Chapitre 12

Structure usuelle

Hugo Salou MP2I

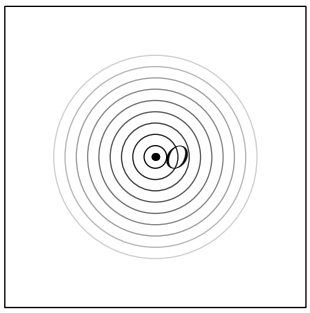
Dernière mise à jour le 30 janvier 2022

Table des matières

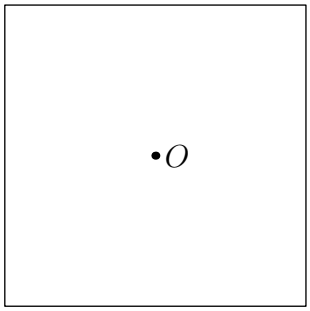
Première partie

Groupes

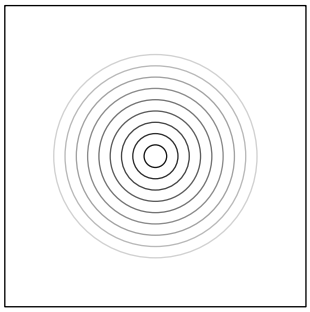
Principe de symétrie (Pierre Curie)
La symétrie des causes se retrouvent dans les effets.
On fait tomber un caillou dans un plan d'eau ce qui crée une onde qui se propage.

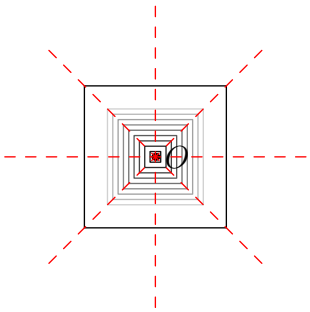


— Symétries des "causes"
(conserver O en place)
  — translation de vecteur $\vec{0}$
  — rotations de centre O d'angle quelconque
  — symétries d'axe passant par O



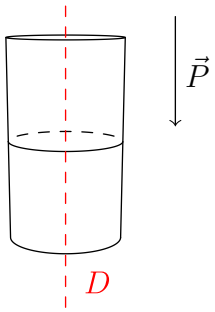
— Symétries des "effets"
(conserver les ondes en place)
  — translation de vecteur $\vec{0}$
  — rotations de centre O d'angle quelconque
  — symétries d'axe passant par O



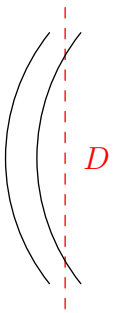


- translation de vecteur $\vec{0}$
- 4 rotations de centre O d'angle $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$
- 4 symétries axiales

— Causes
- translations de vecteur $\vec{u} \in \vec{D}$
- rotations d'axe D



— Effet



Definition

Soit G un ensemble, muni d'une loi de composition interne $\diamond$.
On dit que $(G, \diamond)$ est un groupe si :
- $\diamond$ est associative
- $\diamond$ a un neutre $e \in G$
- $\forall x \in G, \exists y \in G, x \diamond y = y \diamond x = e$

Definition

On dit que $(G, \diamond)$ est un groupe commutatif ou abélien si c'est un groupe et $\diamond$ est une loi commutative.

Definition

Soit $(G, \cdot)$ un groupe (d'élément neutre e) et $H \subset G$. On dit que H est un sous groupe de G si

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

Proposition

Soit H un sous groupe de $(G, \cdot)$. Alors, $(H, \cdot)$ est un groupe. □

Proposition

Soit $(G, \cdot)$ un groupe et $H \subset G$.

$$H \text{ est un sous groupe de } G \iff \begin{cases} \forall (x, y) \in H, x \cdot y^{-1} \in H \\ H \neq \varnothing \end{cases}$$

Proposition

Soit $(G, \cdot)$ un groupe et $(H_i)_{i \in I}$ une famille non vide de sous groupes de G. Alors, $\bigcap_{i \in I} H_i$ est un sous groupe de G.

Proposition

Soit $(G, \cdot)$ un groupe.
$\{e\}$ et G sont des sous groupes de G

Remarque

Une réunion de sous groupes n'est pas nécessairement un sous groupe.

$$(G, \cdot) = (\mathbb{Z}, +)$$

$2\mathbb{Z} \cup 3\mathbb{Z} = A$
$2 \in A$ et $3 \in A$ mais $2 + 3 = 5 \notin A$.
Donc, A n'est pas un sous groupe de $\mathbb{Z}$

Proposition
Définition

Soit $(G, \cdot)$ un groupe et $A \subset G$. Alors,

$$\bigcap_{\substack{H \text{ sous groupe de } G \\ A \subset H}} H$$

est le plus petit (au sens de l'inclusion) sous groupe de G qui contient A. On dit que c'est le sous groupe engendré par A et on le note $\langle A \rangle$

Definition

Soit $(G, \cdot)$ un groupe et $A \subset G$.
On dit que A est une partie génératrice de G ou que A engendre G si $G = \langle A \rangle$

Remarque *Notation*
Soit $(G, \cdot)$ un groupe et $a \in G$.
Pour $n \in \mathbb{N}_*$, on pose $a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ fois}}$.
On pose $a^0 = e$ et pour $n \in Z_*^-$,

$$a^n = \left(a^{-1}\right)^{-n}$$

Remarque

Si le groupe est noté additivement. On note na $(n \in \mathbb{Z}, a \in G)$ à la place de a^n

Definition

On dit qu'un groupe $(G, \cdot)$ est monogène s'il existe $a \in G$ tel que

$$G = \langle a \rangle$$

On dit alors que a est un générateur de G

Definition

Un groupe monogène fini est cyclique

Proposition

Soit $(G, \cdot)$ un groupe monogène fini. Soit a un générateur de G. Il existe $k \in \mathbb{N}$ tel que

$$G = \{e, a, a^2, \ldots a^{k-1}\}$$

Definition

Soit $(G, \cdot)$ un groupe et $a \in G$.
Si $\langle a \rangle$ est fini, le cardinal de $\langle a \rangle$ est appelé ordre de a : c'est le plus petit entier strictement positif n tel que $a^n = e$

Definition

Soient $(G_1, \cdot)$ et $(G_2, *)$ deux groupes et $f : G_1 \to G_2$. On dit que f est un (homo)morphisme de groupes si

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

Proposition

Avec les notations précédentes,
- l'image directe d'un sous groupe de G_1 est un sous groupe de G_2
- l'image réciproque d'un sous groupe de G_2 est un sous groupe de G_1

Lemme

$$\begin{cases} f(e_1) = e_2 \\ \forall u \in G_1, f\left(u^{-1}\right) = (f(u))^{-1} \end{cases}$$

Corollaire

Soit $f : (G_1, \cdot) \to (G_2, *)$ un morphisme de groupes. Alors, $\mathrm{Im}(f)$ est un sous groupe de G_2.

$$\mathrm{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\} = f^{-1}(\{e_2\})$$

est un sous groupe de G_1. □

Théorème

Avec les notations précédentes,

$$f \text{ injective} \iff \mathrm{Ker}(f) = \{e_1\}$$

Théorème

Soit $f : (G_1, \cdot) \to (G_2, *)$ un morphisme de groupes, $y \in G_2$ et $(\mathscr{E})$ l'équation

$$f(x) = y$$

d'inconnue $x \in G_1$.
Si $y \notin \mathrm{Im}(f)$, alors $(\mathscr{E})$ n'a pas de solution.

Sinon, soit $x_0 \in G_1$ tel que $f(x_0) = y$ (x_0 est une solution particulière de $(\mathscr{E})$)

$$f(x) = y \iff \exists h \in \mathrm{Ker}(f), x = x_0 \cdot h$$

Proposition

Soient $f : G_1 \to G_2$ et $g : G_2 \to G_3$ deux morphisme de groupes. Alors, $g \circ f$ est un morphisme de groupes.

Definition

Soit G un groupe.

- Un endomorphisme de G est un morphisme de groupes de G dans G.
- Un isomorphisme de G dans H un morphisme de groupes $f : G \to H$ bijectif.
- Un automorphisme de G est un endomorphisme de G bijectif.

Proposition

Soit $f : G \to H$ un isomorphisme de groupes.
Alors, $f^{-1} : H \to G$ est aussi un isomorphisme.

Corollaire

On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.
$\mathrm{Aut}(G)$ est un sous groupe de $(S(G), \circ)$.

Definition

Soit $(G, \cdot)$ un groupe et $g \in G$. L'application

$$\begin{aligned} c_g : G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

est appelée conjugaison par g. On dit aussi que c'est un automorphisme intérieur.

Proposition

Avec les notations précédentes,

$$c_g \in \mathrm{Aut}(G)$$

Corollaire

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

□

Proposition

L'application

$$\begin{aligned} G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto c_g \end{aligned}$$

est un morphisme de groupes.

Proposition **Rappel**

$$\forall g, h \in G, (gh)^{-1} = h^{-1}g^{-1}$$

Proposition
Définition

Soient $(G_1, *)$ et $(G_2, *)$ deux groupes. On définit une loi sur $G_1 \times G_2$ en posant

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

Alors, $G_1 \times G_2$ est un groupe pour cette loi appelée groupe produit

Deuxième partie

Anneaux

Definition

Un anneau $(A, +, \times)$ est un ensemble A muni de deux lois de compositions internes notées $+$ et $\times$ vérifiant

1. $(A, +)$ est un groupe commutatif (son neutre est noté 0_A)
2. $(A, \times)$ est un monoïde
   (a) $\times$ est associative
   (b) $\times$ a un neutre $1_A \in A$
3. distributivité à gauche et à droite :

$$\forall (a,b,c) \in A^3, \begin{cases} a \times (b+c) = (a \times b) + (a \times c) \\ (b+c) \times a = (b \times a) + (c \times a) \end{cases}$$

Remarque *Convention*

Soit $(A, +, \times)$ un anneau.
On convient que la multiplication est prioritaire sur l'addition.

$$(a \times b) + (a \times c) = a \times b + a \times c$$

et l'exponentiation est prioritaire sur la multiplication ($n \in \mathbb{N}$)

$$\begin{aligned} a \times b^n &= a \times (\underbrace{b \times b \times \cdots \times b}_{n \text{ fois}}) \\ &\neq (a \times b)^n \end{aligned}$$

Proposition

Soit $(A, +, \times)$ un anneau. Alors, 0_A est absorbant

$$\forall a \in A, a \times 0_A = 0_A \times a = 0_A$$

Remarque

On peut imaginer $\begin{cases} a \times b = 0_A \\ a \neq 0_A \\ b \neq 0_A \end{cases}$

Definition

On dit qu'un anneau $(A, +, \times)$ est intègre si

$$\forall (a,b) \in A^2, (a \times b = 0_A \implies a = 0_A \text{ ou } b = 0_A)$$

Proposition

Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$, $n \in \mathbb{Z}$. Alors,

$$n(a \times b) = (na) \times b = a \times (nb)$$

Théorème **Formule du binôme de Newton**

Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$, $n \in \mathbb{N}$.
Si a et b commutent alors

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Proposition

Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$ et $n \in \mathbb{N}_*$.
Si a et b commutent, alors

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

□

Proposition

On note $A^\times$ l'ensemble des éléments inversibles d'un anneau $(A, +, \times)$.
$(A^\times, \times)$ est un groupe. □

Definition

Soit $(A, +, \times)$ un anneau <u>commutatif</u>.

1. Soient $(a, b) \in A^2$. On dit que a <u>divise</u> b s'il existe $k \in A$ tel que $b = a \times k$. On dit aussi que a est un <u>diviseur</u> de b et que b est un <u>multiple</u> de a.
2. On dit que a et b sont <u>associés</u> s'il existe $k \in A^\times$ tel que $ak = b$ (dans ce cas, $a \mid b$ et $b \mid a$)

Remarque

Le théorème des deux carrés peut se démontrer en exploitant les propriétés arithmétiques de l'anneau $(Z[i], +, \times)$ où $Z[i] = \{a + ib \mid a \in \mathbb{Z}, b \in \mathbb{Z}\}$.
$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

<u>Théorème des deux carrés :</u>

1. Soit p un nombre premier.

$$\exists (a,b) \in \mathbb{N}^2, p = a^2 + b^2 \iff p \equiv 1\ [4]$$

2. Soit $n \in \mathbb{N}_*$, $n = \prod_{p \in \mathscr{P}} p^{\alpha(p)}$

$$\exists (a,b) \in \mathbb{N}^2, n = a^2 + b^2 \iff \forall p \in \mathscr{P} \text{ tel que } \alpha(p) \neq 0, p \equiv 1\ [4]$$

Definition

Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que B est un sous anneau de A si

1. B est un sous groupe de $(A, +)$
2. $\forall (a,b) \in B^2, a \times b \in B$
3. $1_A \in B$

Proposition

Soit $(A, +, \times)$ un anneau et B un sous anneau de A. Alors, $(B, +, \times)$ est un anneau. □

Proposition

Soit $(A, +, \times)$ un anneau.
Si $0_A = 1_A$ alors $A = \{0_A\}$. On dit alors que A est l'anneau nul.

Definition

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux (les lois notés de la même façon mais ne sont pas forcément les mêmes !).
Soit $f : A \to B$. On dit que f est un (homo)morphisme d'anneaux si

1. $\forall (a,b) \in A^2, f(a + b) = f(a) + f(b)$
2. $\forall (a,b) \in A^2, f(a \times b) = f(a) \times f(b)$
3. $f(1_A) = 1_B$

Proposition

Avec les notations précédentes, **si** $a \in A^\times$ alors $f(a) \in B^\times$ et dans ce cas,

$$f(a)^{-1} = f\left(a^{-1}\right)$$

Definition

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux et $f : A \to B$ un morphisme d'anneaux.
On dit que f est un

— isomorphisme d'anneaux si f est bijective
— endomorphisme d'anneaux si $\begin{cases} A = B \\ + = + \\ \times = \times \end{cases}$
— automorphisme d'anneaux si f est à la fois un isomorphisme et un endomorphisme d'anneaux

Proposition

La composée de deux morphismes d'anneaux est un morphisme d'anneaux. □

Proposition

La réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux. □

Proposition

L'ensemble des automorphismes d'anneaux de A est un sous groupe de $(S(A), \circ)$. □

Proposition

L'image directe ou réciproque d'un sous anneau par un morphisme d'anneaux est un sous anneaux.

Definition

Soi $f : A \to B$ un morphisme d'anneaux. Le noyau de f est

$$\mathrm{Ker}(f) = \{a \in A \mid f(a) = 0_B\}$$

Proposition

Avec les notations précédents,

$$f \text{ injective} \iff \mathrm{Ker}(f) = \{0_A\}$$

□

Remarque

$\mathrm{Ker}(f)$ n'est pas un sous anneau en général (car $1_A \notin \mathrm{Ker}(f)$ sauf si $A = \{0_A\}$)

Definition

Soit $(A, +, \times)$ un anneau et $a \in A \setminus \{0_A\}$.

On dit que a est un diviseur de zéro s'il existe $b \in A \setminus \{0_A\}$ tel que $a \times b = b \times a = 0_A$

Proposition

Les diviseurs de zéro ne sont pas inversibles. □

Troisième partie

Corps

Definition

Soit $(\mathbb{K}, +, \times)$ un ensemble muni de deux lois de composition internes. On dit que c'est un corps si

1. $(\mathbb{K}, \times)$ est un groupe abélien
2. $(\mathbb{K}, \times)$ est un monoïde commutatif
3. $\forall x \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}, \exists y \in \mathbb{K}, xy = 1_{\mathbb{K}}$
4. $0_{\mathbb{K}} \neq 1_{\mathbb{K}}$

Proposition

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

Proposition

Tout corps est un anneau intègre.

Proposition

Soit $(\mathbb{K}, +, \times)$ un corps et P un polynôme à coefficients dans $\mathbb{K}$ de degré n. Alors, l'équation $P(x) = 0_{\mathbb{K}}$ a au plus n solutions dans $\mathbb{K}$ □

Corollaire **(Théorème de Wilson)**

voir exercice 16 du TD 12

Definition

Soit $(\mathbb{K}, +, \times)$ un corps et $L \subset \mathbb{K}$.
On dit que L est un sous corps de $\mathbb{K}$ si

1. L est un anneau de $(\mathbb{K}, +, \times)$ non nul
2. $\forall x \in L \setminus \{0_{\mathbb{K}}\}, x^{-1} \in L$

en d'autres termes si

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

On dit aussi que $\mathbb{K}$ est une extension de L.

Proposition

Tout sous corps est un corps. □

Definition

Soient $(\mathbb{K}_1, +, \times)$ et $(\mathbb{K}_2, +, \times)$ deux corps et $f : \mathbb{K}_1 \to \mathbb{K}_2$.
On dit que f est un morphisme de corps si f est un morphisme d'anneaux.

i.e. si

$$\begin{cases} \forall (x,y) \in {\mathbb{K}_1}^2, & f(x+y) = f(x) + f(y) \\ \forall (x,y) \in {\mathbb{K}_1}^2, & f(x \times y) = f(x) \times f(y) \end{cases}$$

Proposition

Tout morphisme de corps est injectif.

Quatrième partie

Actions de groupes

Definition

Soit $(G, \cdot)$ un groupe et X un ensemble non vide. Une action de G sur X est une application

$$\begin{aligned} \varphi : G \times X &\longrightarrow X \\ (g, x) &\longmapsto \underbrace{g \cdot x}_{\text{ce n'est pas la loi de } G} \end{aligned}$$

qui vérifie

1. $\forall x \in X, \varphi(e, x) = e \cdot x = x$
2. $\forall x \in X, \forall g, h \in G, g \cdot (h \cdot x) = (g \cdot h) \cdot x$

Dans ce cas, $\begin{array}{ccc} G & \longrightarrow & S(X) \\ g & \longmapsto & \varphi(g, \cdot) \end{array}$: $\begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & g \cdot x \end{array}$ est un morphisme de groupes.