

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

Julien Houle

Automne 2025

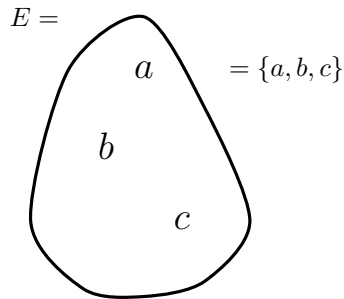
Table des matières

1	Ensembles	1
	Manières de définir une fonction	1
6	Groupes	8
	Propriétés élémentaires des groupes	9
	Produit cartésien de groupes	11
	Isomorphismes de groupes	11
	Puissances d'éléments de groupes	13
	Sous-groupes	16
2		19
	2.4 Relations d'équivalence	19

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

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 $x \in F$
- $E = F$ ssi $E \subseteq F$ 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
- $\mathbb{1}$ $\mathbb{1}_E : E \rightarrow E$ est définie comme $\mathbb{1}_E(x) = x$

Manières de définir une fonction

- énumérer $f(x)$ pour chaque $x \in E$
- donner une formule
une formule ne définit pas tjrs 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 $g(y) = y - 1$

démo.

On vérifie que

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

□

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

démo.

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

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

□

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). $g \circ f = \mathbb{1}_E$

$$f \circ g = \mathbb{1}_F$$

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

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

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

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

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

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

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 $f(x) = f(y) = |y| = y$.

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

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 $f(x) = 0$, $x + 1 = 0$, $x = -1$, $x \notin \mathbb{N}$.

$f : \mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto 2x + 3$.

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.

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

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

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 $x \in A \mapsto c$.

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 ssi elle est inversible.

démo.

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

\Rightarrow :

Supposons f est injective et surjective.

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

démo.

Existence : Comme f est surjective, x existe.

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

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 $g(\underbrace{f(x)}_y) = x$, 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. $E = \mathbb{Z}$,

$$\begin{aligned} m : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (n, m) &\longmapsto n + m \end{aligned}$$

$$\begin{aligned} m : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (n, m) &\longmapsto n \cdot m \end{aligned}$$

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

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
$$\begin{array}{ccc} * : & E \times E & \rightarrow E \\ & (x, y) & \mapsto z \end{array}$$
- 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 $+$.

$$0 + n = n$$

$$n + 0 = n$$

- 1 est neutre pour \times .

$$1 \times n = n$$

$$n \times 1 = n$$

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 $-1 = 1$.

4

- Sur l'ensemble $E = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$, 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. $A = \{0, 1\}$

$$f_1 : \begin{array}{c} 0 \mapsto 0 \\ 1 \mapsto 0 \end{array}, f_2 : \begin{array}{c} 0 \mapsto 0 \\ 1 \mapsto 1 \end{array}, f_3 : \begin{array}{c} 0 \mapsto 1 \\ 1 \mapsto 0 \end{array}, f_4 : \begin{array}{c} 0 \mapsto 1 \\ 1 \mapsto 1 \end{array} \quad \text{On a } f_2 = \mathbb{1}_A.$$

\circ	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

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

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,

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

□

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 $a \in A$.

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

□

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).

- 1. $GL(n, \mathbb{R})$ 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
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.
- 2. A un ensemble quelconque
 $S(A) = \{f : A \rightarrow A | f \text{ est bijective}\}$ est un groupe pour \circ .
Neutre : 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

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

démonstration.

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

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

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

- (d) 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.

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

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

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$+$ 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.

$\mathbb{D}_3 = \left\{ \begin{array}{l} \varepsilon \text{ 'identité', } \alpha \text{ 'réflexion par rapport à la verticale', } \beta \text{ 'réflexion par rapport à /', } \gamma \text{ 'réflexion par rapport à \', } \rho \text{ 'rotation de } 120^\circ \text{', } \sigma \text{ 'rotation de } -120^\circ \end{array} \right\}$.

\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 .

—

$$a * b = a * c$$

$$\Rightarrow b = c$$

$$b * a = c * a$$

$$\Rightarrow b = c$$

$$(a^{-1})^{-1} = a$$

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

—

Exemple.

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{Q}_*, \times), (\mathbb{R}_*, \times)$ abéliens, $\mathbb{Z}_3, \mathbb{D}_3, GL(n, \mathbb{R})$.

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

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) .

exercice

(A) exercice

□

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)

$$\begin{aligned}f : \mathbb{R} &\rightarrow \mathbb{R}_*^+ \\ x &\mapsto e^x\end{aligned}$$

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. $f(a) = b$

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

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.

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

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 ".

$$G : \begin{array}{c|c|c|c|c} * & e_G & a_1 & a_2 & \dots \\ \hline e_G & & & & \\ \hline a_1 & & & a_1 * a_2 & \\ \hline a_2 & & & & \\ \hline \vdots & & & & \end{array} \xrightarrow{f} \begin{array}{c|c|c|c|c} * & e_H & f(a_1) & f(a_2) & \dots \\ \hline f(e_G) & & & & \\ \hline f(a_1) & & & f(a_1) \diamond f(a_2) & \\ \hline f(a_2) & & & & \\ \hline \vdots & & & & \end{array} : H$$

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

Exemple.

$$\mathbb{Z}_2 : \begin{array}{c|c|c} + & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{1} \\ \hline \bar{1} & \bar{1} & \bar{0} \end{array} \quad H : \begin{array}{c|c|c} \circ & \varepsilon & \alpha \\ \hline \varepsilon & \varepsilon & \alpha \\ \hline \alpha & \alpha & \varepsilon \end{array} \quad C_2 : \begin{array}{c|c|c} \times & 1 & -1 \\ \hline 1 & 1 & -1 \\ \hline -1 & -1 & 1 \end{array}$$

\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 .

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

□

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.

—

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

— 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. $a^{-3} = a^{-1} * a^{-1} * a^{-1}$.

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

Proposition. $(a^m)^n = a^{mn}, \forall m, n \in \mathbb{N}$. 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.
 $\mathbb{1}_G : G \rightarrow G$ 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 $n \in \mathbb{Z}$.

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

$n < 0$ 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.

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

(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.

$$\begin{aligned} f : \mathbb{R} &\rightarrow H \\ \text{On définit} \quad x &\mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \end{aligned}$$

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 $f(x) = f(y)$

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

— 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.

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

démonstration.

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

- (c) $a \in H$, 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-vidé $H \subseteq G$ est un sous-groupe ssi 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-vidé, 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.

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

H est non-vidé, 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 ssi $f(K)$ 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 $H \leq G$.

Proposition.

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

démonstration.

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

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

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

Exemple. $2\mathbb{Z} \leq \mathbb{Z}$ et $3\mathbb{Z} \leq \mathbb{Z}$. $2\mathbb{Z} \cup 3\mathbb{Z}$ 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. $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z} \leq \mathbb{Z}$.

Chapitre 2

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 $x \sim y$ ssi $(x, y) \in R$.

Exemple.

- (a) $E = \mathbb{R}$

$$x \sim y \text{ ssi } |x| = |y|$$

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

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

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

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

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

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. $\bar{x} = \bar{y}$ ssi $x \sim y$.

démonstration.

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

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

$$(\Leftarrow) \quad \text{Supposons } x \sim y.$$

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

$$(\supseteq) \quad \text{idem}$$

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

□

Cours 9

Rappel.

- $H \leq G$, H un sous-groupe de G , ssi
 - $H \neq \emptyset$;
 - $\forall a, b \in H, ab^{-1} \in H$.
- 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 :

$a \sim b$ ssi $a - b = km$, 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 $a, b \in \mathbb{Z}$.

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

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

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

Alors, $a - b = k_1m$ et $b - c = k_2m$, 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.

$$\bar{0} = \bar{2} = \bar{4} = \overline{-2} = \dots \qquad \bar{1} = \bar{3} = \bar{5} = \overline{-1} = \dots$$

Plus généralement, pour m , on a m classes d'équivalence.

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

Notation. L'ensemble des classes d'équivalence est noté $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$ 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) $E_i \cap E_j = \emptyset$, si $i \neq j$.

Remarque. Chaque $x \in E$ est élément d'exactly 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 $\bar{a} \cap \bar{b} = \emptyset, \forall \bar{a}, \bar{b} \in \mathcal{P}$.

□

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

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

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 $\bar{a} + \bar{b} = \bar{a'} + \bar{b'}$.