Notation.

$H \subseteq G$ un sous-groupe est équivalent à $H \leqslant G$.

Proposition.

Soit $\{H_i\}_{i \in I}$ une collection de sous-groupes de G . Alors $\bigcap_{i \in I} H_i \leqslant G$.

Démonstration.

$H_i \leqslant G, \forall i \in I$.

Alors, $e \in H_i, \forall i$. Donc, $e \in \bigcap_{i \in I} H_i$. En particulier, $\bigcap_{i \in I} H_i \neq \emptyset$.

Soient $a, b \in \bigcap_{i \in I} H_i$. Alors, $a, b \in H_i, \forall i$.

Comme $H_i \leqslant G$, $ab^{-1} \in H_i, \forall i$, donc $ab^{-1} \in \bigcap_{i \in I} H_i$.

□

Remarque. Si $H_1, H_2 \leqslant G$, $H_1 \cup H_2$ n'est pas nécessairement un sous-groupe de G .

Exemple. $2\mathbb{Z} \leqslant \mathbb{Z}$ et $3\mathbb{Z} \leqslant \mathbb{Z}$. $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de \mathbb{Z} .

Plus précisément, $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, mais $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Exemple. $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z} \leqslant \mathbb{Z}$.

Chapitre 2 Applications et équivalences

Section 2.4 Relations d'équivalence

Définition. Une *relation d'équivalence* sur un ensemble E est un sous-ensemble $R \subseteq E \times E$ satisfaisant

(1) réflexivité

$$x \sim x, \forall x \in E.$$

(2) symétrie

$$x \sim y \Rightarrow y \sim x.$$

(3) transitivité

$$x \sim y \text{ et } y \sim z, \text{ alors } x \sim z.$$

Notation. On note $x \sim y$ si, et seulement si, $(x, y) \in R$.

Exemple.

(1) $E = \mathbb{R}$

$$x \sim y \text{ si, et seulement si, } |x| = |y|$$

$$(\text{refl}) \quad |x| = |x|, \text{ donc } x \sim x.$$

$$(\text{sym}) \quad \text{Supposons } x \sim y. \text{ Alors, } |x| = |y|. \text{ Donc, } y \sim x.$$

$$(\text{trans}) \quad \text{Supposons } x \sim y \text{ et } y \sim z. \text{ Alors, } |x| = |y| \text{ et } |y| = |z|. \text{ Donc } |x| = |z|. \text{ Ainsi, } x \sim z.$$

(2) C est l'ensemble des élèves dans la classe.

$$x \sim y \text{ si, et seulement si, } x \text{ et } y \text{ ont le même âge est une relation d'équivalence.}$$

Définition. Si E est un ensemble et \sim est une relation d'équivalence sur E , la *classe d'équivalence* de $x \in E$ est $\bar{x} = \{y \in E \mid y \sim x\} \subseteq E$.

Lemme. $\bar{x} = \bar{y}$ si, et seulement si, $x \sim y$.

Démonstration.

(\Rightarrow) Supposons $\bar{x} = \bar{y}$.

Par (refl), $x \sim x$, donc $x \in \bar{x}$. Alors, $x \in \bar{y}$. Ainsi, $x \sim y$.

(\Leftarrow) Supposons $x \sim y$.

(\subseteq) Soit $z \in \bar{x}$. Alors $z \sim x$. Comme $x \sim y$, par (trans), $z \sim y$. Donc, $z \in \bar{y}$.

(\supseteq) Soit $z \in \bar{y}$. Alors, $z \sim y$ et, par (sym), $y \sim z$. Comme $x \sim y$, par (trans), $x \sim z$ et, par (sym), $z \sim x$. Donc, $z \in \bar{x}$.

Ainsi, $\bar{x} = \bar{y}$.

□

Cours 9

Rappel.

- $H \leqslant G$, H un sous-groupe de G , si, et seulement si,
 - $H \neq \emptyset$;
 - $\forall a, b \in H, ab^{-1} \in H$.

- Si $H \leq G$, H a le même neutre que G , mêmes inverses.
- G abélien $\Rightarrow H \leq G$ abélien.
- Si $f : G \rightarrow H$ isomorphisme, alors $K \leq G \Leftrightarrow f(K) \leq H$.
- Relations d'équivalence \sim sur E :
 - (Refl) $a \sim a, \forall a \in E$;
 - (Sym) $a \sim b \Rightarrow b \sim a$;
 - (Trans) $a \sim b, b \sim c \Rightarrow a \sim c$.
- Classe d'équivalence : $\bar{a} = \{b \in E \mid b \sim a\}$.
- $a \sim b \Leftrightarrow \bar{a} = \bar{b}$.

Exemple. $E = \mathbb{Z}$.

Équivalence modulo m :

$a \sim b$ si, et seulement si, $a - b = km$, avec $k \in \mathbb{Z}$.

Notation. $m \mid a - b$, m divise $a - b$: $\exists k \in \mathbb{Z}$ t.q. $a - b = km$.

$$a \sim b \Leftrightarrow m \mid a - b.$$

Démonstration. que c'est bel et bien une équivalence

(Refl) Soit $a \in \mathbb{Z}$.

$$a - a = 0m \Rightarrow a \sim a.$$

(Sym) Supposons que $a \sim b$, avec $a, b \in \mathbb{Z}$.

$$\text{Alors, } a - b = km, \text{ avec } k \in \mathbb{Z}.$$

$$\text{Or, } -(a - b) = -km \Rightarrow b - a = (-k)m, \text{ donc } b \sim a.$$

(Trans) Supposons que $a \sim b$ et $b \sim c$, avec $a, b, c \in \mathbb{Z}$.

$$\text{Alors, } a - b = k_1m \text{ et } b - c = k_2m, \text{ avec } k_1, k_2 \in \mathbb{Z}.$$

En additionnant les deux équations, on obtient

$$\begin{aligned} a - c &= k_1m + k_2m \\ &= (k_1 + k_2)m \end{aligned}$$

Donc, $a \sim c$.

□

Si $m = 2$, les classes d'équivalence sont

$$\begin{aligned} \bar{0} &= \{a \in \mathbb{Z} \mid a \sim 0\} & \bar{1} &= \{a \in \mathbb{Z} \mid a \sim 1\} \\ &= \{a \in \mathbb{Z} \mid a - 0 = 2k\} & &= \{a \in \mathbb{Z} \mid a - 1 = 2k\} \\ &= \{a \in \mathbb{Z} \mid a = 2k\} & &= \{a \in \mathbb{Z} \mid a = 2k + 1\} \\ &= 2\mathbb{Z} & &= \mathbb{Z} \setminus 2\mathbb{Z} \end{aligned}$$

Remarque.

$$\bar{0} = \bar{2} = \bar{4} = \bar{-2} = \dots$$

$$\bar{1} = \bar{3} = \bar{5} = \bar{-1} = \dots$$

Plus généralement, pour $m\mathbb{Z}$, on a m classes d'équivalence.

$$\bar{0}, \bar{1}, \bar{2}, \dots, \bar{m-1}$$

Notation. L'ensemble des classes d'équivalence est noté $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{m-1}\}$ pour la relation de congruence modulo m .

Définition. Une *partition* d'un ensemble E est une collection $\mathcal{P} = \{E_i\}$, avec $i \in I$ de sous-ensembles de E t.q.

$$(1) \bigcup_{i \in I} E_i = E;$$

$$(2) E_i \cap E_j = \emptyset, \text{ si } i \neq j.$$

Remarque. Chaque $x \in E$ est élément d'exactement un E_i .

Proposition. Si \sim est une relation d'équivalence sur E , alors $\mathcal{P} = \{\bar{a} \mid a \in E\}$ est une partition de E .

Exemple. $E = \mathbb{Z}$, \sim équivalence modulo 3.

$\mathcal{P} = \{\bar{0}, \bar{1}, \bar{2}\}$ est une partition de \mathbb{Z} .

Démonstration.

(1) Clairement, $\bigcup_{a \in E} \bar{a} \subseteq E$.

On veut montrer que $E \subseteq \bigcup_{a \in E} \bar{a}$.

Soit $x \in E$, alors $x \sim x$ par réflexivité, donc $x \in \bar{x}$ et $x \in \bigcup_{a \in E} \bar{a}$.

(2) Supposons que $x \in \bar{a}$ et $x \in \bar{b}$, avec $\bar{a} \neq \bar{b}$.

Alors, $x \sim a$ et $x \sim b$. Donc, par symétrie, $a \sim x$ et $x \sim b$. Donc, par transitivité, $a \sim b$. Donc $\bar{a} = \bar{b}$. Ceci est une contradiction, donc $\bar{a} \cap \bar{b} = \emptyset, \forall \bar{a} \neq \bar{b} \in \mathcal{P}$.

□

On définit une opération sur \mathbb{Z}_m pour la congruence modulo m .

$$\begin{aligned} + : \mathbb{Z}_m \times \mathbb{Z}_m &\rightarrow \mathbb{Z}_m \\ (\bar{a}, \bar{b}) &\mapsto \bar{a+b} \end{aligned}$$

Autrement dit, $\bar{a} + \bar{b} = \overline{a+b}$.

Remarque. L'écriture d'un élément \bar{a} n'est pas unique ($\bar{a} = \bar{a'}$ si $a \sim a'$).

Il faut vérifier que l'opération $+$ est correctement définie (définie sans ambiguïté).

Autrement dit, si $\bar{a} = \bar{a'}$ et $\bar{b} = \bar{b'}$, on veut montrer que $\bar{a} + \bar{b} = \bar{a'} + \bar{b'}$.

Cours 10

Rappel.

- Relation d'équivalence (\sim) \rightarrow partition en classes d'équivalence ($\bar{a} = \{b \mid b \sim a\}$).
- Équivalence (congruence) mod m (sur \mathbb{Z}) :

$$\begin{aligned} a \sim b &\Leftrightarrow m \mid a - b \\ &\Leftrightarrow \exists k \in \mathbb{Z} \text{ t.q. } a - b = km \end{aligned}$$

On note l'ensemble des classes d'équivalence mod m par $\mathbb{Z}_m = \{\bar{a} \mid a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \dots, \bar{m-1}\}$.

On veut définir une opération $+$ sur \mathbb{Z}_m par $\bar{a} + \bar{b} = \overline{a+b}$.

On doit vérifier que cette définition n'est pas ambiguë (ne dépend pas des représentants).

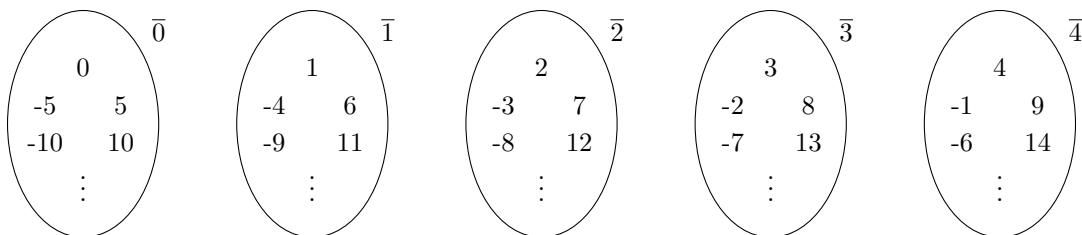
Supposons $\bar{a} = \bar{a'}$ et $\bar{b} = \bar{b'}$. On doit vérifier que $\overline{a_1 + b_1} = \overline{a_2 + b_2}$, c'est-à-dire que $a_1 + b_1 \sim a_2 + b_2$.

Les hypothèses donnent : $a_1 - a_2 = k_a m$ et $b_1 - b_2 = k_b m$. En additionnant ces deux équations, on obtient $(a_1 - a_2) + (b_1 - b_2) = k_a m + k_b m$. Alors, $(a_1 + b_1) - (a_2 + b_2) = (k_a + k_b)m$. Donc, $a_1 + b_1 \sim a_2 + b_2$.

□

Remarque. On doit faire ce genre de preuve pour chaque définition de fonction/opération qui ont comme domaine des classes d'équivalence.

Exemple. $m = 5$.



Pour faire $\bar{2} + \bar{1}$, on peut prendre $\overline{2+1} = \bar{2}$, ou bien $\overline{17 + (-4)} = \bar{13}$.

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

Démonstration.

(A) Soient $a, b, c \in \mathbb{Z}_m$.

$$\begin{aligned} (\bar{a} + \bar{b}) + \bar{c} &= \overline{\bar{a} + \bar{b}} + \bar{c} \\ &= \overline{(\bar{a} + \bar{b}) + c} \\ &= \overline{\bar{a} + (\bar{b} + \bar{c})} \\ &= \overline{\bar{a}} + \overline{\bar{b} + \bar{c}} \\ &= \bar{a} + (\bar{b} + \bar{c}) \end{aligned}$$

(C) $\bar{a} + \bar{b} = \overline{\bar{a} + \bar{b}} = \overline{\bar{b} + \bar{a}} = \bar{b} + \bar{a}$.

(N) $\bar{0} + \bar{a} = \overline{\bar{0} + \bar{a}} = \bar{a}$, donc $\bar{0}$ est neutre. Par commutativité, la propriété est satisfaite.

(I) $\bar{a} + \overline{-\bar{a}} = \overline{\bar{a} - \bar{a}} = \bar{0}$, donc $\overline{-\bar{a}}$ est l'inverse de \bar{a} . Par commutativité, la propriété est satisfaite.

On peut donc écrire $-\bar{a} = \overline{-a}$.

□

Ordre et groupes cycliques

Définition. Soient G un groupe et $a \in G$.

L'*ordre* de a , noté $o(a)$ est la plus petite quantité positive $k \in \mathbb{N}_*$ t.q. $a^k = e$, si elle existe. Sinon, on note $o(a) = \infty$.

Exemple.

- $o(e) = 1$
- Dans \mathbb{D}_3
 - $o(\alpha) = 2$
 - $o(\rho) = 3$
- Dans \mathbb{Z}
 - $o(0) = 1$
 - $o(n) = \infty, \forall n \neq 0$
- Dans \mathbb{Z}_6
 - $o(\bar{2}) = 3$

Proposition. Soit $m \in \mathbb{Z}$. $a^m = e$, si, et seulement si, $o(a) \mid m$.

Démonstration.

(\Rightarrow) Supposons $a^m = e$.

On divise m par $o(a)$: $m = q \cdot o(a) + r$, avec $0 \leq r < o(a)$.

Si $r = 0$, $o(a) \mid m$ et on a terminé.

Supposons que $0 < r < o(a)$, alors

$$\begin{aligned} r &= m - q \cdot o(a) \\ a^r &= a^{m-q \cdot o(a)} \\ &= a^m \cdot a^{-q \cdot o(a)} \\ &= e \cdot (a^{o(a)})^{-q} \\ &= e \cdot e^{-q} \\ &= e \end{aligned}$$

mais $0 < r < o(a)$ contredit la minimalité de $o(a)$.

□

Cours 11

Rappel.

- $a \sim b \Leftrightarrow m \mid a - b$ est une relation d'équivalence sur \mathbb{Z} .
- $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ sont les classes d'équivalence.
- $(\mathbb{Z}_m, +)$ est un groupe, où $\overline{a} + \overline{b} = \overline{a+b}$.
- $o(a) = \min\{k \in \mathbb{N}_* \mid a^k = e\}$ ordre de a . Si $a^k \neq e$, $\forall k > 0$, $o(a) = \infty$.
- Si $a^k = e$, $o(a) \mid k$.

Exemple.

$$M = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \in GL(2, \mathbb{R}).$$

$$\begin{aligned} M^2 &= \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} & M^4 &= -M \\ M^3 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} & M^5 &= - \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \\ &= - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & M^6 &= \left(- \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \left(- \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \\ & & &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Ainsi, $o(M) = 6$, puisque $M^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Chapitre 6 Groupes (suite)

Section 6.13 Groupes symétriques S_n

Rappel. $S(E) = \{f : E \rightarrow E \mid f \text{ est bijective}\}$.

$S(E)$ est un groupe lorsque muni de l'opération \circ .

1_E est l'élément neutre.

f^{-1} est l'élément inverse de f .

$S(E)$ s'appelle le *groupe symétrique* de l'ensemble E .

Remarque.

$E = \{\text{rouge, orange, jaune, vert, bleu, indigo, violet}\}$.

$$S(E) \ni f : \begin{cases} \text{rouge} & \mapsto \text{jaune} \\ \text{jaune} & \mapsto \text{rouge} \\ \text{autres} & \mapsto \text{elles-mêmes} \end{cases}.$$

Le groupe $S(E)$ est isomorphe au groupe $S(\{1, 2, 3, 4, 5, 6, 7\})$, en numérotant les éléments.

Définition. $S_n = S(\{1, 2, \dots, n\})$ le groupe symétrique de n éléments.

Les éléments de S_n sont des bijections, aussi appelées permutations.

Notation. On note une permutation σ de la manière suivante :

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

Exemple.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \iff \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 4 \\ 4 \mapsto 3 \end{array}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \implies \sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \sigma$$

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

$$\eta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \eta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

L'élément neutre est $e = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$.

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} \cong \mathbb{Z}_2.$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \cong \mathbb{D}_3.$$

Remarque. Tous les élément de S_3 donnent des isométries du triangle, mais pas tous les éléments de S_4 donnent des isométries du carré.

Proposition. S_n contient $n!$ éléments.

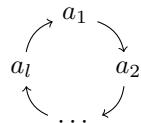
idée.

$$\begin{array}{ccccccc} 1 & & 2 & & 3 & & n \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ n \text{ choix} & n-1 \text{ choix} & n-2 \text{ choix} & \cdots & 1 \text{ choix} & & \end{array}$$

Ainsi, $n(n-1)(n-2) \cdots 1 = n!$.

#

Définition. Un *cycle* est une permutation de la forme $a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_l \rightarrow a_1$, où $a_i \neq a_j$ quand $i \neq j$.



Exemple. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ est un cycle de longueur $l = 3$.

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$ est un cycle de longueur $l = 3$.

Notation. Écriture raccourcie pour un cycle : $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \ 2 \ 3)$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} = (2 \ 4 \ 5) \in S_5$.

Proposition. L'ordre d'un cycle est égal à sa longueur.

Démonstration.

Si le cycle σ permute les éléments a_i comme $\sigma = a_1 \xrightarrow{\sigma} a_2 \xrightarrow{\sigma} \cdots \xrightarrow{\sigma} a_l \xrightarrow{\sigma} a_1$.
Alors, calculons σ^l

$$\left(\begin{array}{cccccc} a_1 & a_2 & a_3 & \cdots & a_l \\ a_2 & a_3 & a_4 & \cdots & a_1 \\ a_3 & a_4 & a_5 & \cdots & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_l & a_1 & a_2 & \cdots & a_{l-1} \\ a_1 & a_2 & a_3 & \cdots & a_l \end{array} \right)$$

Ainsi, $\sigma^l = e$.

□

Exemple. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ n'est pas un cycle.

Cependant, σ se décompose en cycles $\sigma = \sigma_1 \circ \sigma_2$, où $\sigma_1 = (1 \ 2)$, $\sigma_2 = (3 \ 4)$.

Proposition. Toute permutation $\sigma \in S_n$ s'écrit de manière unique comme une composition de cycles disjoints. (les cycles sont uniques, mais pas l'ordre de l'écriture).

Notation. Des cycles disjoints sont des cycles de supports disjoints, où le support d'un cycle est $\text{supp}(\sigma) \{ i \mid \sigma(i) \neq i \}$.

Lemme. Les cycles disjoints commutent entre eux.

Exemple.

$$(1 \ 4 \ 5) \circ (2 \ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} = (2 \ 3) \circ (1 \ 4 \ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$$

Démonstration.

Soient $\sigma = (a_1 \ a_2 \ \cdots \ a_l)$ et $\eta = (b_1 \ b_2 \ \cdots \ b_k)$ deux cycles disjoints.

Soit $i \in \{1, 2, \dots, n\}$.

Il y a trois cas :

(1) $i \in \text{supp}(\sigma), i \notin \text{supp}(\eta)$.

$$\begin{aligned}\sigma \circ \eta(i) &= \sigma(i) \\ \eta \circ \sigma(i) &= \sigma(i)\end{aligned}$$

(2) $i \notin \text{supp}(\sigma), i \in \text{supp}(\eta)$.

$$\begin{aligned}\sigma \circ \eta(i) &= \eta(i) \\ \eta \circ \sigma(i) &= \eta(i)\end{aligned}$$

(3) $i \notin \text{supp}(\sigma), i \notin \text{supp}(\eta)$.

$$\begin{aligned}\sigma \circ \eta(i) &= i \\ \eta \circ \sigma(i) &= i\end{aligned}$$

□

idée de la démonstration. Par récurrence.

$n = 2, (1 \ 2)$.

Si vrai pour toutes les permutations de longueur $\leq n$.

σ permutation de $n + 1$ éléments.

On prend $i \in \text{supp}(\sigma)$.

$$\underbrace{i \rightarrow \sigma(i) \rightarrow \sigma^2(i) \rightarrow \sigma^3(i) \rightarrow \cdots \rightarrow \sigma^n(i)}_{n+1 \text{ éléments de } \{1, 2, \dots, n\}}$$

ces éléments ne peuvent pas tous être distincts.

$\exists m_1 > m_2$ t.q. $\sigma^{m_1}(i) = \sigma^{m_2}(i)$, donc $\sigma^{m_1-m_2}(i) = i$.

Alors, $i \rightarrow \sigma(i) \rightarrow \sigma^2(i) \rightarrow \cdots \rightarrow \sigma^{m_1-m_2-1}(i) \rightarrow i$ est un cycle.

Les éléments restants $\{1, 2, \dots, n\} \setminus \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{m_1-m_2-1}(i)\}$ sont permutés entre eux par σ .

Utiliser l'hypothèse de récurrence.

#

Exemple.

•

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

•

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 2 & 8 & 3 & 1 & 5 & 6 \end{pmatrix} = (1 \ 4 \ 8 \ 6) (2 \ 7 \ 5 \ 3)$$

Proposition. L'ordre d'une permutation σ est le ppcm des longueurs des cycles dans sa décomposition.

Démonstration. $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$, où σ_i sont des cycles de longueur l_i .

Puisque les cycles disjoints commutent, $\sigma^m = (\sigma_1 \sigma_2 \cdots \sigma_k)^m = \sigma_1^m \sigma_2^m \cdots \sigma_k^m$.

$\sigma_1^m \sigma_2^m \cdots \sigma_k^m = e$, si, et seulement si, $\sigma_1^m = e, \sigma_2^m = e, \dots, \sigma_k^m = e$.

Alors, $o(\sigma_1) \mid m, o(\sigma_2) \mid m, \dots, o(\sigma_k) \mid m$.

Donc, $l_i \mid m, \forall i$.

L'ordre de σ m est le plus petit multiple des l_i .

□

Cours 12

Rappel.

- $S_n = S(\{1, 2, \dots, n\}) = \{\sigma \mid \sigma \text{ est une bijection de } \{1, 2, \dots, n\}\}$ est un groupe pour \circ .

- Notations : $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$

Cycle : $(a_1 \ a_2 \ \cdots \ a_l)$

- $o(a_1 \ a_2 \ \cdots \ a_l) = l$

- Toute permutation de S_n s'écrit comme un produit (composition) de cycles disjoints uniques

- Les cycles disjoints commutent
- Si $\sigma = \sigma_1 \cdots \sigma_k$ est la décomposition, $o(\sigma) = \text{ppcm}(l_1, \dots, l_k)$, où l_k est la longueur de σ_k

Exemple.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 4 & 3 & 7 & 8 & 6 \end{pmatrix} = (1 \ 2) \circ (3 \ 5) \circ (6 \ 7 \ 8)$$

$$o(\sigma) = \text{ppcm}(2, 2, 3) = 6.$$

$$\sigma^2 = (1 \ 2)^2 \circ (3 \ 5)^2 \circ (6 \ 7 \ 8)^2 = (6 \ 7 \ 8)^2 = (6 \ 8 \ 7)$$

Définition. Le *signe* d'une permutation $\sigma \in S_n$ est le nombre

$$\text{sgn}(\sigma) = \prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Exemple.

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

$$\begin{aligned} \text{sgn}(\sigma) &= \left(\frac{3 \rightarrow 4}{1 \rightarrow 2} \right) \left(\frac{3 \rightarrow 1^{-1}}{1 \rightarrow 3} \right) \left(\frac{3 \rightarrow 2^{-1}}{1 \rightarrow 4} \right) \left(\frac{4 \rightarrow 1^{-1}}{2 \rightarrow 3} \right) \left(\frac{4 \rightarrow 2^{-1}}{2 \rightarrow 4} \right) \left(\frac{1 \rightarrow 2}{3 \rightarrow 4} \right) \\ &= (-1)^4 = 1 \end{aligned}$$

Remarque. Chaque terme $(i - j)$ apparaît au dénominateur et au numérateur, à signe près, donc $\text{sgn}(\sigma) \in \{-1, 1\}$.

Proposition. Soient $\alpha, \beta \in S_n$, alors $\text{sgn}(\alpha \circ \beta) = \text{sgn}(\alpha) \cdot \text{sgn}(\beta)$.

Démonstration.

$$\begin{aligned} \text{sgn}(\alpha \circ \beta) &= \prod_{i < j} \frac{\alpha(\beta(i)) - \alpha(\beta(j))}{i - j} \\ &= \prod_{i < j} \left(\frac{\alpha(\beta(i)) - \alpha(\beta(j))}{i - j} \right) \left(\frac{\beta(i) - \beta(j)}{\beta(i) - \beta(j)} \right) \\ &= \prod_{i < j} \frac{\alpha(\beta(i)) - \alpha(\beta(j))}{\beta(i) - \beta(j)} \cdot \prod_{i < j} \frac{\beta(i) - \beta(j)}{i - j} \\ &= \left(\prod_{i < j} \frac{\alpha(\beta(i)) - \alpha(\beta(j))}{\beta(i) - \beta(j)} \right) \cdot \text{sgn}(\beta) \\ &= \text{sgn}(\alpha) \cdot \text{sgn}(\beta) \end{aligned}$$

□

Définition. Un cycle longueur 2 s'appelle une *transposition*.

Remarque. On peut décomposer un cycle en un produit de transposition :

$$(a_1 \ a_2 \ \cdots \ a_l) = (a_1 \ a_l) \circ (a_1 \ a_{l-1}) \circ \cdots \circ (a_1 \ a_2)$$

Exemple.

$$\sigma = (2 \ 3 \ 5 \ 6 \ 8)$$

$$(2 \ 8) \circ (2 \ 6) \circ (2 \ 5) \circ (2 \ 3) (2) = 3 \quad (2)$$

$$\begin{aligned} (2 \ 8) \circ (2 \ 6) \circ (2 \ 5) \circ (2 \ 3) (3) &= (2 \ 8) \circ (2 \ 6) \circ (2 \ 5) (2) \\ &= 5 \end{aligned} \quad (3)$$

$$\begin{aligned} (2 \ 8) \circ (2 \ 6) \circ (2 \ 5) \circ (2 \ 3) (5) &= (2 \ 8) \circ (2 \ 6) \circ (2 \ 5) (5) \\ &= (2 \ 8) \circ (2 \ 6) (2) \\ &= 6 \end{aligned} \quad (5)$$

$$\begin{aligned} (2 \ 8) \circ (2 \ 6) \circ (2 \ 5) \circ (2 \ 3) (6) &= (2 \ 8) \circ (2 \ 6) \circ (2 \ 5) (6) \\ &= (2 \ 8) \circ (2 \ 6) (6) \\ &= (2 \ 8) (2) \\ &= 8 \end{aligned} \quad (6)$$

$$\begin{aligned} (2 \ 8) \circ (2 \ 6) \circ (2 \ 5) \circ (2 \ 3) (8) &= (2 \ 8) \circ (2 \ 6) \circ (2 \ 5) (8) \\ &= (2 \ 8) \circ (2 \ 6) (8) \\ &= (2 \ 8) (8) \\ &= 2 \end{aligned} \quad (8)$$

$$(2 \ 8) \circ (2 \ 6) \circ (2 \ 5) \circ (2 \ 3) = (2 \ 3 \ 5 \ 6 \ 8)$$

Alors, $\text{sgn}(\sigma) = \text{sgn}((2 \ 8) \circ (2 \ 6) \circ (2 \ 5) \circ (2 \ 3)) = (-1)^4 = 1$.

Proposition. *Le signe d'une transposition est -1 .*

Démonstration. par exemple

$$(2 \ 4) \in S_4.$$

$$\begin{aligned} \text{sgn}(\sigma) &= \left(\frac{\begin{array}{c} 1 \rightarrow 4 \\ 1 \rightarrow 2 \end{array}}{\begin{array}{c} 1 \rightarrow 2 \\ 1 \rightarrow 3 \end{array}} \right) \left(\frac{\begin{array}{c} 1 \rightarrow 3 \\ 1 \rightarrow 4 \end{array}}{\begin{array}{c} 2 \rightarrow 3 \\ 2 \rightarrow 4 \end{array}} \right) \left(\frac{\begin{array}{c} 1 \rightarrow 2 \\ 4 \rightarrow 3^{-1} \end{array}}{\begin{array}{c} 2 \rightarrow 4 \\ 3 \rightarrow 4 \end{array}} \right) \left(\frac{\begin{array}{c} 4 \rightarrow 2^{-1} \\ 2 \rightarrow 3 \end{array}}{\begin{array}{c} 2 \rightarrow 4 \\ 3 \rightarrow 4 \end{array}} \right) \\ &= (-1)^3 = -1 \end{aligned}$$

#

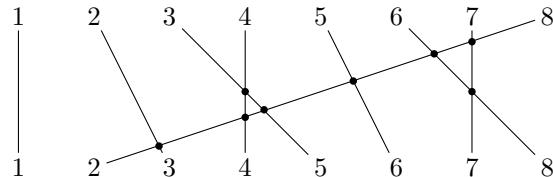
Proposition. *Le signe d'un cycle de longueur l est*

- 1 si l est impair
- -1 si l est pair

Plus généralement, le signe d'une permutation σ est $(-1)^\gamma$, où γ est le nombre de transpositions dans une décomposition de σ en transpositions.

Remarque. Une autre façon de calculer le signe d'une permutation.

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



Connecter chaque élément, compter les intersections des segments, $\text{sgn}(\sigma) = (-1)^\gamma$, où γ est le nombre d'intersections. Ici, $\text{sgn}(\sigma) = (-1)^8 = 1$.

Chapitre 8 Homomorphismes

Cours 13

Définition. Soient G, H deux groupes et $f : G \rightarrow H$.

On dit que f est un *homomorphisme* (ou morphisme de groupes) si $f(ab) = f(a)f(b)$, $\forall a, b \in G$.

Exemple.

- (1) Tous les isomorphismes sont des morphismes.
- (2) $f : G \rightarrow H$, $a \mapsto e_H$ est toujours un homomorphisme.
En effet, $f(ab) = e_H = e_H e_H = f(a)f(b)$.
 f n'est pas un isomorphisme, sauf si $G = H = \{e\}$.
- (3) $\text{sgn} : S_n \rightarrow \{-1, 1\} = C_2$.
 $\text{sgn}(\alpha \circ \beta) = \text{sgn}(\alpha) \cdot \text{sgn}(\beta)$, donc sgn est un homomorphisme.
- (4) $\det : GL(n, \mathbb{R}) \rightarrow \mathbb{R}_*$ est un homomorphisme, car $\det(AB) = \det(A) \cdot \det(B)$.
- (5) Pour un $m \in \mathbb{Z}$ fixé, $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(n) = m \cdot n$ est un homomorphisme.
En effet, $f(n_1 + n_2) = m(n_1 + n_2) = mn_1 + mn_2 = f(n_1) + f(n_2)$.
- (6) Si $H \leqslant G$, $i : H \rightarrow G$, $i(x) = x$ est un homomorphisme.
Ce n'est pas $\mathbb{1}$, car $H \neq G$ en général.

Proposition.

Si $f : G \rightarrow H$ est un homomorphisme, alors

- (1) $f(e_G) = e_H$
- (2) $f(a^{-1}) = f(a)^{-1}$

Démonstration.

(1)

$$\begin{aligned} f(e_G) &= f(e_G e_G) \\ &= f(e_G) f(e_G) \\ f(e_G)^{-1} f(e_G) &= f(e_G)^{-1} f(e_G) f(e_G) \\ e_H &= e_H f(e_G) \\ &= f(e_G) \end{aligned}$$

(2) $f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H$, donc $f(a^{-1}) = f(a)^{-1}$.

□

Proposition.

La composition de deux homomorphismes est un homomorphisme.

Démonstration.

Soient $f : G \rightarrow H$ et $g : H \rightarrow K$ deux homomorphismes, et $a, b \in G$.

$$\begin{aligned}(g \circ f)(ab) &= g(f(ab)) \\ &= g(f(a)f(b)) \\ &= g(f(a))g(f(b)) \\ &= (g \circ f)(a)(g \circ f)(b)\end{aligned}$$

□

Proposition. Soit $f : G \rightarrow H$ un homomorphisme. Alors,

- (1) $\text{Im}(f) = \{f(a) \mid a \in G\}$ est un sous-groupe de H ;
- (2) le noyau $\ker(f) = \{a \in G \mid f(a) = e\}$ est un sous-groupe de G .

Exemple.

$$(a) \text{ Im}(\det) = \mathbb{R}_*, \det \begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} = x$$

$$\ker(\det) = \{M \in GL(n, \mathbb{R}) \mid \det(M) = 1\} = SL(n, \mathbb{R}).$$

- (b) $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(n) = mn$.

$$\text{Im}(f) = m\mathbb{Z} \leqslant \mathbb{Z}$$

$$\ker(f) = \begin{cases} \mathbb{Z} & \text{si } m = 0 \\ \{0\} & \text{sinon} \end{cases}$$

Démonstration.

- (1) $f(e_G) \in \text{Im}(f)$, donc $\text{Im}(f) \neq \emptyset$.

Si $a, b \in \text{Im}(f)$, alors $a = f(c)$ et $b = f(d)$.

On a alors

$$\begin{aligned}ab^{-1} &= f(c)f(d)^{-1} \\ &= f(c)f(d^{-1}) \\ &= f(cd^{-1}) \in \text{Im}(f)\end{aligned}$$

- (2) $f(e_G) = e_H \Rightarrow f(e_G) \in \ker(f) \Rightarrow \ker(f) \neq \emptyset$.

Soient $a, b \in \ker(f)$. Alors, $f(a) = e_H$ et $f(b) = e_H$.

$$\begin{aligned}f(ab^{-1}) &= f(a)f(b^{-1}) \\ &= f(a)f(b)^{-1} \\ &= e_H e_H^{-1} \\ &= e_H\end{aligned}$$

donc $ab^{-1} \in \ker(f)$.

□

Exemple.

$$\text{Im}(\text{sgn}) = C_2 = \{-1, 1\}, \text{ si } n \geqslant 1.$$

$$\ker(\text{sgn}) = \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\} \text{ est un sous-groupe de } S_n.$$

Notation. On note ce sous-groupe A_n et on l'appelle le *groupe alterné*.

Exemple. $n = 3$.

$$A_3 = \{e, (123), (132)\}.$$

Proposition.

Soit $f : G \rightarrow H$ un morphisme.

$\ker(f) = \{e\}$ si, et seulement si, f est injective.

Démonstration.

(\Leftarrow) Supposons que f est injective.

On sait que $e_G \in \ker(f)$.

Supposons que $\exists a \in \ker(f)$. On a

$$\begin{aligned} f(a) &= e_H && \text{par définition de } \ker \\ &= f(e_G) \\ a &= e_G && \text{car } f \text{ est injective} \end{aligned}$$

Donc, $\ker(f) = \{e_G\}$.

(\Rightarrow) Supposons que $\ker(f) = \{e_G\}$.

Soient $a, b \in G$ t.q. $f(a) = f(b)$.

$$\begin{aligned} f(a) &= f(b) \\ f(a)f(b)^{-1} &= e_H \\ f(a)f(b^{-1}) &= e_H \\ f(ab^{-1}) &= e_H \\ ab^{-1} &= e_G \\ a &= b \end{aligned}$$

□

Remarque. $\text{Im}(f) = H$ si, et seulement si, f est surjective.

Cours 14

Rappel.

- homomorphisme : $f : G \rightarrow H$ t.q. $f(ab) = f(a)f(b)$
- Si f est un homomorphisme, alors
 - $f(e_G) = e_H$
 - $f(a^{-1}) = f(a)^{-1}$
 - $f(a^n) = f(a)^n$
- $\text{Im}(f) = \{f(a) \mid a \in G\} \leqslant H$
- $\ker(f) = \{a \in G \mid f(a) = e_H\} \leqslant G$
- $\ker(f) = \{e_G\} \Leftrightarrow f$ est injective

Exemple.

$$\begin{array}{rcl} f : \mathbb{Z} & \rightarrow & \mathbb{Z}_m \\ n & \mapsto & \bar{n} \end{array} \text{ est un homomorphisme.}$$

En effet,

$$\begin{aligned} f(n_1 + n_2) &= \overline{n_1 + n_2} \\ &= \overline{n_1} + \overline{n_2} \\ &= f(n_1) + f(n_2) \end{aligned}$$

$$\text{Im}(f) = \mathbb{Z}_m.$$

$$\ker(f) = m\mathbb{Z}.$$

Équivalence modulo H et théorème de Lagrange

G un groupe quelconque et $H \leq G$ un sous-groupe.

On définit une relation sur G par $a \sim b$ si, et seulement si, $ab^{-1} \in H$.

Cette relation est appelée *équivalence modulo H* .

Proposition.

\sim est une relation d'équivalence.

Démonstration.

(refl) Soit $a \in G$.

$aa^{-1} = e_G \in H$, puisque $H \leq G$.

Alors, $a \sim a$.

(sym) Soient $a, b \in G$.

Supposons que $a \sim b$.

Alors, $ab^{-1} \in H$.

Comme H est un groupe, H est fermé pour la prise d'inverses, donc $(ab^{-1})^{-1} = ba^{-1} \in H$.

Ainsi, $b \sim a$.

(trans) Soient $a, b, c \in G$.

Supposons que $a \sim b$ et $b \sim c$.

Alors, $ab^{-1} \in H$ et $bc^{-1} \in H$.

Comme H est un groupe, H est fermé pour son opération, donc $(ab^{-1})(bc^{-1}) = a(bb^{-1})c^{-1} = ac^{-1} \in H$.

Ainsi, $a \sim c$.

□

Le groupe G se partitionne en classes d'équivalence modulo H : $G = \bar{a}_1 \cup \bar{a}_2 \cup \dots$

Exemple.

$G = \mathbb{Z}_8$, $H = \{\bar{0}, \bar{4}\}$.

La classe de $\bar{0} \in G \pmod{H}$ est l'ensemble des $\bar{n} \in \mathbb{Z}_8$ t.q. $\bar{0} - \bar{n} \in H$.

Alors, $-\bar{n} \in \{\bar{0}, \bar{4}\}$, donc $\bar{n} = \bar{0}$ ou $\bar{n} = \bar{4}$.

$C(\bar{0}) = \{\bar{0}, \bar{4}\}$, $C(\bar{1}) = \{\bar{1}, \bar{5}\}$, $C(\bar{2}) = \{\bar{2}, \bar{6}\}$, $C(\bar{3}) = \{\bar{3}, \bar{7}\}$.

Lemme.

La classe modulo H de $a \in G$ est $\{ha \mid h \in H\}$.

Notation.

$\{ha \mid h \in H\}$ est noté Ha .

Démonstration.

Soient $a, b \in G$.

(\subseteq) Supposons que $b \sim a \pmod{H}$, c'est-à-dire $b \in \bar{a}$.

Alors, $ba^{-1} \in H$, disons $ba^{-1} = h$ avec $h \in H$, donc $b = ha$.

$\therefore \bar{a} \subseteq Ha$.

(\supseteq) Supposons que $b \in Ha$.

Alors, $b = ha$ avec $h \in H$, donc $ba^{-1} = h \in H$. Ainsi, $b \sim a$, donc $b \in \bar{a}$.

$\therefore Ha \subseteq \bar{a}$.

Ainsi, $Ha = \bar{a}$.

□

Corollaire.

Toutes les classes d'équivalence modulo H ont le même nombre d'éléments.

Plus précisément, $|Ha| = |H|$.

Démonstration.

$f : H \rightarrow Ha$ est bijective, car elle est inversible d'inverse $f^{-1} : Ha \rightarrow H$ $b \mapsto ba^{-1}$.

□

Cours 15

Rappel. Pour déterminer $\ker(f)$ et $\text{Im}(f)$ d'un homomorphisme f .

Exemple. $f : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_6$.
 $\bar{n} \mapsto \bar{n}$.

$$\ker(f) = \{a \in G \mid f(a) = e\}.$$

Supposons que $\bar{n} \in \ker(f)$. Alors,

$$\begin{aligned} f(\bar{n}) &= \bar{0} \\ \bar{n} &= \bar{0} \\ n &= 6k \end{aligned}$$

avec $k \in \mathbb{Z}$. Donc, $\ker(f) \subseteq 6\mathbb{Z}_{12}$.

Pour avoir $\ker(f) = 6\mathbb{Z}_{12}$, il faut aussi montrer $6\mathbb{Z}_{12} \subseteq \ker(f)$.

Supposons que $n = 6k \Rightarrow \bar{n} = \bar{6k} \Rightarrow f(\bar{n}) = f(\bar{6k}) = \bar{6k} = \bar{0}$, donc $\bar{n} \in \ker(f)$.

Rappel.

G groupe, $H \leqslant G$ sous-groupe.

- Équivalence mod H :
- $a \sim b \Leftrightarrow ab^{-1} \in H$;
- Les classes d'équivalence mod H sont $\bar{a} = Ha = \{ha \mid h \in H\}$;
- Toutes les classes ont la même taille, $|Ha| = |H|$.

Exemple.

$G = S_3 = \{e, (1 \ 2), (1 \ 3), (2 \ 3), (1 \ 2 \ 3), (1 \ 3 \ 2)\}$, $H = \{e, (1 \ 2)\}$.
Calculons les classes mod H .

- $He = \{e \circ e, (1 \ 2) \circ e\} = H$;
- $H(1 \ 3) = \{e \circ (1 \ 3), (1 \ 2) \circ (1 \ 3)\} = \{(1 \ 3), (1 \ 3 \ 2)\}$;
- $H(2 \ 3) = \{e \circ (2 \ 3), (1 \ 2) \circ (2 \ 3)\} = \{(2 \ 3), (1 \ 2 \ 3)\}$.

Théorème (Lagrange).

Soit G un groupe fini.

Si $H \leqslant G$, alors $|H| \mid |G|$.

Démonstration.

Les classes modulo H partitionnent G est sous-ensembles (classes) de taille $|H|$ chacun, donc

$$\begin{aligned} G &= Ha_1 \cup Ha_2 \cup \cdots \cup Ha_n \\ |G| &= |H| + |H| + \cdots + |H| \\ &= n|H| \end{aligned}$$

□

Corollaire. $a \in G$, $o(a) \mid |G|$.

Démonstration.

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, le sous-groupe engendré par a , est un sous-groupe car

- $a^0 = e \in \langle a \rangle$, donc $\langle a \rangle \neq \emptyset$;
- Si $a^n, a^m \in \langle a \rangle$, alors $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$, donc $\langle a \rangle \leqslant G$.

Par le théorème de Lagrange, $|\langle a \rangle| \mid |G|$.

De plus, $|\langle a \rangle| = o(a)$, qu'on démontrera plus tard, donc $o(a) \mid |G|$. □

Corollaire. Si $|G| = m$ et $a \in G$, alors $a^m = e$.

Démonstration.

On sait que $a^{o(a)} = e$.

Par le corollaire précédent, $m = ko(a)$, car $o(a) \mid m$, donc $a^m = a^{ko(a)} = (a^{o(a)})^k = e^k = e$. □

Corollaire (petit théorème de Fermat). *Si $a \in \mathbb{Z}$ et p est un nombre premier t.q. $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$.*

Lemme. \mathbb{Z}_{p_*} est un groupe pour la multiplication.

Démonstration.

\mathbb{Z}_{p_*} est un groupe avec $|\mathbb{Z}_{p_*}| = p - 1$.

Par le corollaire précédent, si $a \in \mathbb{Z}_{p_*}$, alors $\bar{a}^{p-1} = \bar{1}$, donc $a^{p-1} \equiv 1 \pmod{p}$. \square

Notation. $|G|$ s'appelle aussi l'*ordre* de G .

Définition. $H \leq G$.

On appelle *indice* de H dans G le nombre de classes modulo H et on le note $[G : H]$.

Le théorème de Lagrange implique que si G est fini, $[G : H] = \frac{|G|}{|H|}$.

L'indice peut être fini même si G et H sont infinis.

Exemple. $[\mathbb{Z} : m\mathbb{Z}] = m$.

Exemple. Les seuls sous-groupes de \mathbb{Z}_p avec p premier sont $\{\bar{0}\}$ et \mathbb{Z}_p , car si $H \leq \mathbb{Z}_p$. Par Lagrange, $|H| \in \{1, p\}$.

Exemple. $H \leq \mathbb{Z}_8$ qui contient au moins 5 éléments distincts, alors $H = \mathbb{Z}_8$, car les diviseurs de 8 sont $\{1, 2, 4, 8\}$.

Section 8.6 Groupes quotients

On veut définir une opération sur les classes d'équivalence mod H pour en faire un groupe.

Tentative

On voudrait définir $Ha * Hb = H(a * b)$. Est-ce défini sans ambiguïté?

Supposons que $Ha = Ha'$ et $Hb = Hb'$, c'est-à-dire $a(a')^{-1} \in H$ et $b(b')^{-1} \in H$. Alors, on voudrait montrer que $H(ab) = H(a'b') \Leftrightarrow (ab)(a'b') \in H \Leftrightarrow ab(b')^{-1}(a')^{-1} \in H$. Cependant, ce n'est pas vrai en général.

Définition.

Un sous-groupe $H \leq G$ est *distingué*, ou *normal*, si $\forall a \in G$, $Ha = aH$, c'est-à-dire, $\{ha \mid h \in H\} = \{ah \mid h \in H\}$.

Remarque.

$Ha = aH$ ne veut pas dire $ha = ah$ pour tout $h \in H$.

Plutôt, $Ha = aH$ signifie $ha = ah'$ pour un certain $h' \in H$.

Exemple.

Pour $G = S_3 = \{e, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)\}$.

- Le sous-groupe $H = \{e, (1 2)\}$ n'est pas distingué. En effet, regardons la classe de $(1 3)$.

$$H(1 3) = \{(1 3), (1 3 2)\}$$

$$(1 3)H = \{(1 3) \circ e, (1 3) \circ (1 2)\} = \{(1 3), (1 2 3)\}$$

- Le sous-groupe $N = \{e, (1 2 3), (1 3 2)\}$ est distingué. En effet

$$Ne = \{e \circ e, (1 2 3) \circ e, (1 3 2) \circ e\} = \{e, (1 2 3), (1 3 2)\} = N$$

$$eN = \{e \circ e, e \circ (1 2 3), e \circ (1 3 2)\} = \{e, (1 2 3), (1 3 2)\} = N$$

$$N(1 2) = \{e \circ (1 2), (1 2 3) \circ (1 2), (1 3 2) \circ (1 2)\} = \{(1 2), (1 3), (2 3)\}$$

$$(1 2)N = \{(1 2) \circ e, (1 2) \circ (1 2 3), (1 2) \circ (1 3 2)\} = \{(1 2), (2 3), (1 3)\}$$

Proposition. Si $f : G \rightarrow H$ est un homomorphisme, $\ker(f)$ est un sous-groupe distingué de G .

Démonstration. $\ker(f) = \{a \in G \mid f(a) = e\}$.

Soit $b \in G$. On veut montrer que $b \ker(f) = \ker(f)b$.

(\subseteq) Soit $ba \in b \ker(f)$.

$$ba = bab^{-1}b$$

posons $a' = bab^{-1}$

$$\begin{aligned} f(a') &= f(bab^{-1}) \\ &= f(b)f(a)f(b^{-1}) \\ &= f(b)ef(b^{-1}) \\ &= e \end{aligned}$$

donc $a' \in \ker(f) \Rightarrow ba = a'b \in \ker(f)b \Rightarrow b \ker(f) \subseteq \ker(f)b$.

(\supseteq) Soit $ab \in \ker(f)b$.

$$ab = bb^{-1}ab$$

posons $a' = b^{-1}ab$

$$\begin{aligned} f(a') &= f(b^{-1}ab) \\ &= f(b^{-1})f(a)f(b) \\ &= f(b^{-1})ef(b) \\ &= e \end{aligned}$$

donc $a' \in \ker(f) \Rightarrow ab = ba' \in b \ker(f) \Rightarrow \ker(f)b \subseteq b \ker(f)$.

□

Cours 16

Rappel.

- Classes d'équivalence à droite modulo H de $a \in G : Ha$
- Théorème de Lagrange : $|H| \mid |G|$
- Indice de H dans $G : [G : H]$ représente le nombre de classes
- Corollaires de Lagrange :
 - $o(a) \mid |G|$
 - $a^{|G|} = e$
 - petit théorème de Fermat : si $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$, avec p un nombre premier
- Sous-groupe *normal* ou *distingué* : $Ha = aH$
- $\ker(f)$ est toujours distingué

Proposition.

$H \leqslant G$ est distingué si, et seulement si, pour tous $h \in H$ et $g \in G$, $ghg^{-1} \in H$.

Démonstration.

(\Rightarrow) Supposons que H est distingué.

Soient $h \in H$ et $g \in G$. On a $gh \in gH$. Mais alors, $gh \in Hg$, donc $gh = h'g$ avec $h' \in H$.

$$\begin{aligned} ghg^{-1} &= h'gg^{-1} \\ &= h' \in H \end{aligned}$$

(\Leftarrow) Supposons que $ghg^{-1} \in H, \forall g \in G, \forall h \in H$.

On veut montrer que $gH = Hg, \forall g \in G$.

(\subseteq) Soit $gh \in gH$. On a

$$\begin{aligned} gh &= ghg^{-1}g \\ &= h'g \in Hg \end{aligned}$$

(\supseteq) Soit $hg \in Hg$. Alors

$$\begin{aligned} hg &= gg^{-1}hg \\ &= gh' \in gH \end{aligned}$$

□

Nouvelle tentative

Soit G un groupe. Soit N un sous-groupe normal de G .

On a G/N l'ensemble des classes mod N :

$$G/N = \{Na \mid a \in G\}$$

Proposition.

G/N est un groupe par l'opération $(Na)(Nb) = N(ab)$.

Démonstration.

Montrons que l'opération est définie sans ambiguïté.

Supposons que $Na = Na'$ et $Nb = Nb'$. Alors, $a(a')^{-1} \in N$ et $b(b')^{-1} \in N$.

$$\begin{aligned} ab(a'b')^{-1} &= ab(b')^{-1}(a')^{-1} \\ &= ab(b')^{-1}(a')^{-1}aa^{-1} \end{aligned}$$

On sait que $b(b')^{-1} \in N$.

De plus, $(a')^{-1}a \in N$, car $a(a')^{-1} \in N$ et N est normal, donc $a^{-1}(a(a')^{-1})a \in N$.

Comme N est fermé pour la multiplication, $b(b')^{-1}(a')^{-1}a \in N$ que nous noterons n .

On a donc

$$ab(a'b')^{-1} = ana^{-1} \in N$$

Ainsi, $N(ab) = N(a'b')$, donc l'opération est définie sans ambiguïté.

Maintenant, montrons que G/N est un groupe.

(A) Soient $Na, Nb, Nc \in G/N$.

$$\begin{aligned} (NaNb)Nc &= N(ab)Nc \\ &= N((ab)c) \\ &= N(a(bc)) \\ &= NaN(bc) \\ &= Na(NbNc) \end{aligned}$$

(N) On vérifie que $Ne = N$ est neutre.

$$\begin{aligned} NeNa &= N(ea) \\ &= Na \end{aligned}$$

$$\begin{aligned} NaNe &= N(ae) \\ &= Na \end{aligned}$$

(I) L'inverse de Na est Na^{-1}

$$\begin{aligned} NaNa^{-1} &= N(aa^{-1}) \\ &= N \end{aligned}$$

$$\begin{aligned} Na^{-1}Na &= N(a^{-1}a) \\ &= N \end{aligned}$$

□

Notation. $N \trianglelefteq G$ représente N est un sous-groupe normal de G .

Proposition.

$p : G \rightarrow G/N$ est un homomorphisme.
 $a \mapsto Na$

Démonstration.

$$\begin{aligned} p(ab) &= N(ab) \\ &= NaNb \\ &= p(a)p(b) \end{aligned}$$

□