Chapitre 1 : ENSEMBLES APPLICATIONS RELATIONS

La plupart des notions introduites dans ce chapitre sont déjà connues des étudiants. Notre but est donc de préciser le vocabulaire et les notations qui seront utilisés dans tout le cours.

Nous aurons toujours à considérer des propositions exprimées dans un langage formalisé, mais il ne s'agit pas pour nous de construire une logique formalisée. Nous resterons toujours sur un plan « naïf » et utiliserons le langage usuel, qui doit cependant être précisé.

Le lecteur intéressé par l'étude axiomatique de la logique et de la théorie des ensembles pourra consulter les ouvrages spécialisés consacrés à cette question.

1.1. Notion de logique

1.1.1. PROPOSITIONS. CONNECTEURS LOGIQUES

1.1.1.1. Définition

On appelle **proposition** *un énoncé qui est vrai dans certaines conditions, faux dans d'autres, mais dont on peut toujours dire s'il est vrai ou s'il est faux.*

La propriété essentielle d'une proposition P est donc d'être dotée de l'une des **valeurs de vérité** V (vrai) ou F (faux).

1.1.1.2. Exemple

« n est un nombre entier et n est multiple de 2 » est une proposition vraie pour les nombres pairs mais fausse pour les nombres impairs.

Nous appellerons **assertion** une proposition qui est toujours vraie ou qui est toujours fausse.

Par exemple, « 10 est un nombre premier » est une assertion fausse.

On appelle **axiome**, dans une théorie mathématique, toute proposition à laquelle on attribue, par convention, la valeur **vrai**.

On appelle **théorème**, toute proposition dont on démontre qu'elle a la valeur **vrai**.

A partir des propositions P et Q, on peut former d'autres propositions à l'aide des liaisons **et, ou, non**, ... appelées **connecteurs logiques**.

Les principaux connecteurs sont :

1.1.1.3. Le connecteur de négation

Si P est une proposition, on note $\neg P$, et on lit « non P », la négation de P.

Par définition, « non P » est vraie si P est fausse, fausse si P est vraie.

La valeur de vérité de $\neg P$ en fonction de celle de P est donnée par un tableau appelé **table de vérité de** $\neg$:

P	$\neg P$
V	F
F	V

1.1.1.4. La conjonction et la disjonction

La **conjonction et** est le connecteur logique noté $\wedge$, qui associe à tout couple (P, Q) de propositions, la proposition (P et Q), vraie si et seulement si P et Q sont vraies simultanément.

De même $P \vee Q$, qu'on lit « P ou Q », est vraie si l'une au moins des propositions P, Q est vraie, fausse si P et Q le sont.
Le signe $\vee$ s'appelle le **connecteur de disjonction** ; il se lit « **ou** ».

Les tables de vérité de $\vee$ et $\wedge$ sont :

P	Q	$P \wedge Q$	$P \vee Q$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	F

1.1.1.5. L'implication

L'implication est le connecteur logique qui, à tout couple (P, Q) de propositions, associe la proposition $(P \Longrightarrow Q)$ (lue « P implique Q ») fausse lorsque P est vraie et Q fausse, vraie dans les autres cas.

En mathématiques il est d'usage de n'écrire que des propositions vraies ; c'est pourquoi, pour traduire « $P \Longrightarrow Q$ », on emploie souvent l'expression « si P, alors Q ». Mais la relation $(P \Longrightarrow Q)$ peut fort bien être vraie alors que ni P ni Q ne le sont ; par exemple la proposition (4 est impair) $\Longrightarrow$ (7 est pair) est vraie.

Les propositions suivantes sont également vraies :
(4 est pair) $\Longrightarrow$ (7 est impair), (4 est impair) $\Longrightarrow$ (7 est impair).

1.1.1.6. Le connecteur d'équivalence

noté $\Longleftrightarrow$:

Si P et Q sont des propositions, on note $P \Longleftrightarrow Q$, et on lit « P est équivalente à Q », la proposition :

$$(P \Longrightarrow Q) \wedge (Q \Longrightarrow P).$$

Les tables de vérité des connecteurs $\Longrightarrow$ et $\Longleftrightarrow$ sont :

P	Q	$P \Longrightarrow Q$	$P \Longleftrightarrow Q$
V	V	V	V
V	F	F	F
F	V	V	F
F	F	V	V

En comparant les tables de vérité, on montre facilement que deux propositions P et Q étant données, $(P \Longrightarrow Q)$ est équivalente à $((\neg Q) \Longrightarrow (\neg P))$. On dit que $(\neg Q) \Longrightarrow (\neg P)$ est la **contraposée** de $(P \Longrightarrow Q)$ ou encore qu'elle est obtenue par **contraposition** de $(P \Longrightarrow Q)$.

1.1.2. QUANTIFICATEURS

Soit $P(x)$ une proposition contenant un objet x appelé **variable** assujetti à appartenir à un ensemble E appelé **référentiel.**

On convient d'écrire :

$$(\forall x \in E)\ P(x) \qquad \text{ou} \qquad (\forall x)\ P(x)$$

pour exprimer que lorsque x appartient au référentiel E, la proposition P est toujours vraie. On lit « pour tout x, $P(x)$ » ou « quel que soit x, $P(x)$ ».

Le symbole $\forall$ s'appelle le **quantificateur universel.**

Pour exprimer l'assertion « il existe au moins un objet x du référentiel pour lequel $P(x)$ est vraie » on convient d'écrire

$$(\exists x \in E)\ P(x) \qquad \text{ou} \qquad (\exists x)\ P(x).$$

ce qui se lit « il existe au moins un élément x de E tel que "$P(x)$" ».

Le symbole $\exists$ s'appelle le **quantificateur existentiel.**

Enfin l'expression $\exists !\ x, < P(x)$ signifie «il existe un et un seul élément x tel que l'assertion $P(x)$ soit vraie».

On utilise très souvent les équivalences logiques suivantes :

$$(\neg((\exists x)\ P(x))) \iff ((\forall x)\ (\neg P(x)))$$
$$(\neg((\forall x)\ P(x))) \iff ((\exists x)\ (\neg P(x)))$$
$$(\neg((\forall x)\ (P(x) \Longrightarrow Q(x))) \iff (\exists x)\ (P(x) \text{ et } \neg Q(x)))$$

1.1.2.1. Exemple

$$(\forall x \text{ réel})\ ((x+1)^2 = x^2 + 2x + 1)$$
$$(\exists x \text{ réel}),\ (x^2 + 3x - 1 = 0)$$

1.2. Ensembles

1.2.1. DÉFINITIONS ET NOTATIONS

La théorie axiomatique des ensembles est trop délicate pour être exposée au niveau élémentaire auquel nous nous plaçons. Intuitivement, un ensemble est une collection d'objets ; ces objets s'appellent les **éléments** ou les **points** de l'ensemble.

Nous désignerons en général les ensembles par des lettres majuscules : E, F, A, B, etc. Les éléments d'un ensemble seront désignés en général par des lettres minuscules : a, b, x, y, etc.

Si a est un élément d'un ensemble E, on écrit $a \in E$ et on lit «a appartient à E» ou «a est élément de E».

Pour exprimer que a n'est pas un élément de E, on écrit :

$$a \notin E \text{ et on lit «} a \text{ n'appartient pas à } E \text{»}.$$

Nous admettons l'existence d'un ensemble noté $\emptyset$, appelé **ensemble vide**, qui ne contient aucun élément.

Un ensemble réduit à un seul élément a est noté $\{a\}$. Plus génerlament, un ensemble qui ne contient que les éléments $x_1, ..., x_n$ est noté $\{x_1, ..., x_n\}$.

Si E est un ensemble et P une propriété vraie pour certains éléments de E, l'ensemble des éléments de E qui vérifient la propriété P est souvent noté :

$$\{x\ :\ x \text{ vérifie } P\}$$

1.2.1.1. Exemples

Les exemples suivants sont déjà bien connus du lecteur.

$\mathbb{N} = \{0, 1, 2, ...\}$ est l'ensemble des entiers naturels ;
$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, ...\}$ est l'ensemble des entiers relatifs ;
$\mathbb{Q}$ est l'ensemble des nombres relationnels ;
$\mathbb{R}$ est l'ensemble des nombres réels ;
$\mathbb{R}^*$ est l'ensemble des nombres réels non nuls ;
$\mathbb{R}_+$ est l'ensemble des nombres réels positifs ou nuls ;
$\mathbb{R}_+^*$ désigne l'ensemble des nombres réels strictement positifs ;
$\mathbb{C}$ est l'ensemble des nombres complexes ;
$\mathbb{C}^*$ est l'ensemble des nombres complexes non nuls.

1.2.2. PARTIES D'UN ENSEMBLE – COMPLÉMENTAIRE

1.2.2.1. Définition

On dit que l'ensemble E est **inclus** *ou est* **contenu** *dans l'ensemble F si tout élément de E est élément de F.*

On dit aussi que E est une **partie** *ou un* **sous-ensemble** *de F.*

On écrit

$$E \subset F \text{ ou } F \supset E$$

Par définition,

$$(E \subset F) \Longleftrightarrow (\forall x, x \in E \Longrightarrow x \in F)$$

Il est immédiat que :

$$E \subset E \text{ quel que soit } E,$$

$$(E \subset F \text{ et } F \subset X) \Longrightarrow (E \subset X)$$

On dit que **l'ensemble E est égal à l'ensemble F**, et on note $E = F$, si on a $E \subset F$ et $F \subset E$.

Nous admettrons que pour tout ensemble E, il existe un nouvel ensemble appelé **ensemble des parties de E**, noté $\mathcal{P}(E)$, et dont les éléments sont tous les sous-ensembles de E, y compris l'ensemble vide et E lui-même. Ainsi

$$A \in \mathcal{P}(E) \Longleftrightarrow A \subset E$$

On note souvent 2^E l'ensemble de parties de E car si E possède n éléments, $\mathcal{P}(E)$ possède 2^n éléments.

1.2.2.2. Définition

Soient E un ensemble et A une partie de E. On appelle **complémentaire** *de A dans E l'ensemble des éléments de E qui n'appartiennent pas à A.*

Le complémentaire de A dans E se note

$$E - A \text{ ou } \mathbf{C}_E A \text{ ou } \mathbf{C}_A$$

s'il n'y a pas de confusion à craindre.

On a donc

$$\mathbf{C}_E A = \{x : x \in E \text{ et } x \notin A\}.$$

Les égalités suivantes sont évidentes :

$$\mathbf{C}_E\left(\mathbf{C}_E A\right) = A;\ \mathbf{C}_E E = \emptyset;\ \mathbf{C}_E \emptyset = E.$$

De même, on verrait facilement que si A et B sont des parties d'un ensemble E, et si $A \subset B$, alors

$$\mathbf{C}_E B \subset \mathbf{C}_E A.$$

1.2.3. INTERSECTION ET RÉUNION DE DEUX ENSEMBLES

On appelle **intersection** de deux ensembles E et F, et on note $E \cap F$, l'ensemble des éléments x tels que $x \in E$ et $x \in F$.

On a donc

$$E \cap F = \{x : x \in E \text{ et } x \in F\}.$$

Si $E \cap F = \emptyset$, on dit que E et F sont **disjoints.**

On a évidemment

$$E \cap \emptyset = \emptyset.$$

On appelle **réunion** de deux ensembles E et F, et on note $E \cup F$, l'ensemble des éléments x tels que $x \in E$ ou $x \in F$.

On a donc

$$E \cup F = \{x : x \in E \text{ ou } x \in F\}.$$

Il est évident que

$$E \cup \emptyset = E \text{ et } E \cup F = \emptyset \Longrightarrow (E = \emptyset \text{ et } F = \emptyset)$$

Voici quelques propriétés de l'intersection et de la réunion.

• La réunion et l'intersection sont **associatives** :

$$(A \cup B) \cup C = A \cup (B \cup C) \text{ et } (A \cap B) \cap C = A \cap (B \cap C)$$

quels que soient les ensembles A, B et C.

• Elles sont **commutatives** :

$$A \cup B = B \cup A \text{ et } A \cap B = B \cap A$$

quels que soient les ensembles A et B.

• Elles sont **distributives** l'une par rapport à l'autre :

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

• Elles sont **idempotentes** :

$$A \cup A = A \text{ et } A \cap A = A.$$

Les démonstrations sont simples et sont laissées au lecteur.

Il existe des relations simples entre le complémentaire, la réunion et l'intersection. Ces relations sont données par le théorème suivant.

1.2.3.1. Théorème

Soient A et B deux parties d'un ensemble E. Alors on a les égalités suivantes :

$$\mathbf{C}_{(A \cap B)} = \left(\mathbf{C}_A\right) \cup \left(\mathbf{C}_B\right) \text{ et } \mathbf{C}_{(A \cup B)} = \left(\mathbf{C}_A\right) \cap \left(\mathbf{C}_B\right).$$

Démonstration. Il suffit de démontrer la première égalité. La deuxième s'en déduit en posant $A_1 = \mathbf{C}_A$, $B_1 = \mathbf{C}_B$ et en utilisant l'égalité $\mathbf{C}\left(\mathbf{C}_A\right) = A$.

Soit $x \in \mathbf{C}_{(A \cap B)}$. Alors $x \in E$ et $x \notin A \cap B$; donc $x \in \mathbf{C}_A$ ou bien $x \in \mathbf{C}_B$. Donc $x \in \left(\mathbf{C}_A\right) \cup \left(\mathbf{C}_B\right)$, d'où l'inclusion

$$\mathbf{C}_{(A \cap B)} \subset \left(\mathbf{C}_A\right) \cup \left(\mathbf{C}_B\right).$$

Réciproquement, soit x un élément de $\left(\mathbf{C}_A\right) \cup \left(\mathbf{C}_B\right)$.

Si $x \in \mathbf{C}_A$, $x \notin A$, donc $x \notin A \cap B$ et par suite $x \in \mathbf{C}_{(A \cap B)}$.
De même si $x \in \mathbf{C}_B$, $x \notin B$, donc $x \notin A \cap B$ et par suite $x \in \mathbf{C}_{(A \cap B)}$.

Dans les deux cas, $x \in \mathbf{C}_{(A \cap B)}$ d'où l'inclusion

$$\left(\mathbf{C}_A\right) \cup \left(\mathbf{C}_B\right) \subset \mathbf{C}_{(A \cap B)}$$

La première égalité est donc démontrée.

1.2.4. PRODUIT D'ENSEMBLES

Soient x et y deux objets. Nous admettrons qu'il est possible de former un troisième objet que l'on note (x, y) et qu'on appelle le **couple** (x, y), tel qu'on ait l'équivalence :

$$((x, y) = (x', y')) \Longleftrightarrow ((x = x') \text{ et } (y = y')).$$

On dit que x est le **premier élément** et y le **deuxième élément** du couple (x, y).

L'équivalence précédente montre que l'ordre dans lequel on écrit les deux éléments figurant dans un couple est essentiel. Il ne faut donc pas confondre (x, y) et (y, x), sauf si $x = y$; de même le couple (x, y) est différent de l'ensemble $\{x, y\}$.

1.2.4.1. Définition

Soient E et F deux ensembles. On appelle **produit cartésien** *de E et F, et on note $E \times F$,* **l'ensemble des couples** (x, y) *tels que $x \in E$ et $y \in F$.*

$$E \times F = \{(x, y) : x \in E \text{ et } y \in F\}.$$

On vérifie facilement les propriétés suivantes :

a) Si A, B, E et F sont quatre ensembles tels que

$$A \subset E \text{ et } B \subset F, \text{ alors } A \times B \subset E \times F.$$

b) Si A, B et C sont des ensembles quelconques, alors

$$A \times (B \cup C) = (A \times B) \cup (A \times C),$$

$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

c) $(E \times F = \emptyset) \Longleftrightarrow (E = \emptyset \text{ ou } F = \emptyset)$
$(E \times F \neq \emptyset) \Longleftrightarrow (E \neq \emptyset \text{ et } F \neq \emptyset)$.

Lorsque $E = F$, $E \times E$ se note E^2 et on appelle **diagonale** de E^2 l'ensemble des couples (x, x) avec $x \in E$.

Plus généralement, le produit cartésien de n ensembles $E_1, ..., E_n$ est l'ensemble

$$E_1 \times ... \times E_n \text{ encore noté } \prod_{j=1}^{n} E_j$$

de toutes les suites ordonnées $(x_1, ..., x_n)$ telles que $x_1 \in E_1, ..., x_n \in E_n$.

On dit que $(x_1, ..., x_n)$ est un **n-uple.**

Si $E_1 = ... = E_n = E$, on note E^n au lieu de $E \times E \times ... \times E$.

Par exemple, $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ se note $\mathbb{R}^3$.

1.3. Applications

1.3.1. DÉFINITIONS. EXEMPLES

Soient E et F deux ensembles. On appelle **graphe** de E vers F, toute partie non vide Γ de $E \times F$. Autrement dit, tout élément de Γ est un couple ordonné (x, y) où $x \in E$ et $y \in F$.

L'étude générale des graphes n'est pas notre objectif immédiat. Nous allons appliquer cette notion de graphe à l'étude des **applications d'un ensemble dans un autre ensemble.**

1.3.1.1. Définition

Soient E et F deux ensembles. On appelle **fonction** ou **application** *de E dans F, tout triplet $f = (\Gamma, E, F)$ vérifiant les conditions suivantes :*

a) *Γ est un graphe de E vers F.*

b) *Pour tout $x \in E$, il existe un élément y et un seul de F tel que $(x, y) \in \Gamma$.*

On dit que Γ est le **graphe de la fonction** f.

Si $x \in E$, l'unique élément y de F tel que $(x, y) \in \Gamma$ s'appelle l'**image** ou la **valeur de la fonction** f **en** x ; on la note $f(x)$.

Le graphe Γ de la fonction f est donc l'ensemble des couples $(x, f(x))$ où $x \in E$.

Si $f = (\Gamma, E, F)$ est une fonction, on dit que E est **l'ensemble de départ** (ou de **définition**) et F **l'ensemble d'arrivée.**

Pour exprimer que f est une application de E dans F on utilise les notations suivantes :

$$f : E \longrightarrow F, \qquad E \overset{f}{\longrightarrow} F \quad \text{ou } x \longmapsto f(x).$$

L'ensemble des applications de E dans F se note

$$\mathcal{F}(E, F) \text{ ou } F^E.$$

1.3.1.2. Exemples

a) Si $F = \mathbb{R}$, on dit que f est une **fonction réelle.** Si $E \subset \mathbb{R}$, ont dit que f est une **fonction d'une variable réelle.** Par exemple $x \longmapsto \sin x$ est une fonction réelle d'une variable réelle.

b) On appelle **application identique** d'un ensemble E, et on note Id_E ou 1_E, l'application qui à tout $x \in E$ fait correspondre x lui-même.
On a donc par définition :

$$Id_E(x) = x \text{ pour tout } x \in E.$$

c) Soient E et F deux ensembles. Les applications $(x, y) \longmapsto x$ de $E \times F$ dans E et $(x, y) \longmapsto y$ de $E \times F$ dans F s'appellent respectivement la **première projection** et la **deuxième projection.** On les note pr_1 et pr_2 respectivement.

d) On dit qu'une application $f : E \longrightarrow F$ est **constante** si l'on a $f(x) = f(y)$ quels que soient $x, y \in E$.

e) Soient $f = (\Gamma, E, F)$ et $g = (\Gamma', E', F')$ deux fonctions. On dit que ces fonctions sont **égales** si les trois conditions suivantes sont vérifiées :

$$E = E', \quad F = F' \text{ et } f(x) = g(x) \text{ pour tout } x \in E.$$

f) Soit $f = (\Gamma, E, F)$ une fonction et soit A une partie de E. On appelle **restriction** de f à A, et on note $f|A$, l'application h de A dans F telle que $h(x) = f(x)$ pour tout $x \in A$.

Inversement, étant donné deux fonctions $f = (\Gamma, E, F)$ et $g = (\Gamma', E', F')$, on dit que f est **un prolongement de** g si l'on a les relations

$$E' \subset E, \ F' \subset F \text{ et } f(x) = g(x) \text{ pour tout } x \in E'.$$

g) Soit E un ensemble. On appelle **fonction caractéristique de** E, la fonction χ_E à valeurs réelles définie par :

$$\chi_E(x) = \begin{cases} 1 \text{ si } x \in E \\ 0 \text{ si } x \notin E \end{cases}$$

1.3.2. COMPOSITIONS DES APPLICATIONS

Soient E, F, G trois ensembles et $f = (\Gamma, E, F)$, $g = (\Gamma', F, G)$ deux applications de E dans F et de F dans G respectivement.

Pour tout $x \in E$, $f(x) \in F$, donc $g(f(x)) \in G$. L'application $x \longmapsto g(f(x))$ de E dans G s'appelle **l'application composée de** f **et** g et se note gof ou gf s'il n'y a pas de confusion possible.

On a donc par définition

$$(gof)(x) = g(f(x)) \text{ pour tout } x \in E.$$

On notera bien que dans l'écriture gof, on effectue d'abord l'opération $x \longmapsto f(x)$ puis l'opérateur $f(x) \longmapsto g(f(x))$.

On définit de même la composée d'un nombre fini d'applications. En particulier, si f est une application de E dans E, on peut former fof, $fofof$, etc. Ces applications sont notées f^2, f^3, ...

1.3.2.1. Exemples

Prenons $E = F = G = \mathbb{R}$ et $f(x) = \cos x$, $g(x) = x^2 + 1$. On a

$$\begin{array}{rcl} (gof)(x) & = & g(f(x)) \quad = \quad \cos^2 x + 1 \\ (fog)(x) & = & f(g(x)) \quad = \quad \cos(x^2 + 1), \end{array}$$

ce qui montre que $fog \neq gof$ en général.

1.3.2.2. Théorème

Quelles que soient les applications

$$f : E \longrightarrow F, \quad g : F \longrightarrow G, \quad h : G \longrightarrow H,$$

on a

(I.3,1) $$(hog)of = ho(gof).$$

En calculant la valeur du premier membre en un point x quelconque de E, on trouve $h(g(f(x)))$. De même la valeur du second membre au même point x est $h(g(f(x)))$, d'où l'égalité à établir.

Le théorème permet de noter simplement $hogof$ l'application $(hog)of = ho(gof)$.

1.3.3. APPLICATIONS INJECTIVES, SURJECTIVES, BIJECTIVES

1.3.3.1. Définition

Soient E et F deux ensembles et f une application de E dans F.

a) *On dit que f est* **injective** *(ou est une* **injection***) si quels que soient $x, y \in E$, la relation $f(x) = f(y)$ entraîne $x = y$, ou encore si la relation $x \neq y$ implique $f(x) \neq f(y)$.*

b) *On dit que f est* **surjective** *(ou est une* **surjection***) ou* **applique** E **sur** F *si pour tout $y \in F$ il existe au moins un $x \in E$ tel que $y = f(x)$.*

c) *On dit que f est* **bijective** *(ou est une* **bijection***) si elle est à la fois injective et surjective, c'est-à-dire si, pour tout $y \in F$, il existe un et un seul $x \in E$ tel que $y = f(x)$.*

1.3.3.2. Exemples

a) Soit A une partie d'un ensemble E.
L'application $j : A \longrightarrow E$ définie par $j(x) = x$ pour tout $x \in A$ est injective; on l'appelle **l'injection canonique** de A dans E.

b) On appelle **permutation** d'un ensemble E, toute application bijective de E sur E. L'ensemble des permutations de E se note $\mathcal{S}(E)$.

Si $E = \{1, ..., n\}$, on écrit $\mathcal{S}_n$ au lieu de $\mathcal{S}(E)$. Cet ensemble sera étudié au Chapitre 3.

c) Si a et b sont des nombres réels et si $a \neq 0$, l'application $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie par $f(x) = ax + b$ pour tout $x \in \mathbb{R}$, est bijective (vérification facile laissée au lecteur).

1.3.3.3. Définition

Soient E et F deux ensembles et $f : E \longrightarrow F$ une application. On dit que f est **inversible** *s'il existe une application $g : F \longrightarrow E$ telle que*

(1.3.3.1) $$gof = Id_E \qquad \text{et} \qquad fog = Id_F.$$

Voici une caractérisation des applications inversibles.

1.3.3.4. Théorème

Soit f une application d'un ensemble E dans un ensemble F. Pour que f soit inversible, il faut et il suffit qu'elle soit bijective.

Démonstration. Si f est bijective, alors pour tout $y \in F$, il existe un x unique de E tel que $y = f(x)$. On peut donc définir une application $g : F \longrightarrow E$ en associant à tout $y \in F$ l'unique $x \in E$ tel que $y = f(x)$. Ainsi, si $y = f(x)$, on a $x = g(y)$. Par suite, pour tout $y \in F$ et pour tout $x \in E$, on a

$$(fog)(y) = f(x) = y$$
$$(gof)(x) = g(y) = x.$$

Donc f est inversible.

Réciproquement, supposons que f soit inversible ; donc il existe une application $g : F \longrightarrow E$ telle que $gof = Id_E$ et $fog = Id_F$.

Soient $x \in E$, $x' \in E$ tels que $f(x) = f(x')$. On en déduit $g(f(x)) = g(f(x'))$ d'où, puisque $gof = Id_E$, $x = x'$ et f est injective.

Soit maintenant z un élément de F. Comme $fog = Id_F$, on a $f(g(z)) = z$. Il existe donc au moins un $x \in E$ (à savoir $x = g(z)$) tel que $f(x) = z$, ce qui montre que f est surjective, donc bijective.

1.3.3.5. Remarque

On montrerait de même que l'application g est bijective. De plus g est unique car si g_1 et g_2 sont deux applications de F dans E vérifiant (1.3.3.1), on a

$$g_1 = g_1 o Id_F = g_1 o(fog_2) = (g_1 of)og_2 = Id_E og_2 = g_2.$$

Ainsi, si $f : E \longrightarrow F$ est bijective, il existe une bijection $g : F \longrightarrow E$ et une seule telle que l'on ait

$$gof = Id_E \text{ et } fog = Id_F.$$

On dit que g est **l'application réciproque** de f et on la note f^{-1}.

1.3.3.6. Théorème

Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications. Si f et g sont injectives (resp. surjectives) il en est de même de gof. Si f et g sont bijectives alors gof est bijective et l'on a

$$(gof)^{-1} = f^{-1}og^{-1}. \tag{1.3.3.2}$$

Enfin, si f est bijective, f^{-1} est bijective et on a

$$(f^{-1})^{-1} = f.$$

Démonstration. Supposons que f et g soient injectives et soient $x \in E$, $x' \in E$ tels que $g(f(x)) = g(f(x'))$. Alors $f(x) = f(x')$ puisque g est injective, donc $x = x'$ puisque f est injective; ceci prouve que gof est injective.

Si f et g sont surjectives, pour tout $z \in G$, il existe un $y \in F$ tel que $z = g(y)$, puis un $x \in E$ tel que $y = f(x)$, d'où $z = g(f(x))$, ce qui montre que gof est surjective.

On déduit de ce qui précède que si f et g sont bijectives, il en est de même de gof. De plus, on a

$$(f^{-1}o\,g^{-1})\,o\,(gof) = f^{-1}o\,(g^{-1}og)\,of = f^{-1}o\,Id_F\,o\,f = f^{-1}of = Id_E.$$

$$(gof)\,o\,(f^{-1}o\,g^{-1}) = g\,o\,(fof^{-1})\,o\,g^{-1} = g\,o\,Id_F\,o\,g^{-1} = g\,o\,g^{-1} = Id_G,$$

ce qui montre que l'application réciproque de gof est bien $f^{-1}o\,g^{-1}$ (bien noter l'ordre des facteurs).

Enfin, si f est bijective, les relations

$$fof^{-1} = Id_F \text{ et } f^{-1}o\,f = Id_E$$

montrent que f^{-1} est bijective et admet f pour bijection réciproque.

1.3.3.7. Remarque

D'après le Théorème 1.3.3.4, toute application $f : E \longrightarrow E$ telle que $fof = Id_E$ est bijective et $f^{-1} = f$. Une telle bijection s'appelle une **involution** de E.

1.3.4. IMAGES DIRECTES ET IMAGES RÉCIPROQUES

1.3.4.1. Définition

Soient E et F deux ensembles, $f : E \longrightarrow F$ une application, $A \subset E$ et $B \subset F$.

a) *On appelle* **image directe** *de A par f, et l'on note $f(A)$, l'ensemble des $f(x)$ pour $x \in A$.*

On a

$$f(A) = \{y \in F : \exists x \in A,\ y = f(x)\}.$$

b) *On appelle* **image réciproque** de B *par* f, *et l'on note* $f^{-1}(B)$, *l'ensemble des* $x \in E$ *tels que* $f(x) \in B$.

On a

$$f^{-1}(B) = \{x \in E : f(x) \in B\}.$$

L'image $f(E)$ *de* E *s'appelle* **l'image** *de* f *et se note* $Im(f)$.

On remarquera que la notation $f^{-1}(B)$ ne signifie nullement que l'application réciproque de f existe : il s'agit simplement d'une notation « abusive ».

On a les relations évidentes suivantes :

$$f(\emptyset) = \emptyset,\ f^{-1}(\emptyset = \emptyset,\ f^{-1}(F) = E.$$

$$A \subset f^{-1}(f(A)) \text{ pour toute partie } A \text{ de } E,$$

$$f\left(f^{-1}(B)\right) \subset B \text{ pour toute partie } B \text{ de } F.$$

Soit f une application d'un ensemble E dans lui même et soit A une partie de E. On dit que A est **stable par** f si l'on a $f(A) \subset A$. On dit que A est **invariant par** f si $f(A) = A$. L'application $h : A \longrightarrow A$ qui coïncide avec f sur A s'appelle **l'application induite** par f sur A.

Nous donnons ci-après quelques propriétés de l'image directe et de l'image réciproque ; ces propriétés ne doivent pas être apprises par coeur mais doivent être retrouvées rapidement en cas de besoin.

1.3.4.2. Théorème

Soit $f : E \longrightarrow F$ une application.

a) *Soient* A *et* A' *deux parties de* E.

1. *Si* $A \subset A'$ *alors* $f(A) \subset f(A')$.

2. *Si* A *et* A' *sont quelconques, on a*

$$f(A \cup A') = f(A) \cup f(A');$$

$$f(A \cap A') \subset f(A) \cap f(A') \text{ avec égalité si } f \text{ est injective.}$$

b) *Soient* B *et* B' *deux parties de* F.

1. *Si* $B \subset B'$, *on a* $f^{-1}(B) \subset f^{-1}(B')$.

2. *Si* B *et* B' *sont quelconques, on a*

$$f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B');$$

$$f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B').$$

3. $f^{-1}\left(\mathbf{C}_F B\right) = \mathbf{C}_E f^{-1}(B)$.

On vérifiera toutes ces propriétés à titre d'exercice.

1.3.5. FAMILLES

Soient E un ensemble et I un autre ensemble non vide appelé **ensemble d'indices**. On appelle **famille d'éléments** de E indexée par I, toute application de I dans E.

Si $x : i \longmapsto x(i)$ est une telle famille, on utilise la notation indicielle $i \longmapsto x_i$ et on parle de la famille $(x_i)_{i \in I}$ d'éléments de E.

Si I est un ensemble fini, on dit que la famille est **finie**.

Si J est une partie non vide de I, on dit que la famille $(x_i)_{i \in J}$ est une **sous-famille** ou une **famille extraite** de la famille $(x_i)_{i \in I}$.

Si nous prenons $I = \mathbb{N}$, une famille d'éléments de E indexée par $\mathbb{N}$ s'appelle une **suite d'éléments de** E et se note $(x_0, x_1, ...)$ ou $(x_n)_{n \geq 0}$.

Si $(k_1, k_2, ...)$ est une suite strictement croissante d'entiers et si on pose $x_{k_1} = z_1, x_{k_2} = z_2, ...$, on dit que la suite $z_1, z_2, ...)$ est une **suite extraite** de la suite $(x_1, x_2, ...)$.

On appelle **famille d'ensembles** $(A_i)_{i \in I}$, une famille telle que chaque A_i soit un ensemble.

Nous aurons souvent à considérer une famille $(A_i)_{i \in I}$ de parties d'un ensemble E. La relation $A_i \subset E$ est donc équivalente à $A_i \in \mathcal{P}(E)$; alors la famille $(A_i)_{i \in I}$ de parties de E est la famille des éléments A_i de $\mathcal{P}(E)$.

Pour une famille d'ensembles, on peut généraliser les notions d'intersection, de réunion et de produit de la façon suivante :

Soit $(A_i)_{i \in I}$ une famille d'ensembles.

a) On appelle **intersection** de cette famille, et on note $\bigcap_{i \in I} A_i$, l'ensemble des éléments x tels que $x \in A_i$ pour tout $i \in I$.

b) On appelle **réunion** de cette famille, et on note $\bigcup_{i \in I} A_i$, l'ensemble des éléments x qui appartiennent à l'un au moins des A_i.

Rappelons que le produit cartésien $A_1 \times ... \times A_n$ des ensembles $A_1, ..., A_n$ est l'ensembles des n-uples $(x_1, ..., x_n)$ tels que $x_1 \in A_1, ..., x_n \in A_n$, ou encore l'ensemble des suites ordonnées $(x_i)_{1 \leq i \leq n}$ telles que $x_i \in A_i$ pour $1 \leq i \leq n$.

Cette remarque va nous permettre de généraliser la notion d'ensemble produit.

Si $A = \bigcup_{i \in I} A_i$ est la réunion de la famille $(A_i)_{i \in I}$, on appelle **produit** de cette famille, et on note $\prod_{i \in I} A_i$, l'ensemble des familles $(x_i)_{i \in I}$ d'éléments de A telles que $x_i \in A_i$ pour tout $i \in I$.

Donc $x \in \prod_{i \in I} A_i$ si et seulement si $x = (x_i)_{i \in I}$ avec $x_i \in A_i$ pour tout $i \in I$.

On dit que x_i est la **composante** ou la **coordonnée**, ou encore la **projection d'indice** i de x. L'ensemble A_i est appelé **facteur d'indice** i du produit $\prod_{i \in I} A_i$.

L'application $(x_i)_{i \in I} \longmapsto x_i$ de $\prod_{i \in I} A_i$ dans A_i s'appelle la **projection d'indice** i et se note pr_i.

Pour terminer ce numéro, donnons encore deux définitions.

On dit qu'une famille d'ensembles $(A_i)_{i \in I}$, I non vide, est un **recouvrement** d'un ensemble E si

$$E \subset \bigcup_{i \in I} A_i.$$

On appelle **partition d'un ensemble** E une famille de parties de E, non vides, deux à deux disjointes, dont la réunion est E.

Par exemple si $A \subset E (A \neq \emptyset$ et $A \neq E)$ alors A et $\complement_E A$ forment une partition de E.

1.3.6. FONCTIONS DE PLUSIEURS VARIABLES

Soient $E_1, ..., E_n$ des ensembles, $E_1 \times ... \times E_n$ leur produit cartésien et $E \subset E_1 \times ... \times E_n$. Si f est une application de E dans un ensemble F, on dit que f est une **fonction de n variables.**

Si $x = (x_1, ...x_n)$ est un point de E, la valeur de f au point x devrait s'écrire $f((x_1, ...x_n))$ mais on préfère écrire $f(x_1, ...x_n)$.

Il arrive souvent qu'on ait à considérer des fonctions dont les ensembles d'arrivée sont des produits d'ensembles. Considérons par exemple une application

$$f : E \longrightarrow F_1 \times F_2 \times ... \times F_n$$

où $E, F_1, ..., F_n$ sont des ensembles.

Pour tout $x \in E$, on a $f(x) \in F_1 \times ... \times F_n$, donc $f(x)$ est un n-uple. Si nous désignons par $f_1(x), ..., f_n(x)$ les coordonnées de $f(x)$, on peut écrire pour chaque $x \in E$,

$$f(x) = (f_1(x), ...f_n(x)).$$

On voit donc que l'application f détermine les applications

$$f_i = pr_i o f : E \longrightarrow F_i \qquad (1 \leq i \leq n),$$

et réciproquement, la donnée des fonctions f_i définit une application f de E dans $F_1 \times ... \times F_n$ en posant

$$f : x \longmapsto (f_1(x), ..., f_n(x)).$$

1.4. Relations dans un ensemble

Nous rappelons dans ce paragraphe les notions élémentaires de relations, de relation d'équivalence et de relation d'ordre. Nous nous limitons volontairement aux développements indispensables à la compréhension du reste du cours.

1.4.1. DÉFINITIONS. EXEMPLES

1.4.1.1. Définition

Soit E un ensemble. On appelle **relation binaire** *sur E, tout couple $\mathcal{R} = (E, \Gamma)$, où Γ est une partie de $E \times E$ que l'on appelle* **graphe** *de la relation $\mathcal{R}$.*

Si $(x, y) \in \Gamma$, on dit que x est **en relation** avec y ; on note $x\mathcal{R}y$, sinon on note $\neg(x\mathcal{R}y)$.

1.4.1.2. Exemples

a) Soit E un ensemble et soient $x, y \in E$. $x\mathcal{R}y$ si et seulement si $x = y$ est une relation binaire sur E.

b) La relation d'inclusion est une relation binaire dans l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E.

1.4.1.3. Définition

Soient E un ensemble et $\mathcal{R}$ une relation binaire sur E. On dit que :

a) *$\mathcal{R}$ est* **réflexive** *si pour tout $x \in E$, on a $x\mathcal{R}x$;*

b) *$\mathcal{R}$ est* **symétrique** *si pour tout $x \in E$ et pour tout $y \in E$, $x\mathcal{R}y \Longrightarrow y\mathcal{R}x$;*

c) *$\mathcal{R}$ est* **antisymétrique** *si pour tout $x \in E$ et pour tout $y \in E$, ($x\mathcal{R}y$ et $y\mathcal{R}x$) $\Longrightarrow x = y$;*

d) *$\mathcal{R}$ est* **transitive** *si quels que soient $x, y, z \in E$, ($x\mathcal{R}y$ et $y\mathcal{R}z$) $\Longrightarrow x\mathcal{R}z$.*

1.4.1.4. Exemples

a) La relation d'égalité de l'exemple 1.4.1.2 est réflexive : pour tout $x \in E$, on a $x = x$.

b) Dans l'ensemble $\mathcal{P}(E)$ des parties non videes d'un ensemble E, l'inclusion est réflexive, antisymétrique et transitive.

c) Dans $\mathbf{Z}^* = \mathbf{Z} - \{0\}$, la relation $x\mathcal{R}y \Longleftrightarrow x$ divise y est réflexive et transitive mais elle n'est ni symétrique ni antisymétrique, ce qui montre au passage que la propriété d'antisymétrie n'est pas la négation de la propriété de symétrie.

1.4.2. RELATIONS D'ÉQUIVALENCE

1.4.2.1. Définition

On dit qu'une relation binaire $\mathcal{R}$ dans un ensemble E est une **relation d'équivalence** *si elle est réflexive, symétrique et transitive.*

On note $x\mathcal{R}y$ ou $x \equiv y(\text{mod } \mathcal{R})$ qui se lit « x est équivalent à y modulo $\mathcal{R}$ ».

1.4.2.2. Exemples

a) L'égalité dans E, $(x\mathcal{R}y \iff x = y)$ est une relation d'équivalence.

b) Dans $\mathbf{Z} \times \mathbf{Z}^*$, $(p, q)\mathcal{R}(p', q') \iff pq' = p'q$ est une relation d'équivalence.

c) Soit p un entier ≥ 1. Dans $\mathbf{Z}$ la relation

$$x \equiv y(\text{mod } p) \iff p \text{ divise } x - y$$

est une relation d'équivalence. En effet si $n \in \mathbf{Z}$, on a $n - n = o.p$, donc la relation est réflexive. Si n, m et k sont des éléments de $\mathbf{Z}$ tels que $n - m = kp$, on a $m - n = (-k)p$ et la relation est symétrique. Si $n, n', m, k, k' \in \mathbf{Z}$ sont tels que $n - n' = kp$ et $n' - m = k'p$, on a $n - m = (n - n') + (n' - m) = (k + k')p$, donc la relation est transitive.

1.4.2.3. Définition

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. On appelle **classe d'équivalence** *d'un élément x de E, et on note $cl(x)$ ou $\overline{x}$ ou $\dot{x}$, l'ensemble des $y \in E$ qui sont équivalents à x modulo $\mathcal{R}$.*

L'ensemble des classes d'équivalence s'appelle **l'ensemble quotient** *de E par $\mathcal{R}$ et se note $E/\mathcal{R}$. Tout élément d'une classe d'équivalence s'appelle un* **représentant** *de cette classe.*

Par définition de $E/\mathcal{R}$, l'application $\pi : x \longmapsto \dot{x}$ de E dans $E/\mathcal{R}$ est surjective ; on l'appelle **l'application canonique** ou la **surjection canonique.**

1.4.2.4. Exemple

Dans l'exemple 1.4.2.2 **c)** la classe d'équivalence d'un entier n est l'ensemble

$$\{..., n - 2p, n - p, n, n + p, n + 2p, ...\}$$

qu'on appelle la **classe de congruence de n modulo p** ; une classe de congruence modulo p est aussi appelée un **entier modulo p.**
L'ensemble quotient $E/\mathcal{R}$ se note ici

$$\mathbf{Z}/p\mathbf{Z}.$$

1.4.2.5. Théorème

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. L'ensemble des classes d'équivalence modulo $\mathcal{R}$ forme une partition de E. Réciproquement, toute partition de E définit une relation d'équivalence dont les classes sont les éléments de la partition donnée.

Démonstration. On a $x \in \dot{x}$, puisque la relation est réflexive ; donc pour tout $x \in E$, $\dot{x} \neq \emptyset$. Puisque $x \in \dot{x}$, on a

$$E = \bigcup_{x \in E} \{x\} \subset \bigcup_{x \in E} \dot{x} \subset E.$$

Les classes ne sont donc pas vides et leur réunion est l'ensemble E.

Montrons que deux classes d'équivalence $\dot{x}$ et $\dot{y}$ sont identiques si et seulement si $x\mathcal{R}y$.

Supposons d'abord que $x\mathcal{R}y$ et soit $z \in \dot{x}$; alors on a $x\mathcal{R}z$, donc $y\mathcal{R}z$ et par suite $z \in \dot{y}$, ce qui montre que $\dot{x} \subset \dot{y}$. Par symétrie, on verrait de même que $\dot{y} \subset \dot{x}$. Donc $\dot{x} = \dot{y}$.

Inversement supposons que $\dot{x} = \dot{y}$. On a toujours $x \in \dot{x} = \dot{y}$, donc $x\mathcal{R}y$.

Supposons maintenant que $\dot{x} \neq \dot{y}$. S'il existait $z \in E$ tel que $z \in \dot{x} \cap \dot{y}$, alors $z\mathcal{R}x$ et $z\mathcal{R}y$. Comme la relation est symétrique et transitive, on en déduirait $x\mathcal{R}y$, d'où $\dot{x} = \dot{y}$ contrairement à l'hypothèse. Donc $\dot{x} \cap \dot{y} = \emptyset$.

Réciproquement, si $(A_i)_{i \in I}$ est une partition de E, la relation $x\mathcal{R}y$ si et seulement si x et y appartiennent au même A_i est une relation d'équivalence. En effet puisque $\bigcup_{i \in I} A_i = E$, pour tout $x \in E$, il existe un indice i tel que $x \in A_i$. Donc $x\mathcal{R}x$. La relation $\mathcal{R}$ est évidemment symétrique. Soient x, y, z des éléments de E tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors il existe $i \in I$ tel que $x \in A_i$ et $y \in A_i$, et il existe $j \in I$ tel que $y \in A_j$ et $z \in A_j$. Comme $y \in A_i \cap A_j$, on a $A_i \cap A_j \neq \emptyset$, donc $A_i = A_j$, et par suite $x\mathcal{R}z$, d'où la transitivité de $\mathcal{R}$.

Il est clair que les classes d'équivalence sont les éléments A_i de la partition donnée.

Le résultat suivant sera souvent utilisé dans la suite du cours.

1.4.2.6. Théorème *(Décomposition canonique d'une application.)*

Soient E et F deux ensembles et $f : E \longrightarrow F$ une application.

a) *La relation binaire $\mathcal{R}$ définie sur E par : $x\mathcal{R}y$ si et seulement si $f(x) = f(y)$ est une relation d'équivalence dans E dite* associée *à f.*

b) *Soient π la surjection canonique de E sur $E/\mathcal{R}$ et j l'injection canonique de $f(E)$ dans F. Alors il existe une application bijective unique $\overline{f} : E/\mathcal{R} \longrightarrow f(E)$ telle que $f = j \circ \overline{f} \circ \pi$.*

Démonstration.

a) On vérifie facilement que $\mathcal{R}$ est une relation d'équivalence dans E.

b) Définissons une application $\overline{f} : E/\mathcal{R} \longrightarrow f(E)$ en posant, pour toute classe $\dot{x} \in E/\mathcal{R}$,

$$\overline{f}(\dot{x} = f(x)$$

où x est un représentant de la classe $\dot{x}$; autrement dit, on a

$$f = \overline{f} o \pi.$$

L'application $\overline{f}$ ne dépend que des classes modulo $\mathcal{R}$ et non du représentant de la classe $\dot{x}$. Si en effet y est un autre représentant de la classe $\dot{x}$, on a $x\mathcal{R}y$, *i.e.* $f(x) = f(y) = \overline{f}(\dot{x})$.

Montrons que $\overline{f}$ est bijective.

Soient $\dot{x}, \dot{y} \in E/\mathcal{R}$ tels que $\overline{f}(\dot{x}) = \overline{f}(\dot{y})$; si x est un représentant de $\dot{x}$ et y est un représentant de $\dot{y}$, on a

$$f(x) = \overline{f}(\dot{x}) = \overline{f}(\dot{y}) = f(y),$$

donc $x\mathcal{R}y$ et par suite $\dot{x} = \dot{y}$, ce qui prouve que $\overline{f}$ est injective.

Pour tout $y \in f(E)$, il existe un $x \in E$ tel que $y = f(x)$. Donc $y = \overline{f}(\dot{x})$ et $\overline{f}$ est surjective, donc bijective.

S'il existait une autre application $g : E/\mathcal{R} \longrightarrow F$ telle que $f = go\pi$, on aurait pour tout $x \in E$,

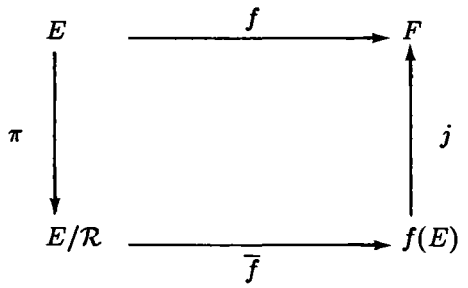
$$\overline{f}(\dot{x}) = f(x) = g(\dot{x})$$

d'où $\overline{f} = g$, ce qui prouve l'unicité de $\overline{f}$.

Si enfin j est l'injection canonique de $f(E)$ dans F, il est clair que pour tout $x \in E$, on a

$$j(\overline{f}\,(\pi(x))) = \overline{f}(\pi(x)) = \overline{f}(\dot{x}) = f(x).$$

Donc $f = jo\overline{f}o\pi$ et on a le diagramme suivant



1.4.2.7. Définition

La décomposition $f = j \circ \overline{f} \circ \pi$ *s'appelle la* **décomposition canonique ou la factorisation canonique de** f.

La bijection $\overline{f}$ *s'appelle* **l'application induite par** f *ou encore* **l'application déduite de** f **par passage au quotient.**

1.4.3. RELATIONS D'ORDRE

1.4.3.1. Définition

On dit qu'une relation binaire dans un ensemble E *est une* **relation d'ordre** *si elle est réflexive, antisymétrique et transitive.*

En général, une relation d'ordre sera notée $\leq$ et on dit que $(E, \leq)$ est un **ensemble ordonné.**

$x \leq y$ se lit « x est inférieur ou égal à y » ou « x est plus petit que y ».

Si $x \leq y$ et $x \neq y$, on écrit $x < y$ ou $y > x$ et on dit que « x est **strictement inférieur à** y » ou « y est **strictement supérieur à** x ».

Soit $(E, \leq)$ un ensemble ordonné. On dit que deux éléments x et y de E sont **comparables** si $x \leq y$ ou $y \leq x$. Si deux éléments quelconques de E sont comparables, on dit que la relation d'ordre $\leq$ est une relation **d'ordre total**; $(E, \leq)$ est alors dit **totalement ordonné.** Dans le cas contraire on dit que $\leq$ est une relation **d'ordre partiel** et $(E, \leq)$ est dit **partiellement ordonné.**

1.4.3.2. Exemples

a) Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$, l'ordre usuel est un ordre total.

b) Soit E un ensemble. La relation d'inclusion est une relation d'ordre partiel (en général) entre éléments de $\mathcal{P}(E)$. On dit que $\mathcal{P}(E)$ est **ordonné par inclusion.**

c) Dans $\mathbb{N}$, la relation de divisibilité est une relation d'ordre partiel. Par exemple 3 ne divise pas 8 et 8 ne divise pas 3.

Ici encore, notre but n'est pas de faire la théorie générale des ensembles ordonnés. Nous n'exposerons que les notions dont nous aurons besoin ultérieurement.

Soit $(E, \leq)$ un ensemble ordonné et soit A une partie de E. La relation $x \leq y$ entre éléments de A est évidemment une relation d'ordre sur A, appelée **relation d'ordre induite sur** A par celle de E.

1.4.3.3. Définition

Soient $(E, \leq)$ *un ensemble ordonné et* A *une partie non vide de* E.

a) *On dit qu'un élément $a \in E$ est un* **majorant** *(resp. un* **minorant***) de A, si $x \leq a$ (resp. $a \leq x$) pour tout $x \in A$.*

b) *On dit qu'un élément $a \in E$ est un* **plus grand** *(resp. un* **plus petit***)* **élément** *de A, si $a \in A$ et si a est un majorant (resp. un minorant) de A.*

On dit que A est **majorée** *(resp.* **minorée***) si A admet des majorants (resp. des minorants). Si A est majorée et minorée, on dit que A est une* **partie bornée**.

Remarquons qu'une partie A d'un ensemble ordonné n'admet pas nécessairement un plus grand ou un plus petit élément. Par exemple si $E = \mathbb{N}$ et si A est l'ensemble des nombres pairs, A n'a pas de plus grand élément. Toutefois, si A admet un plus grand (ou un plus petit) élément, celui-ci est unique. En effet, si $a, a' \in A$ sont tels que $x \leq a$ et $x \leq a'$ quel que soit $x \in A$, alors, en particulier, on a : $a \leq a'$ et $a' \leq a$, d'où $a = a'$. On pourra donc parler du plus grand (ou du plus petit) élément de A lorsqu'il existe.

Le plus petit des majorants (resp. le plus grand des minorants) de A, s'il existe, s'appelle la **borne supérieure** (resp. la **borne inférieure**) de A et se note $\sup(A)$ (resp. $\inf(A)$).

Une partie A d'un ensemble ordonné E n'admet pas nécessairement une borne supérieure (resp. inférieure). Toutefois, si A admet une borne supérieure (resp. inférieure), elle est unique mais elle peut ne pas appartenir à A.

Par exemple, si $E = \mathbb{Q}$, ordonné par l'inégalité habituelle, et si $A = \{x \in \mathbb{Q} : x > 0 \text{ et } x^2 < 2\}$, alors l'ensemble A est minoré par n'importe quel nombre rationnel négatif ou nul. On a $\inf(A) = 0$ mais A n'admet pas de borne supérieure dans $\mathbb{Q}$ puisque $\sqrt{2} \notin \mathbb{Q}$.

Si A possède un plus grand (resp. un plus petit) élément a, alors a, qui appartient à A, est la borne supérieure (resp. la borne inférieure) de A. Soit en effet a le plus grand élément de A ; alors a est un majorant de A et si a' est un autre majorant de A, on a : $a \leq a'$ car $a \in A$. Donc a est le plus petit des majorants de A, c'est-à-dire la borne supérieure de A.

On démontrerait de même l'assertion concernant la borne inférieure.

Il faut bien noter qu'une partie peut très bien avoir une borne supérieure (resp. inférieure) sans avoir de plus grand (resp. plus petit) élément. Si en effet nous reprenons $E = \mathbb{Q}$ et $A = \{x \in \mathbb{Q} : x > 0 \text{ et } x^2 < 2\}$, 0 est bien la borne inférieure de A mais A n'admet pas de plus petit élément. De même A n'admet pas de borne supérieure, donc pas de plus grand élément.

Voici une caractérisation de la borne supérieure.

Théorème

Soient $(E, \leq)$ un ensemble totalement ordonné, et A une partie de E. Pour qu'un élément b de E soit la borne supérieure de A, il faut et il suffit que b vérifie les deux conditions.

a) *Pour tout $x \in A$, on a : $x \leq b$.*

b) *Pour tout élément $c \in E$ tel que $c < b$, il existe $x \in A$ tel que $c < x$.*

Démonstration. Si b est la borne supérieure de A, b est un majorant de A. La condition **b)** est vérifiée car sinon c serait un majorant de A strictement inférieur à b.

Réciproquement, si les deux conditions sont vérifiées, alors b est un majorant de A et tout élément de E strictement inférieur à b n'est pas un majorant de A. Donc b est le plus petit des majorants de A, i.e., la borne supérieure de A.

Soit $(E, \leq)$ un ensemble ordonné. S'il existe un élément $a \in E$ tel que la relation $a \leq x$ entraîne $x = a$ (resp. la relation $x \leq a$ entraîne $x = a$) pour tout $x \in E$, on dit que a est un **élément maximal** (resp. **minimal**) de E.

On dit qu'un élément de E est **extrémal** s'il est ou maximal ou minimal.

Un élément maximal (resp. minimal) de E, s'il existe, est noté $\max E$ (resp. $\min E$).

Par exemple, pour la relation de divisibilité dans $\mathbb{N} - \{0, 1\}$, les éléments minimaux sont les nombres premiers mais il n'y a pas d'élément maximal, ni de plus petit élément.

De même pour la relation d'ordre naturel $\leq$ dans $\mathbb{R}$, il n'y a ni élément minimal, ni élément maximal.

Remarquons que si E est totalement ordonné, les notions d'élément maximal et de plus grand élément coïncident ; mais lorsque E est partiellement ordonné, il n'en est pas ainsi, c'est donc dans ce dernier cas que la notion d'élément maximal présente un intérêt (voir l'exemple de $\mathbb{N} - \{0, 1\}$ ci-dessus).

1.4.4. APPLICATIONS MONOTONES. APPLICATIONS DANS UN ENSEMBLE ORDONNÉ

Soient E et F deux ensembles ordonnés (on notera $\leq$ ou $<$ la relation d'ordre dans E et dans F) et soit f une application de E dans F.

On dit que f est **croissante** (resp. **strictement croissante**) si la relation $x \leq y$ (resp. $x < y$) dans E entraîne la relation $f(x) \leq f(y)$ (resp. $f(x) < f(y)$) dans F.

On dit que f est **décroissante** (resp. **strictement décroissante**) si la relation $x \leq y$ (resp. $x < y$) dans E entraîne la relation $f(x) \geq f(y)$ (resp. $f(x) > f(y)$) dans F.

On dira que f est **nonotone** (resp. **strictement monotone**) si f est croissante ou décroissante (resp. strictement croissante ou strictement décroissante).

Soit maintenant f une application d'un ensemble quelconque A dans un ensemble ordonné E. On dit que f est **majorée** (resp. **minorée**) si $f(A)$ est une partie majorée (resp. minorée) dans E. Si f est majorée et minorée dans A, on dit que f est **bornée** dans A.

On appelle **borne supérieure** (resp. **borne inférieure**) de f dans A la borne supérieure (resp. la borne inférieure) dans E (si elle existe) de l'ensemble $f(A)$.

On les note respectivement

$$\sup_{x \in A} f(x) \quad , \quad \inf_{x \in A} f(x)$$

Remarquons que les notations et les définitions précédentes s'appliquent aux familles d'éléments de E. Soit $(x_i)_{i \in I}$ une famille d'éléments de E. Si les bornes supérieure et inférieure de la famille existent, on les note

$$\sup_{i \in I} x_i \quad \text{et} \quad \inf_{i \in I} x_i .$$

En particulier, pour une suite $(x_n)_{n \geq 1}$, on écrit

$$\sup_{n \geq 1} x_n \quad , \quad \inf_{n \geq 1} x_n .$$

1.4.5. INTERVALLES

Soient $(E, \leq)$ un ensemble totalement ordonné, a, b des éléments de E tels que $a \leq b$. On appelle **intervalle fermé** $[a, b]$ l'ensemble des $x \in E$ tels que $a \leq x \leq b$.

Soient a et b des éléments de E tels que $a < b$. On appelle **intervalle ouvert** $]a, b[$, l'ensemble des $x \in E$ tels que $a < x < b$.

On définit de même les intervalles **semi-ouverts**

$$]a, b] = \{x \in E : a < x \leq b\}$$

et

$$[a, b[= \{x \in E : a \leq x < b\}.$$

Par extension, on définit les **demi-droites fermées**

$$[a, \longrightarrow [= \{x \in E : x \geq a\}$$

$$] \longleftarrow, a] = \{x \in E : x \leq a\}$$

et les **demi-droites ouvertes**

$$]a, \longrightarrow [= \{x \in E : x > a\}$$

$$] \longleftarrow, a[= \{x \in E : x < a\},$$

pour tout $a \in E$.

Il est clair que si I est un intervalle ou une demi-droite de E, alors pour tout couple (x, y) d'éléments de I, tout élément compris entre x et y appartient encore à I. On vérifie cette propriété en utilisant la transitivité de la relation d'ordre.

Soit E un ensemble totalement ordonné et soit $x \in E$. On appelle **prédécesseur** $'x$ de x tout élément tel que $]'x, x[= \emptyset$. On notera que si $'x$ existe, il est unique.

De même le **successeur** x' de x est un élément tel que $]x, x'[= \emptyset$. Si x' existe, il est unique.

1.5. Entiers naturels. Ensembles finis

Dans ce paragraphe, nous allons donner quelques propriétés des entiers naturels. Nous n'exposerons pas ici les détails de la construction axiomatique de l'ensemble $\mathbb{N}$ des entiers naturels ce qui déborderait largement le cadre de ce cours. Nous admettons donc l'existence de $\mathbb{N}$ et nous supposons que le lecteur est familiarisé avec l'addition, la multiplication des entiers et les propriétés usuelles de ces opérations.

Nous étudierons ensuite quelques propriétés élémentaires des ensembles finis.

1.5.1. L'ENSEMBLE DES ENTIERS NATURELS

Nous admettrons qu'il existe un ensemble non vide et ordonné, noté $\mathbb{N}$, appelé **ensemble des entiers naturels**, et vérifiant les axiomes suivants :

(N_1) Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
(N_2) Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.
(N_3) $\mathbb{N}$ n'a pas de plus grand élément.
Le plus petit élément de $\mathbb{N}$ est noté 0.

Conséquences de la définition

a) Toute partie $\{n, m\}$ à deux éléments de $\mathbb{N}$ admet un plus petit élément, donc $\mathbb{N}$ est totalement ordonné.

b) Tout élément $a \in \mathbb{N} - \{0\}$ admet un prédécesseur.

Posons

$$N(a) = \{n \in \mathbb{N} : n < a\}.$$

On a $N(a) \neq \emptyset$ car $0 \in N(a)$. L'ensemble non vide $N(a)$ est majoré par a ; il admet donc un plus grand élément que nous oterons α. On a évidemment $\alpha < a$ et $]\alpha, a[= \emptyset$, donc α est le prédécesseur de a.

c) Tout élément $a \in \mathbb{N}$ admet un successeur.

Posons en effet

$$N'(a) = \{n \in \mathbb{N} : a < n\}.$$

$N'(a)$ est non vide car si $N'(a)$ était vide, $\mathbb{N}$ admettrait un plus grand élément contrairement à l'axiome (N_3). D'après (N_1), $N'(a)$ admet un plus petit élément que nous noterons β. Il est clair que $a < \beta$ et $]a, \beta[= \emptyset$, ce qui montre que β est le successeur de a.

Le successeur de 0 est noté 1, celui de 1 est noté 2, etc.
On pose

$$\mathbb{N}^* = \mathbb{N} - \{0\}.$$

Ces remarques montrent que l'application qui, à tout élément de $\mathbb{N}$ associe son successeur, est une bijection croissante de $\mathbb{N}$ sur $\mathbb{N}^*$.

Nous allons introduire le raisonnement par récurrence qui joue un rôle essentiel en mathématiques. Il est fondé sur le résultat suivant appelé **théorème de récurrence**.

1.5.1.1. Théorème

Soit $P(n)$ une propriété dépendant de l'entier n. Supposons que

a) *$P(0)$ est vraie.*

b) *Pour tout $n \in \mathbb{N}$, la relation $P(n)$ vraie implique $P(n+1)$ est vraie. Alors $P(n)$ est vraie pour tout $n \in \mathbb{N}$.*

Démonstration. Considérons l'ensemble A des éléments n de $\mathbb{N}$ tels que $P(n)$ soit vraie. C'est une partie de $\mathbb{N}$, non vide puisque $0 \in A$. Il s'agit de montrer que $A = \mathbb{N}$ ou, ce qui revient au même, que $\mathbb{N} - A = \emptyset$. Supposons que $\mathbb{N} - A \neq \emptyset$. Alors d'après l'axiome (N_1), $\mathbb{N} - A$ possède un plus petit élément m et comme $0 \notin \mathbb{N} - A$, on a $m \in \mathbb{N}^*$. Soit a le prédécesseur de m. Puisque m est le plus petit élément de $\mathbb{N} - A$, $a \in A$. Alors d'après l'hypothèse **b)**, $a \in A$ entraîne $m \in A$ contrairement au fait que $m \in \mathbb{N} - A$. Donc $\mathbb{N} - A = \emptyset$ et par suite $A = \mathbb{N}$.

1.5.1.2. Exemple

Soient x un nombre réel positif et n un entier. Montrons que $(1+x)^n \geq 1+nx$.

Nous allons démontrer cette propriété par récurrence sur n. Soit $P(n)$ la propriété

$$(\forall x \in \mathbb{R}_+)\ ((1+x)^n \geq 1+nx).$$

$P(0)$ est vraie car $(\forall x \in \mathbb{R}_+)\ ((1+x)^0 \geq 1)$.

Montrons que $P(n) \Longrightarrow P(n+1)$. Supposons $P(n)$ vraie, i.e. $(1+x)^n \geq 1+nx$. Multiplions les deux membres de cette inégalité par $1+x$ qui est positif; on obtient

$$(1+x)^{n+1} \geq (1+nx)(1+x) = 1+(n+1)x+nx^2.$$

Comme $1+(n+1)x+nx^2 \geq 1+(n+1)x$, il vient

$$(1+x)^{n+1} \geq 1+(n+1)x,$$

et la propriété $P(n+1)$ est vérifiée.

1.5.2. ENSEMBLES FINIS. CARDINAUX

1.5.2.1. Définition

Soient E et F deux ensembles. On dit que E et F sont **équipotents** *s'il existe une bijection de E sur F.*

On vérifie facilement que l'équipotence est une relation réflexive, symétrique et transitive entre ensembles. Toutefois, il ne s'agit pas d'une relation binaire sur un ensemble dont les éléments sont tous les ensembles ; on montre qu'un tel ensemble n'existe pas. On ne peut donc parler de relation d'équivalence ni *a fortiori* de classes d'équivalence.

1.5.2.2. Définition

On dit qu'un ensemble E est **fini** *s'il est vide ou s'il existe un entier naturel $n \geq 1$ tel que E soit équipotent à l'intervalle $[1, n]$ de $\mathbb{N}$.*

Un ensemble qui n'est pas fini est dit **infini**.

1.5.2.3. Théorème

Soient n et m deux entiers ≥ 1. Pour qu'il existe une injection de $[1, n]$ dans $[1, m]$, il faut et il suffit que $n \leq m$.

Démonstration. Si $n \leq m$, on a $[1, n] \subset [1, m]$. Alors l'injection canonique de $[1, n]$ dans $[1, m]$ est injective.

Pour démontrer la réciproque, nous allons raisonner par l'absurde. Supposons qu'il existe une injection de $[1, n]$ dans $[1, m]$ avec $m < n$. Alors l'ensemble E des entiers $n \geq 1$ tels qu'il existe un entier $m \geq 1$ et une injection de $[1, n]$ dans $[1, m]$ avec $m < n$ est non vide ; donc E admet un plus petit élément que nous noterons n_0. Soit m_0 un entier non nul tel que $m_0 < n_0$ et soit f une injection de $[1, n_0]$ dans $[1, m_0]$. Comme $1 \leq m_0 < n_0$, on a $n_0 \neq 1$, d'où $f(n_0) \neq f(1)$ puisque f est injective. On en déduit que $m_0 > 1$ car si on avait $m_0 = 1$, f serait constante et égale à 1. La restriction f_1 de f à $[1, n_0 - 1]$ est injective comme restriction d'une application injective.

Définissons une application $h : [1, m_0] - f(n_0) \longrightarrow [1, m_0 - 1]$ en posant

$$h(n) = \begin{cases} n & \text{si} \quad n < f(n_0) \\ n-1 & \text{si} \quad n > f(n_0). \end{cases}$$

Alors h est injective. Donc l'application hof_1, composée de deux injections, est une injection de $[1, n_0 - 1]$ dans $[1, m_0 - 1]$; ce résultat contredit la définition de n_0 car $m_0 - 1 < n_0 - 1$ puisque $m_0 < n_0$. Le théorème est donc démontré.

1.5.2.4. Corollaire

Soient n et m deux entiers ≥ 1. Pour qu'il existe une bijection de $[1, n]$ sur $[1, m]$, il faut et il suffit que $n = m$.

On en déduit que si un ensemble E est équipotent à $\{1, ..., n\}$ et à $\{1, ..., m\}$, alors $n = m$.

Nous pouvons donc poser la définition suivante :

1.5.2.5. Définition

Soit E un ensemble fini non vide. On appelle **cardinal** *de E ou* **nombre d'éléments** *de E, l'unique entier naturel $n \geq 1$ tel que E soit équipotent à $[1, n]$.*

On écrit $\quad \text{Card}(E) = n$ ou $|E| = n$.

Par définition, $\text{Card}(\emptyset) = 0$.

On démontre qu'une partie non vide de $\mathbb{N}$ **est finie si et seulement si elle est majorée.** On en déduit que l'ensemble $\mathbb{N}$ est infini.

Nous allons énoncer quelques propriétés élémentaires des ensembles finis. Ces propriétés se démontrent facilement à partir des définitions et des résultats précédents.

1.5.2.6. Théorème

a) *Si E et F sont deux ensembles finis équipotents, on a* $\text{Card}(E) = \text{Card}(F)$.

b) *Si F est une partie d'un ensemble fini E, alors F est fini et* $\text{Card}(F) \leq \text{Card}(E)$. *Si de plus,* $\text{Card}(F) = \text{Card}(E)$, *alors $F = E$.*

c) *L'intersection d'une famille finie ou infinie d'ensembles finis est finie.*

d) *Si E et F sont deux ensembles finis, alors $E \cup F$ est fini et*

$$\text{Card}(E \cup F) + \text{Card}(E \cap F) = \text{Card}(E) + \text{Card}(F).$$

e) *Si E et F sont deux ensembles finis, alors $E \times F$ est fini et*

$$\text{Card}(E \times F) = \text{Card}(E) \,.\, \text{Card}(F).$$

Plus généralement, si $E_1, \ldots, E_p$ sont des ensembles finis, on

$$\text{Card}(E_1 \times \ldots \times E_p) = \text{Card}(E_1) \,.\, \text{Card}(E_2) \ldots \text{Card}(E_p).$$

Voici encore quelques propriétés des applications d'un ensemble fini dans un autre ensemble fini.

1.5.2.7. Théorème

Soient E et F deux ensembles finis et f une application de E dans F. Alors :

a) $\text{Card}(f(E)) \leq \inf(\text{Card}(E), \text{Card}(F))$.

b) $\text{Card}(f(E)) = \text{Card}(E)$ *si et seulement si f est injective.*

c) $\text{Card} f(E)) = \text{Card}(F)$ *si et seulement si f est surjective.*

d) Si $\text{Card}(E) = \text{Card}(F)$, *alors f est injective si et seulement si f est surjective.*

Démonstration

a) Il est clair que $\text{Card}(f(E)) \leq \text{Card}(F)$ puisque $f(E) \subset F$. Donc $f(E)$ est un ensemble fini. Posons

$$f(E) = \{x_1, ..., x_n\}.$$

On peut écrire : $$E = \bigcup_{i=1}^{n} f^{-1}(\{x_i\}).$$

Ainsi E apparaît comme une réunion d'ensembles disjoints deux à deux. Comme $f^{-1}(\{x_i\}) \neq \emptyset$, on a (Théorème **d**)), $\text{Card}(E) \geq n$, c'est-à-dire $\text{Card}(E) \geq \text{Card}(f(E))$.

b) Conservons les notations du **a**). Alors f est injective si et seulement si pour tout $i \in \{1, ..., n\}$, on a $\text{Card}(f^{-1}(\{x_i\})) = 1$, ce qui signifie que $\text{Card}(E) = n = \text{Card}(f(E))$.

c) résulte du Théorème 1.5.2.6, **b**).

d) découle immédiatement des résultats précédents. □

1.6. Ensembles dénombrables

1.6.1. DÉFINITION. EXEMPLES

1.6.1.1. Définition

On dit qu'un ensemble E est **dénombrable** s'il est *équipotent à* $\mathbb{N}$.

On dit qu'un ensemble E est **au plus dénombrable** *s'il est fini ou s'il est dénombrable.*

Si un ensemble E est dénombrable, il est infini comme $\mathbb{N}$. L'existence d'une bijection $f : \mathbb{N} \longrightarrow E$ permet de numéroter les éléments de E ; en notant x_n au lieu de $f(n)$, on peut donc ranger les éléments de E en une suite $x_0, x_1, ..., x_n$).

1.6.1.2. Exemple

L'ensemble P des entiers pairs est dénombrable.

En effet, l'application $f : \mathbb{N} \longrightarrow P$ définie par $f(n) = 2n$ est bijective.

1.6.1.3. Exemple

L'ensemble $\mathbb{N}^*$ est dénombrable car l'application $f : \mathbb{N} \longrightarrow \mathbb{N}^*$ définie par $f(n) = n + 1$ est bijective par définition même de $\mathbb{N}$.

1.6.1.4. Exemple

$\mathbb{Z}$ est dénombrable.

En effet, l'application $f : \mathbb{N} \longrightarrow \mathbb{Z}$ définie par

$$f(n) = \begin{cases} \dfrac{n}{2} \text{ si } n \text{ est pair} \\ -\dfrac{n+1}{2} \text{ si } n \text{ est impair} \end{cases}$$

est bijective.

1.6.1.5. Exemple

$\mathbb{N} \times \mathbb{N}$ est dénombrable.

Ecrivons en effet les éléments de $\mathbb{N} \times \mathbb{N}$ dans un tableau infini à double entrée :

	0	1	2	...	p	...
0	$(0,0)$	$(0,1)$	$(0,2)$	...	$(0,p)$	...
1	$(1,0)$	$(1,1)$	$(1,2)$	...	$(1,p)$	...
2	$(2,0)$	$(2,1)$	$(2,2)$	...	$(2,p)$	...
⋮	⋮					
q	$(q,0)$	$(q,1)$	$(q,2)$	...	(q,p)	...
⋮	⋮					

On obtient la suite :

$$x_0 = (0,0), \quad x_1 = (1,0), \quad x_2 = (0,1), \quad x_3 = (2,0), \quad x_4 = (1,1), \quad \ldots$$

d'où une bijection de $\mathbb{N}$ sur $\mathbb{N} \times \mathbb{N}$.

1.6.2. PROPRIÉTÉS ÉLÉMENTAIRES

1.6.2.1. Théorème

Toute partie A d'un ensemble dénombrable E est au plus dénombrable.

Démonstration. Par hypothèse, il existe une bijection f de E sur $\mathbb{N}$. La restriction de f à A est encore une bijection de A sur une partie $f(A)$ de $\mathbb{N}$. Il suffit donc de démontrer que toute partie infinie B de $\mathbb{N}$ est dénombrable.

Pour cela, définissons par récurrence une application $k \longmapsto n_k$ de $\mathbb{N}$ dans B de la façon suivante ; n_0 est le plus petit élément de B et pour $k \geq 1$, n_k est le plus petit élément de $B - \{n_0, n_1, ..., n_{k-1}\}$ qui est une partie non vide de B puisque B est infinie par hypothèse.

Cette application est injective car si $k < p$, alors par construction, $n_p \notin \{n_0, n_1, ..., n_k\}$, et donc $n_p \neq n_k$. Pour montrer qu'elle est surjective, nous allons raisonner par l'absurde et supposer qu'il existe un élément $a \in B$ tel que $a \neq n_k$ pour tout $k \in \mathbb{N}$. Alors $a \in B - \{n_0, n_1, ...n_{k-1}\}$ pour tout $k \in \mathbb{N}^*$ et, par définition de n_k, on a $n_k \leq a$. Comme d'autre part $n_0 \leq a$, on a : $n_k \leq a$ pour tout $k \in \mathbb{N}$. Ainsi l'image de $\mathbb{N}$ par l'application injective $k \longmapsto n_k$ est contenue dans l'intervalle $[n_0, a]$ de $\mathbb{N}$ et $\mathbb{N}$ est équipotent à cet intervalle. Comme $[n_0, a]$ est un ensemble fini, cela contredit le fait que $\mathbb{N}$ est infini.

Ainsi l'application $k \longmapsto n_k$ est surjective ; elle est donc bijective d'où notre assertion. □

1.6.2.2. Lemme

Si E est un ensemble dénombrable et si f est une application bijective de E sur un ensemble F, alors F est dénombrable.

C'est évident, car si φ est une bijection de $\mathbb{N}$ sur E, alors $f o \varphi$ est une bijection de $\mathbb{N}$ sur F.

1.6.2.3. Lemme

Soient E un ensemble dénombrable et f une application surjective de E sur un ensemble F. Alors F est au plus dénombrable.

Démonstration. Puisque E est équipotent à $\mathbb{N}$, on peut supposer que $E = \mathbb{N}$. Comme f est surjective, pour tout $y \in F$, la partie $f^{-1}(\{y\})$ de $\mathbb{N}$ est non vide. Soit $m(y)$ le plus petit élément de $f^{-1}(\{y\})$; on définit ainsi une application $m : F \longrightarrow \mathbb{N}$. Comme $fom = Id_F$, l'application m est injective. L'application $y \longmapsto m(y)$ est une bijection de F sur la partie $m(F)$ de $\mathbb{N}$. $m(F)$ étant au plus dénombrable d'après le Théorème 1.6.2.1, F est au plus dénombrable.

1.6.2.4. Corrolaire

Tout ensemble quotient d'un ensemble dénombrable est dénombrable.

1.6.2.5. Théorème

Si E_1, E_2, ..., E_n sont des ensembles dénombrables, l'ensemble $E_1 \times E_2 \times ... \times E_n$ est dénombrable.

Démonstration. Il suffit de démontrer le théorème si $n = 2$; le cas général s'en déduit par récurrence.

Soit $m \longmapsto x_m$ (resp. $k \longmapsto y_k$) une bijection de $\mathbb{N}$ sur E_1, (resp. sur E_2). Alors $(m, k) \longmapsto (x_m, y_k)$ est une bijection de $\mathbb{N} \times \mathbb{N}$ sur $E_1 \times E_2$ donc, puisque $\mathbb{N} \times \mathbb{N}$ est dénombrable, $E_1 \times E_2$ est dénombrable (Lemme 1.6.7).

1.6.2.6. Théorème

Soit $(E_1, E_2, ...)$ *une suite finie ou infinie d'ensembles dénombrables. Alors* $E = \bigcup_{i=1}^{\infty} E_i$ *est un ensemble dénombrable.*

Démonstration. Pour tout n fixé, il existe une bijection $f_n : \mathbb{N} \longrightarrow E_n$. Définissons une application $g : \mathbb{N} \times \mathbb{N} \longrightarrow E$ en posant $g(n, m) = f_n(m)$. Cette application est surjective. En effet, pour tout $x \in E$, il existe au moins un $i \in \mathbb{N}$ tel que $x \in E_i$; si on pose $k = f_i^{-1}(x)$, alors $g(i, k) = x$.

D'après le Lemme 1.6.2.3, E est au plus dénombrable ; mais puisque un des ensembles E_n est infini, E est lui-même infini.

1.6.2.7. Corollaire

L'ensemble $\mathbb{Q}$ *des nombres rationnels est dénombrable.*

Démonstration. L'ensemble A des couples (p, q) d'entiers $p > 0$ et $q > 0$ est dénombrable comme sous-ensemble infini de $\mathbb{N} \times \mathbb{N}$. L'ensemble X des nombres rationnels positifs, qui est l'image de A par l'application $(p, q) \longmapsto p/q$, est donc dénombrable d'après le Lemme 1.6.2.3. De même l'ensemble Y des nombres rationnels négatifs est dénombrable (considérer l'application $(p, q) \longmapsto -p/q$). Comme $\mathbb{Q} = \{0\} \cup X \cup Y$, on voit que $\mathbb{Q}$ est dénombrable. □

On démontre que l'ensemble $\mathbb{R}$ des nombres réels n'est pas dénombrable (Théorème de Cantor) et même plus précisément, que si $(a, b) \in \mathbb{R}^2$ avec $a < b$, alors $]a, b[$ n'est pas dénombrable.

1.7. Analyse combinatoire

Dans ce paragraphe, nous allons aborder les problèmes de dénombrement ; il s'agira de calculer les cardinaux d'ensembles finis.

1.7.1. ARRANGEMENTS AVEC RÉPÉTITION

1.7.1.1. Définition

Soit E *un ensemble fini non vide et soit* p *un entier naturel non nul. On appelle* **arrangement de** p **éléments** *de* E **avec répétition** *toute application de* $\{1, 2, ..., p\}$ *dans* E.

Le théorème suivant donne le nombre d'arrangements avec répétition des éléments d'un ensemble fini.

1.7.1.2. Théorème

Soient F un ensemble fini de cardinal p et E un ensemble fini de cardinal n. L'ensemble $\mathcal{F}(F, E)$ des applications de F dans E est fini et a pour cardinal n^p.

Démonstration. Soient $F = \{b_1, ..., b_p\}$ et $E = \{a_1, ..., a_n\}$.

Pour définir une application f de F dans E, il suffit de se donner les éléments $f(b_1), ..., f(b_p)$ de E.

Nous allons calculer le nombre d'applications de F dans E par récurrence sur p, n étant fixé.

Si $p = 1$, on a $F = \{b_1\}$. Les applications de F dans E sont alors définies par

$$b_1 \longmapsto f_i(b_1) = a_i, \quad (1 \leq i \leq n);$$

donc $\mathcal{F}(F, E)$ est fini et a pour cardinal n.

Supposons la propriété vraie pour $\text{Card}(F) = p - 1$ et démontrons-la pour $\text{Card}(F) = p$. Soit b un élément de F ; posons

$$F = F' \cup \{b\}, \quad \text{où } \text{Card}(F') = p - 1.$$

Une application de F dans E est définie de façon unique par sa restriction à F' et par l'image de b. Il y a n images possibles pour b et, d'après l'hypothèse de récurrence, il y a n^{p-1} restrictions possibles à F'. Le nombre d'applications de F dans E est donc $n.\ n^{p-1} = n^p$.

1.7.1.3. Corollaire

Si E est un ensemble fini de cardinal $n \geq 1$, alors l'ensemble $\mathcal{P}(E)$ des parties de E est fini et a pour cardinal 2^n.

Démonstrations. A toute partie A de E associons sa fonction caractéristique $\chi_A : A \longrightarrow \{0, 1\}$ définie par

$$\chi_A(x) = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \in E - A \end{cases}$$

Réciproquement, à toute fonction $\varphi \in \mathcal{F}(E, \{0, 1\})$ associons la partie A de E définie par $A = \varphi^{-1}(\{1\})$. Alors on a $\varphi = \chi_A$.

On a ainsi établi une bijection $A \longrightarrow \chi_A$ de $\mathcal{P}(E)$ sur $\mathcal{F}(E, \{0, 1\})$ et il suffit d'appliquer le Théorème 1.7.1.2.

1.7.1.4. Remarque

C'est à cause de la formule donnée au Théorème 1.7.1.2 que l'ensemble $\mathcal{F}(F; E)$ de toutes les applications de F dans E se note souvent E^F.

De même, en raison de la formule du Corollaire 1.7.1.3, $\mathcal{P}(E)$ est souvent noté 2^E.

1.7.1.5. Théorème

a) *Soient E un ensemble fini et $(A_i)_{1\leq i\leq n}$ une partition finie de A. Alors* $\mathrm{Card}(A) = \sum_{i=1}^{n} \mathrm{Card}(A_i)$;

b) *(Principe des bergers) Soient E et F des ensembles finis et f une application surjective de E sur F. On suppose que pour tout $y \in F$, $\mathrm{Card}(f^{-1}(\{y\})) = p$. Alors* $\mathrm{Card}(E) = p \,.\, \mathrm{Card}(F)$.

Démonstration. a) Comme $A : \bigcup_{i=1}^{n} A_i$ et $A_i \cap A_j = \emptyset$ si $i \neq j$, on a par récurrence sur n (le cas $n = 2$ étant évident):

$$\mathrm{Card}(A) = \sum_{i=1}^{n} \mathrm{Card}(A_i).$$

b) Il suffit d'appliquer **a)** à la partition de E définie par la relation d'équivalence associée à f : $x\mathcal{R}y$ si et seulement si $f(x) = f(y)$.

1.7.2. ARRANGEMENTS SANS RÉPÉTITION. PERMUTATIONS

1.7.2.1. Définition

Soit E un ensemble fini de cardinal n et soit p un entier naturel ≥ 1. On appelle **arrangement de p éléments de E sans répétition**, *toute application injective de $\{1, ..., p\}$ dans E.*

Le nombre de ces arrangements est noté A_n^p.

On remarquera qu'il ne peut exister d'injection de $A = \{1, ..., p\}$ dans E que si $p \leq n$; en effet, si f est une injection de A dans E, c'est une bijection de A sur $f(A) \subset E$, donc (Théorème 1.5.2.7, **b)**) $\mathrm{Card}(f(A)) = p$. On a donc $p \leq n$ (Théorème 1.5.2.7, **a)**). Nous supposerons donc que $p \leq n$.

1.7.2.2. Théorème

Soient F un ensemble fini de cardinal p et E un ensemble fini de cardinal n, avec $p \leq n$. L'ensemble des applications injectives de F dans E est fini et possède $n(n-1) \ldots (n-p+1)$ éléments.

Démonstration. Soient $F = \{b_1, ..., b_p\}$ et $E = \{a_1, ..., a_n\}$. Pour définir une injection f de F dans E, il suffit de se donner les éléments distincts $f(b_1), ..., f(b_p)$ de E. Nous allons calculer le nombre A_n^p d'injections de F dans E par récurrence sur p, n étant fixé.

Si $p = 1$, le résultat est évident. Supposons le théorème vrai pour $\mathrm{Card}(F) = p - 1$ et prouvons-le si $\mathrm{Card}(F) = p$.

Soit b un élément de F ; on a $F = \{b\} \cup F'$, où $\text{Card}(F') = p - 1$. Une application f de F dans E est définie de façon unique par sa restriction f' à F' et par la donnée de $f(b)$. Si f est injective, il est clair que f' est injective. Si f' est injective, f est injective si et seulement si $f(b)$ est choisi parmi les éléments de $E - f'(F')$ qui sont au nombre de $n - (p-1) = n - p + 1$ puisque $\text{Card} f'(F')) = p - 1$.

Toute injection de F' dans E se prolonge ainsi en $n - p + 1$ injections de F dans E. Comme d'après l'hypothèse de récurrence il y a $n(n-1) \ldots (n-p+2)$ injections de F' dans E, on voit qu'il y a $n(n-1) \ldots (n-p+2) \times (n-p+1)$ injections de F dans E et le théorème est démontré.

Notation. *Soit n un entier > 0. On pose*

$$1.2.3 \ldots n = n!,$$

qui se lit « **factorielle n** » *avec par convention* $0! = 1$.

La formule du Théorème 1.7.2.2 peut alors s'écrire, en multipliant et divisant par $(n-p)!$

$$A_n^p = n(n-1) \ldots (n-p+1) = \frac{n!}{(n-p)!}.$$

1.7.2.3. Corollaire

Le nombre des permutations d'un ensemble E à n éléments est $n!$

En effet, si $F = E$, l'ensemble des applications injectives de E dans E possède $n!$ éléments. Mais d'après le Théorème 1.5.2.7 **d)**, les injections de E dans E sont aussi les permutations de E.

1.7.3. COMBINAISONS SANS RÉPÉTITION

1.7.3.1. Définition

Soit E un ensemble fini de cardinal n et soit p un entier $\leq n$. On appelle **combinaison sans répétition** (*ou* **combinaison**) *des n éléments de E p à p, toute partie de E ayant p éléments.*

On dit aussi **combinaison de n objets p à p.**

Une combinaison est formée d'objets distincts ; deux combinaisons diffèrent par la nature de leurs objets, et non par l'ordre de ces objets.

On note C_n^p ou $\binom{n}{p}$ le nombre de combinaisons de n objets p à p.

1.7.3.2. Théorème

Soit E un ensemble fini à n éléments et soit p un entier $\leq n$. Le nombre des parties de E à p éléments est :

$$C_n^p = \frac{n!}{p!(n-p)!} = \frac{n(n-1)\dots(n-p+1)}{p!}.$$

Démonstration. Supposons formé le tableau $\mathcal{I}$ des combinaisons des n éléments de E, p à p. Considérons une combinaison de $\mathcal{I}$ et effectuons sur les p éléments qui la composent toutes les permutations possibles ; nous obtenons $p!$ groupes. En procédant de même avec chaque combinaison du tableau $\mathcal{I}$, nous obtenons le tableau $\mathcal{I}'$ des arrangements des n éléments de E, p à p, sans omission ni répétition.

On a donc

$$A_n^p = p!\, C_n^p.$$

D'où

$$C_n^p = \frac{1}{p!} \cdot A_n^p = \frac{n!}{p!(n-p)!}. \qquad \square$$

Convention. On pose $C_n^p = 0$ si $p > n$.

Donnons ci-dessous quelques propriétés des entiers C_n^p qu'on appelle les **coefficients du binôme** pour des raisons que nous verrons bientôt.

1.7.3.3. Théorème

On a les propriétés suivantes :

a) $C_n^0 = 1, \quad C_n^1 = n$ *pour tout* $n \in \mathbb{N}$;

b) $C_n^p = C_n^{n-p}$;

c) $C_n^p = \frac{n}{p} C_{n-1}^{n-p}$ *pour tout* $n \in \mathbb{N}^*$ *et pour tout* $p \in \mathbb{N}^*$.

d) $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$ *pour tout* $n \in \mathbb{N}^*$ *et pour tout* $p \in \mathbb{N}^*$.

Démonstration. Tous ces résultats peuvent se vérifier à l'aide de calculs simples. Mais à titre d'exercice, nous allons donner une démonstration sans calcul de **b)** et **d)**.

b) Si E est un ensemble à n éléments, notons $\mathcal{P}_p$ l'ensemble des parties de E ayant p élément. L'application qui à toute partie associe son complémentaire est une bijection de $\mathcal{P}_p$ sur $\mathcal{P}_{n-p}$; donc

$$C_n^p = C_n^{n-p}$$

d) Soit E un ensemble à n éléments et soit $a \in E$. Considérons les ensembles :

$$\mathcal{P}'_p = \{A \in \mathcal{P}_p : a \in A\}$$
$$\mathcal{P}''_p = \{A \in \mathcal{P}_p : a \notin A\}.$$

On a évidemment

$$\mathcal{P}'_p \cup \mathcal{P}''_p = \mathcal{P}_p \quad \text{et} \quad \mathcal{P}'_p \cap \mathcal{P}''_p = \emptyset,$$

d'où

$$C_n^p = \text{Card}(\mathcal{P}_p) = \text{Card}(\mathcal{P}'_p) + \text{Card}(\mathcal{P}''_p).$$

Pour calculer $\text{Card}(\mathcal{P}'_p)$, on remarque que l'application qui à $A \in \mathcal{P}'_p$ associe $A - \{a\}$ est une bijection de $\mathcal{P}'_p$ sur l'ensemble des parties à $p-1$ éléments de $E - \{a\}$; comme $\text{Card}(E - \{a\}) = n - 1$, on a $\text{Card}(\mathcal{P}'_p) = C_{n-1}^{p-1}$.

D'autre part, $\text{Card}(\mathcal{P}''_p)$ est le nombre de parties de $E - \{a\}$ ayant p éléments, c'est-à-dire C_{n-1}^p. On en déduit la formule.

Triangle de Pascal

La formule de récurrence $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$ permet de construire un tableau triangulaire, appelé **triangle de Pascal**, dont les éléments sont les C_n^p. On écrit sur une même ligne les valeurs des C_n^p pour n fixé :

$n = 0$ $\quad C_0^0$

$n = 1$ $\quad C_1^0 \quad C_1^1$

$n = 2$ $\quad C_2^0 \quad C_2^1 \quad C_2^2$

$n = 3$ $\quad C_3^0 \quad C_3^1 \quad C_3^2 \quad C_3^3$

– – – – – – – – – – – – – – –

$n-1$ $\quad C_{n-1}^0 \quad C_{n-1}^1 \quad \ldots\ldots\ldots \quad C_{n-1}^{p-1} \quad C_{n-1}^p \quad \ldots\ldots \quad C_{n-1}^{n-1}$

n $\quad C_n^0 \quad C_n^1 \quad \ldots\ldots\ldots\ldots\ldots \quad C_n^p \quad \ldots\ldots \quad C_n^{n-1} \quad C_n^n$

D'après la formule $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$, chaque terme du tableau qui n'est pas un terme extrême est la somme du terme situé au-dessus et du terme à gauche de ce dernier.

Chapitre 2 : LOIS DE COMPOSITION

Dans ce chapitre, nous allons étudier les opérations algébriques permettant de composer entre eux, deux éléments quelconques d'un ensemble donné. Autrement dit, à tout couple d'éléments d'un ensemble E, nous ferons correspondre un élément bien défini de E.

Si l'ensemble considéré et la loi possèdent certaines propriétés, on obtient ce qu'on appelle une **structure algébrique.**

On notera qu'il est souvent possible de définir plusieurs structures algébriques sur un même ensemble E. Par exemple, l'ensemble des endomorphismes d'un espace vectoriel est muni d'une structure d'espace vectoriel et d'une structure d'anneau.

Nous avons regroupé ici les propriétés générales des lois de composition et certaines démonstrations afin que le lecteur puisse s'y reporter aisément.

2.1. Généralités

2.1.1. DÉFINITIONS. NOTATIONS. EXEMPLES

2.1.1.1. Définition

Soit E un ensemble. On appelle **loi de composition interne** *sur E, toute application de $E \times E$ dans E.*

Un ensemble muni d'une loi de composition interne s'appelle un **magma.**

Notations. On note de plusieurs manières les lois de composition. Voici quelques notations utilisées fréquemment :

$$(x, y) \longmapsto x + y \ ; \quad (x, y) \longmapsto x \,.\, y$$
$$(x, y) \longmapsto x \top y \ ; \quad (x, y) \longmapsto x \perp y.$$

Dans ce chapitre, nous utiliserons souvent le signe $\top$ ou le signe $\perp$ pour noter les lois de composition, mais ce sont les notations **additive** $(x, y) \longmapsto x + y$ et **multiplicative** $(x, y) \longmapsto x \,.\, y$ qui sont le plus fréquemment utilisées dans les applications.

L'image $x \top y$ du couple $(x, y) \in E \times E$ par la loi de composition $\top$ s'appelle le **composé de x et de y** pris dans cet ordre.

2.1.1.2. Exemple

Dans $\mathbb{R}$, l'addition $(x, y) \longmapsto x + y$ et la soustraction $(x, y) \longmapsto x - y$ sont des lois de composition internes.

2.1.1.3. Exemple

Soit E un ensemble. Dans $\mathcal{P}(E)$, $(A, B) \longmapsto A \cup B$ et $(A, B) \longmapsto A \cap B$ sont des lois de composition internes.

2.1.1.4. Exemple

Soit $\mathcal{F}(E, E)$ l'ensemble des applications d'un ensemble E dans lui-même. L'application qui, aux éléments f et g de $\mathcal{F}(E, E)$, associe fog (composition des applications) est une loi de composition interne sur $\mathcal{F}(E, E)$.

2.1.2. PARTIES STABLES. LOIS INDUITES

2.1.2.1. Définition

Soient $(E, \top)$ un magma, et A une partie de E. On dit que A est **stable** *pour la loi $\top$ si les relations $x \in A$ et $y \in A$ entraînent $x \top y \in A$.*

L'application $(x, y) \longmapsto x \top y$ de $A \times A$ dans A est donc une loi de composition interne sur A. On l'appelle la **loi induite** sur A par la loi $\top$ définie sur E.

2.1.3. COMPOSÉ DE DEUX PARTIES

Soit $(E, \top)$ un magma et soient A et B deux parties de E. On note $A \top B$ l'ensemble des éléments de la forme $x \top y$, où $x \in A$ et $y \in B$.

Si la loi $\top$ est notée multiplicativement, on a

$$A.\,B = \{xy : x \in A,\ y \in B\}.$$

Si la loi est notée additivement, on a

$$A + B = \{x + y : x \in A,\ y \in B\}.$$

Si par exemple A se réduit à un élément x et si B est une partie quelconque de E, on écrit $x \top B$, soit xB en notation multiplicative et $x + B$ en notation additive.

2.1.4. TRANSLATIONS

2.1.4.1. Définition

Soient $(E, \top)$ *un magma et a un élément de E. On appelle* **translation à gauche** (resp. **à droite**) *définie par a, l'application* L_a (resp. R_a) *de E dans E* définie par :

$$x \longmapsto L_a(x) = a \top x \qquad (\text{resp. } x \longmapsto R_a(x) = x \top a).$$

En notation multiplicative, on écrit :

$$x \longmapsto L_a(x) = ax \quad \text{et} \quad x \longmapsto R_a(x) = xa$$

pour tout $x \in E$.

En notation additive, on écrit :

$$x \longmapsto L_a(x) = a + x \quad \text{et} \quad x \longmapsto R_a(x) = x + a.$$

2.2. Propriétés des lois de composition internes

2.2.1. LOIS ASSOCIATIVES

2.2.1.1. Définition

Soit $(E, \top)$ *un magma. On dit que la loi* $\top$ *est* **associative** *si l'on a*

$$(x \top y) \top z = x \top (y \top z)$$

quels que soient $x, y, z \in E$.

On écrit alors :

$$(x \top y) \top z = x \top (y \top z) = x \top y \top z,$$

et on dit que $(E, \top)$ est un **magma associatif.**

Par exemple, l'addition et la multiplication dans $\mathbb{R}$ sont des lois associatives.

Soit $(x_1, ..., x_n)$ une suite d'éléments d'un ensemble E muni d'une loi de composition associative $\top$. On définit par récurrence sur n, le composé de ces éléments en posant

$$x_1 \top x_2 \top ... \top x_n = (x_1 \top ... \top x_{n-1}) \top x_n.$$

En notation additive, on écrit

$$x_1 + x_2 + ... + x_n = \sum_{i=1}^{n} x_i.$$

En notation multiplicative, on écrit $x_1 \cdot x_2 \dots x_n = \prod_{i=1}^{n} x_i$

Si $x_1 = \dots = x_n = x$, $\sum_{i=1}^{n} x_i$ se note nx et le produit $x \cdot x \dots x$ (n facteurs) se note x^n. On dit que x^n est la **puissance** $n^{\text{ème}}$ de x.

On vérifie facilement que pour tout entier p tel que $1 \leq p \leq n$, on a la relation

$$x_1 \top x_2 \top \dots \top x_n = (x_1 \top \dots \top x_p) \top (x_{p+1} \top \dots \top x_n).$$

Si la loi de composition est notée multiplicativement, cette égalité s'écrit :

$$x_1 \cdot x_2 \dots x_n = (x_1 \cdot x_2 \dots x_p) \cdot (x_{p+1} \dots x_n).$$

On en déduit que, quels que soient les entiers positifs m et n et quel que soit $x \in E$, on a :

$$x^m \cdot x^n = x^{m+n} \quad \text{et} \quad (x^m)^n = x^{mn}.$$

En notation additive, ces formules s'écrivent :

$$mx + nx = (m+n)x \quad \text{et} \quad n(mx) = (nm)x.$$

2.2.2. LOIS COMMUTATIVES

2.2.2.1. Définition

Soit $(E, \top)$ un magma. On dit que la loi $\top$ est **commutative** *si l'on a $x \top y = y \top x$ quels que soient $x, y \in E$.*

Il peut arriver qu'une loi $\top$ n'étant pas commutative, il existe cependant des éléments x et y de E tels que $x \top y = y \top x$. On dit alors que ces éléments **commutent** ou encore qu'ils sont **permutables.**

On dit qu'un élément x de E est **central** si tout élément de E est permutable avec x. On appelle **centre** de E l'ensemble des éléments centraux.

2.2.2.2. Remarque

Soit $\top$ une loi de composition associative et commutative sur un ensemble E, et soit $(x_1, \dots, x_n)$ une suite d'éléments de E. On démontre par récurrence sur n, que le composé $x_1 \top x_2 \top \dots \top x_n$ est indépendant de l'ordre des facteurs.

Soit E un ensemble muni d'une addition et d'une multiplication associatives et commutatives. Soit x_{ij} le terme général d'une famille d'éléments de E telle que $1 \leq i \leq m$ et $1 \leq j \leq n$, i, j, m et n étant des entiers positifs. On suppose que i et j varient indépendamment l'un de l'autre.

Disposons les éléments x_{ij} sous la forme d'un tableau rectangulaire :

$$\begin{array}{cccc} x_{11} & x_{12} & \ldots\ldots & x_{1n} \\ x_{21} & x_{22} & \ldots\ldots & x_{2n} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ x_{m1} & x_{m2} & \ldots\ldots & x_{mn} \end{array}$$

Il est clair que, quel que soit l'ordre de sommation, la somme S des x_{ij} sera la même. On a donc

$$S = (x_{11} + x_{12} + \ldots + x_{1n}) + (x_{21} + x_{22} + \ldots + x_{2n}) + \ldots +$$
$$(x_{m1} + x_{m2} + \ldots + x_{mn}) = \sum_{j=1}^{n} x_{ij} + \sum_{j=1}^{n} x_{2j} + \ldots + \sum_{j=1}^{n} x_{mj} = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} x_{ij} \right).$$

D'autre part, cette même somme vaut

$$(x_{11} + x_{21} + \ldots + x_{m1}) + (x_{12} + x_{22} + \ldots + x_{m2}) + \ldots +$$
$$(x_{1n} + x_{2n} + \ldots + x_{mn}) = \sum_{i=1}^{m} x_{i1} + \sum_{i=1}^{m} x_{i2} + \ldots + \sum_{i=1}^{m} x_{in} = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} x_{ij} \right).$$

Par conséquent, on a

$$S = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} x_{ij} \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} x_{ij} \right)$$

que l'on écrit

$$S = \sum_{i=1}^{m} \sum_{j=1}^{n} x_{ij}.$$

2.2.3. ÉLÉMENT NEUTRE

2.2.3.1. Définition

Soit $(E, \top)$ un magma. On appelle **élément neutre** *pour la loi $\top$, tout élément $e \in E$ tel que l'on ait*

$$x \top e = e \top x$$

pour tout $x \in E$.

On appelle magma **unifère**, *un magma dont la loi de composition possède un élément neutre.*

Pour un tel magma, on pose par convention

$$\overset{0}{\top} x = e, \qquad \text{pour tout } x \in E.$$

2.2.3.2. Exemples

a) Dans $\mathbb{R}$, $e = 0$ est un élément neutre pour l'addition car quel que soit $x \in \mathbb{R}$, on a : $x + 0 = 0 + x = x$.

b) Dans $\mathbb{R}$, $e = 1$ est un élément neutre pour la multiplication car quel que soit $x \in \mathbb{R}$, on a :

$$x \cdot 1 = 1 \cdot x = x.$$

c) Id_E est un élément neutre pour la composition des applications dans $\mathcal{F}(E, E)$.

Une loi de composition peut ne pas admettre d'élément neutre. Toutefois, s'il existe, un tel élément est **unique.** En effet, si e et e' sont des éléments neutres pour la loi $\top$, alors on a $e \top e' = e'$ car e est élément neutre ; de même e' étant élément neutre, on a $e \top e' = e$. Donc $e = e'$.

Cette remarque nous permet de parler de l'élément neutre.

2.2.3.3. Définition

Soit $(E, \top)$ un magma. On dit qu'un élément $a \in E$ est **régulier** *(ou* **simplifiable) à gauche** *(resp.* **à droite**) *si la relation*

$$\begin{array}{ll} a \top x = a \top y & \text{entraîne } x = y \\ (resp. x \top a = y \top a & \text{entraîne } x = y) \end{array}$$

quels que soient $x, y \in E$.

On dit que a est **régulier** ou **simplifiable** s'il est régulier à gauche et à droite.

2.2.3.4. Exemples

a) Dans un magma unifère $(E, \top)$, l'élément neutre est régulier.

b) Dans $\mathbb{N}$ tout élément est régulier pour l'addition et tout élément non nul est régulier pour la multiplication.

2.2.4. ÉLÉMENTS SYMÉTRISABLES

2.2.4.1. Définition

Soit $(E, \top)$ un magma unifère d'élément neutre e. On appelle **symétrique à gauche** *(resp.* **symétrique à droite**) *d'un élément x de E, tout élément $y \in E$ tel que l'on ait*

$$y \top x = e \quad (\text{resp. } x \top y = e).$$

On appelle **symétrique** *de x tout élément y tel que*

$$y \top x = x \top y = e.$$

On dit que x est **symétrisable** *s'il admet un symétrique.*

Notation. Le symétrique d'un élément symétrisable x sera noté x'.

2.2.4.2. Théorème

Soient $(E, \top)$ un magma associatif et unifère, d'élément neutre e, et a un élément de E. Alors :

a) *Si a admet un symétrique à gauche (resp. un symétrique à droite), a est régulier à gauche (resp. à droite).*

b) *Si a admet un symétrique à gauche b et un symétrique à droite c, on a : $b = c$.*

c) *Si a est symétrisable, son symétrique a' est unique ; a' est aussi symétrisable et a' admet a pour symétrique.*

d) *Si deux éléments x et y sont symétrisables, il en est de même de $x \top y$, et on a*

$$(x \top y)' = y' \top x'.$$

Démonstration.

a) Supposons qu'il existe $b \in E$ tel que $b \top a = e$. Alors la relation $a \top x = a \top y$ implique $b \top (a \top x) = b \top (a \top y)$ et puisque la loi $\top$ est associative, on a $(b \top a) \top x = (b \top a) \top y$, c'est-à-dire $e \top x = e \top y$; d'où $x = y$.

b) Supposons qu'il existe $b \in E$ et $c \in E$ tels que $b \top a = e$ et $a \top c = e$. On en déduit, en utilisant l'associativité de $\top$:

$$b \top a \top c = (b \top a) \top c = e \top c = c$$
$$b \top a \top c = b \top (a \top c) = b \top e = b.$$

D'où $b = c$.

c) Si b et c sont deux symétriques de a, le calcul précédent montre que $b = c$. Soit a' le symétrique de a. Les relations

$$a' \top a = a \top a' = e$$

montrent que a' est symétrisable et que $(a')' = a$.

d) Si x et y admettent pour symétriques x' et y' respectivement, on a :

$$(y' \top x') \top (x \top y) = y' \top (x' \top x) \top y = y' \top e \top y = y' \top y = e,$$
$$(x \top y) \top (y' \top x') = x \top (y \top y') \top x' = x \top e \top x' = x \top x' = e$$

ce qui montre que $x \top y$ admet pour symétrique $y' \top x'$.

Remarquons que l'élément neutre e est toujours symétrisable et est égal à son symétrique.

Lorsque la loi de composition est notée multiplicativement, on parle d'**inverse** et d'élément **inversible** ; l'inverse d'un élément inversible x se note alors x^{-1}.

En notation additive, le symétrique de x s'appelle l'**opposé** de x et se note $-x$.

2.2.4.3. Théorème

Soit $(E, \top)$ un magma associatif unifère et soit a un élément symétrisable de E. Alors pour tout $b \in E$, l'équation

$$a \top x = b \qquad (\text{resp. } x \top a = b)$$

admet la solution unique $a' \top b$ (resp. $b \top a'$), a' désignant le symétrique de a.

Démonstration. La relation $a \top x = b$ implique $a' \top (a \top x) = a' \top b$, c'est-à-dire

$$a' \top b = (a' \top a) \top x = e \top x = x.$$

Réciproquement, si $x = a' \top b$, alors

$$a \top x = a \top (a' \top b) = (a \top a') \top b = e \top b = b.$$

La deuxième équation se traite de la même manière.

2.2.4.4. Théorème

Soit $(E, \top)$ un magma associatif unifère et soit a un élément symétrisable de E. Les translations à gauche L_a et $L_{a'}$ sont bijectives et inverses l'une de l'autre.

De même les translations à droite R_a et $R_{a'}$ sont bijectives et inverses l'une de l'autre.

Démonstration. Pour tout $x \in E$, on a

$$\begin{aligned} L_a \circ L_{a'}(x) &= L_a\left(L_{a'}(x)\right) = L_a(a' \top x) = a \top (a' \top x) \\ &= (a \top a') \top x = e \top x = x \\ L_{a'} \circ L_a(x) &= L_{a'}\left(L_a(x)\right) = L_{a'}(a \top x) = a' \top (a \top x) \\ &= (a' \top a) \top x = e \top x = x. \end{aligned}$$

Donc $L_a \circ L_{a'} = L_{a'} \circ L_a = Id_E$.

La démonstration pour les translations à droite se fait de la même manière.

2.2.5. DISTRIBUTIVITÉ

2.2.5.1. Définition

Soit E un ensemble muni de deux lois de composition internes notées $\top$ et $*$. On dit que la loi $\top$ est **distributive à gauche** (*resp.* **à droite**) *par rapport à la loi $*$ si l'on a :*

$$\begin{aligned} x \top (y * z) &= (x \top y) * (x \top z) \\ (\text{resp. } (y * z) \top x &= (y \top x) * (z \top x)) \end{aligned}$$

quels que soient $x, y, z \in E$.

Si la loi $\top$ est distributive à gauche et à droite par rapport à la loi $*$, on dit que $\top$ est **distributive par rapport à** $*$.

Par exemple, sur $\mathcal{P}(E)$, les lois $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre. De même dans $\mathbb{N}$, la multiplication est distributive par rapport à l'addition.

Si la loi $\top$ est commutative les trois notions de distributivité sont identiques.

2.2.6. LOI QUOTIENT

2.2.6.1. Définition

Soit $(E, \top)$ un magma et soit $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est **compatible** *avec $\top$ si quels que soient $x, x', y, y' \in E$, les relations $x\mathcal{R}x'$ et $y\mathcal{R}y'$ impliquent*

$$(x \top y)\mathcal{R}(x' \top y').$$

2.2.6.2. Exemple

Dans $\mathbf{Z}$, considérons la relation binaire: $x\mathcal{R}y$ si et seulement si, il existe $k \in \mathbf{Z}$ tel que $x - y = 2k$. Alors $\mathcal{R}$ est compatible avec l'addition de $\mathbf{Z}$.

2.2.6.3. Théorème

Soient $(E, \top)$ un magma et $\mathcal{R}$ une relation d'équivalence sur E. Si $\mathcal{R}$ est compatible avec $\top$, il existe une loi de composition interne $\dot{\top}$ sur l'ensemble quotient $E/\mathcal{R}$ telle que, quels que soient $x, y \in E$, on ait

$$\dot{x} \dot{\top} \dot{y} = cl(x \top y),$$

où $cl(x \top y)$ désigne la classe d'équivalence de l'élément $x \top y$. On dit que $\dot{\top}$ est la **loi quotient** *de $\top$ par $\mathcal{R}$.*

Démonstration. Soient $\dot{x}$ et $\dot{y}$ des éléments de $E/\mathcal{R}$. Définissons le composé $\dot{x} \dot{\top} \dot{y}$ en posant

$$\dot{x} \dot{\top} \dot{y} = cl(x \top y)$$

où x et y sont des représentants des classes $\dot{x}$ et $\dot{y}$ respectivement. Pour montrer que

$$(\dot{x}, \dot{y}) \longmapsto cl(x \top y)$$

est une application de $(E/\mathcal{R}) \times (E/\mathcal{R})$ dans $E/\mathcal{R}$, il faut s'assurer que $cl(x \top y)$ ne dépend que des classes $\dot{x}$ et $\dot{y}$ mais pas des représentants x de $\dot{x}$ et y de $\dot{y}$. Soient donc x' un autre représentant de $\dot{x}$ et y' un autre représentant de $\dot{y}$; on a $x\mathcal{R}x'$ et $y\mathcal{R}y'$. Comme la relation $\mathcal{R}$ est compatible avec la loi $\top$, on a $(x \top y)\mathcal{R}(x' \top y')$, d'où $cl(x \top y) = cl(x' \top y')$, et le théorème est démontré.

2.3. Morphismes

2.3.1. DÉFINITION. EXEMPLES

2.3.1.1. Définition

Soient E et F des ensembles, $\top$ et $*$ des lois de composition internes sur E et F respectivement. On dit qu'une application $f : E \longrightarrow F$ est un **morphisme** *(ou un* **homomorphisme***) de $(E, \top)$ dans $(F, *)$ si on a*

$$f(x \top y) = f(x) * f(y)$$

quels que soient $x, y \in E$.

Si $(E, \top) = (F, *)$, on dit que f est un **endomorphisme**.

Attention. Si $E = F$ mais si les lois $\top$ et $*$ sont différentes, on ne peut parler d'endomorphisme.

Si f est un morphisme bijectif de $(E, \top)$ sur $(F, *)$, on dit que f est un **isomorphisme**; on dit alors que E et F sont **isomorphes.**

Un isomorphisme de $(E, \top)$ sur lui-même s'appelle un **automorphisme** de $(E, \top)$.

2.3.1.2. Exemples

1) Prenons $(E, \top) = (\mathbb{R}, +)$ et $(F, *) = (\mathbb{R}, \times)$ et soit a un nombre réel > 0. L'application $x \longmapsto f(x) = a^x$ est un homomorphisme car on a

$$f(x + y) = a^{x+y} = a^x \cdot a^y = f(x)\, f(y)$$

quels que soient $x, y \in \mathbb{R}$.

2) $\mathbb{R}_+^*$ désignant l'ensemble des nombres réels strictement positifs, l'application $x \longmapsto \ln(x)$ ($\ln(x)$ désignant la fonction logarithme népérien) est un morphisme de $(\mathbb{R}_+^*, x)$ dans $(\mathbb{R}, +)$. En effet

$$\ln(xy) = \ln(x) + \ln(y) \quad \text{quels que soient } x, y \in \mathbb{R}_+^*.$$

2.3.1.3. Théorème

a) *Soient $(E, \top)$, $(F, *)$ et $G, \perp)$ trois magmas, f un morphisme de $(E, \top)$ dans $(F, *)$ et g un morphisme de $(F, *)$ dans $(G, \perp)$. Alors gof est un morphisme de $(E, \top)$ dans $(G, \top)$.*

b) *Si f est un morphisme bijectif de $(E, \top)$ sur $(F, *)$, l'application réciproque f^{-1} est un morphisme bijectif de $(F, *)$ sur $(E, \top)$.*

Démonstration.

a) On a quels que soient $x, y \in E$

$$\begin{aligned}(gof)\,(x \top y) &= g\,[f(x \top y)] = g\,[f(x) * f(y)] = g\,(f(x)) \perp g\,(f(y)) \\ &= (gof)(x) \perp (gof)(y)\ ,\end{aligned}$$

en utilisant la définition de gof et le fait que f et g sont des morphismes; cela prouve que gof est un morphisme de $(E, \top)$ dans $(G, \perp)$.

b) On sait déjà (Théorème 1.3.3.6) que f^{-1} est bijective si f est bijective. Soient $u, v \in F$; l'application f étant bijective, il existe des éléments x et y uniques de E tels que

$$f(x) = u \quad \text{et} \quad f(y) = v.$$

Alors $f^{-1}(u) = x$ et $f^{-1}(v) = y$.

f étant un homomorphisme, on a $f(x \top y) = f(x) * f(y) = u * v$.
Donc $f^{-1}(u * v) = x \top y = f^{-1}(u) \top f^{-1}(v)$
ce qui montre que f^{-1} est un morphisme.

2.4. Lois de composition externes

2.4.1. DÉFINITION. NOTATION

2.4.1.1. Définition

Soient E et Ω des ensembles. On appelle **loi de composition externe à gauche sur E, ayant pour domaine d'opérateurs** *l'ensemble Ω, toute application de $\Omega \times E$ dans E.*

On appelle **loi de composition externe à droite sur E, de domaine d'opérateurs Ω,** *toute application de $E \times \Omega$ dans E.*

Notation. Une loi de composition externe se note $(\alpha, x) \longmapsto \alpha \top x$ ou $(x, \alpha) \longmapsto x \top \alpha$ suivant le cas, le signe $\top$ pouvant être remplacé par un point (notation multiplicative).

Nous dirons en abrégé «soit $(E, \top)_\Omega$ une loi externe» au lieu de «soit $\top$ une loi de composition externe à gauche sur E, de domaine d'opérateurs l'ensemble Ω».

2.4.2. PARTIES STABLES. LOIS INDUITES

2.4.2.1. Définition

Soient $(E, \top)_\Omega$ une loi externe, et A une partie de E. On dit que A est **stable** *pour la loi $\top$ si l'on a :*

$$\alpha \top x \in A$$

quel que soit $(\alpha, x) \in \Omega \times A$.

L'application $(\alpha, x) \longmapsto \alpha \top x$ de $\Omega \times A$ dans A est donc une loi de composition externe sur A, de domaine d'opérateurs l'ensemble Ω. On l'appelle la **loi induite sur A par $\top$**.

2.4.3. RESTRICTION DU DOMAINE D'OPÉRATEURS

Soit $(E, \top)_\Omega$ une loi externe, et Ω' une partie de Ω. L'application $(\alpha, x) \longmapsto \alpha \top x$ de $\Omega' \times E$ dans E est une loi de composition externe sur E, ayant pour domaine d'opérateurs l'ensemble Ω'. On dit qu'on a **restreint** le domaine d'opérateurs.

Par exemple, un $\mathbb{C}$-espace vectoriel peut toujours être considéré comme un $\mathbb{R}$-espace vectoriel.

Nous verrons des exemples importants de lois externes lorsque nous étudierons les groupes opérant dans un ensemble et les espaces vectoriels.

Chapitre 3 : GROUPES

La théorie des groupes occupe une place très importante en mathématiques, avec des applications dans de nombreuses branches de la science : physique, chimie, sciences de l'ingénieur, cristallographie, etc.

Il n'est évidemment pas question de faire voir ici tous les développements mathématiques auxquels conduit la théorie des groupes ; nous nous proposons, simplement, d'exposer quelques notions élémentaires de cette théorie.

3.1. Généralités

3.1.1. DÉFINITIONS. EXEMPLES

3.1.1.1. Définition

On appelle **groupe**, *un ensemble G muni d'une loi de composition interne $(x, y) \longmapsto x * y$ possédant les propriétés suivantes :*

a) *Elle est associative :*
$x * (y * z) = (x * y) * z$ *quels que soient* $x, y, z \in G$.

b) *Elle admet un élément neutre* $e \in G$.

c) *Tout élément de G admet un symétrique : pour tout $x \in G$, il existe un élément x' de G, tel que*

$$x * x' = x' * x = e.$$

Si de plus, la loi de composition est commutative, le groupe est dit **commutatif** ou **abélien**. Dans ce cas la loi de composition est souvent notée additivement, l'élément neutre est désigné par 0 et le symétrique d'un élément x est noté $-x$.

Un groupe peut être fini ou infini. On appelle **ordre** d'un groupe fini le nombre de ses éléments.

Dans ce qui suit, nous noterons multiplicativement la loi de composition d'un groupe, sauf dans certains exemples particuliers ; l'élément neutre sera noté e.

Rappelons les résultats suivants que nous avons démontrés au Chapitre 2 et qui restent vrais pour les groupes (Théorème 2.2.4.2) :
— Tous les éléments d'un groupe sont réguliers ;
— Si x et y sont deux éléments d'un groupe G, on a $(xy)^{-1} = y^{-1}\, x^{-1}$.

3.1.1.2. Exemples

L'ensemble $\mathbb{R}$ des nombres réels est un groupe abélien pour l'addition. On l'appelle **le groupe additif des nombres réels.**

De même l'ensemble $\mathbf{Z}$ des entiers relatifs et l'ensemble $\mathbb{Q}$ des nombres rationnels sont des groupes abéliens pour l'addition.

3.1.1.3. Exemple

$\mathbb{R}^* = \mathbb{R} - \{0\}$ est un groupe abélien pour la multiplication.

De même $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ et $\mathbb{C}^* = \mathbb{C} - \{0\}$ sont des groupes abéliens pour la multiplication.

3.1.1.4. Exemple

Soient E un ensemble non vide, et $\mathcal{S}(E)$ l'ensemble des bijections de E sur E. Muni de la loi de composition interne $(f, g) \longmapsto fog$ (composition des applications), $\mathcal{S}(E)$ est un groupe, en général non abélien. On l'appelle le groupe des **permutations de** E ou le **groupe symétrique de** E. L'élément neutre est l'application identique Id_E. L'inverse de $f \in \mathcal{S}(E)$ est la bijection réciproque f^{-1} de f.

Lorsque E est l'ensemble $\{1, 2, ..., n\}$ des n premiers nombres entiers positifs, le groupe $\mathcal{S}(E)$ se note $\mathcal{S}_n$ et s'appelle le **groupe symétrique d'ordre** n ; c'est un groupe fini et on a $|\mathcal{S}_n| = n!$
(voir le Corollaire 1.7.2.3).

3.1.1.5. Exemple

Soient G_1 et G_2 deux groupes dont les lois sont notées multiplicativement. On définit sur l'ensemble produit $G = G_1 \times G_2$ une structure de groupe en posant, si $(x_1, x_2) \in G$ et $(y_1, y_2) \in G$:

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

On dit alors que G est le **produit direct** des groupes G_1 et G_2.

On verifiera à titre d'exercice que la multiplication définie par (3.1.1) est associative, qu'elle admet pour élément neutre $e = (e_1, e_2)$ où e_1 et e_2 sont les éléments neutres de G_1 et G_2 respectivement, et que tout élément $x = (x_1, x_2)$ de G admet pour inverse $x^{-1} = (x_1^{-1}, x_2^{-1})$.

De plus le groupe produit $G = G_1 \times G_2$ est abélien si et seulement si G_1 et G_2 sont abéliens.

On définirait de même le produit direct de n groupes $G_1, G_2, ..., G_n$. En particulier, lorsque $G_i = G$, $1 \leq i \leq n$, le groupe G^n est le groupe produit :

$$G^n = G \times G \times ... \times G, \qquad n \text{ facteurs.}$$

Par exemple, l'ensemble $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times ... \times \mathbb{R}$ (n facteurs), muni de la loi de composition :

$$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$$

est un groupe abélien.

3.2. Sous-groupes d'un groupe

3.2.1. DÉFINITION ET CARACTÉRISATION D'UN SOUS-GROUPE

3.2.1.1. Définition

On dit qu'une partie H d'un groupe G est un **sous-groupe** *de G si H vérifie les deux conditions suivantes :*

a) *H est non vide.*

b) *Les relations $x \in H$ et $y \in H$ entraînent $xy^{-1} \in H$.*

Le théorème suivant donne une caractérisation des sous-groupes.

3.2.1.2. Théorème

Soient G un groupe, et H une partie de G. Les propriétés suivantes sont équivalentes :

a) *H est un sous-groupe de G.*

b) *$e \in H$ et quels que soient $x, y \in H$, on a $x^{-1} \in H$ et $xy \in H$.*

Démonstration. a) $\Longrightarrow$ b). Comme H est non vide, il existe au moins un $x \in H$. Les relations $x \in H$ et $x \in H$ impliquent alors $xx^{-1} = e \in H$.

D'autre part, si $x \in H$, comme $e \in H$, on a $ex^{-1} = x^{-1} \in H$.

Enfin si $x, y \in H$, on a $y^{-1} \in H$ d'après ce qui précède et donc $x(y^{-1})^{-1} = xy \in H$.

b) $\Longrightarrow$ a) Si la condition b) est vérifiée, H est non vide car $e \in H$. D'autre part, si $x, y \in H$, H contient x et y^{-1}, donc aussi xy^{-1} ce qui montre que H est un sous-groupe de G.

Le théorème est donc démontré.

3.2.1.3. Remarques

a) Le sous-groupe H muni de la loi induite par la loi de composition définie sur G est un groupe.

Mais une partie stable d'un groupe n'est pas nécessairement un sous-groupe. Par exemple $\mathbb{N}$ est une partie stable de $\mathbb{Z}$ pour l'addition, mais ce n'est pas un sous-groupe de $\mathbb{Z}$.

b) Pour démontrer qu'un ensemble muni d'une loi de composition est un groupe, il est souvent recommandé de montrer que c'est un sous-groupe d'un groupe connu, ce qui abrège les démonstrations.

3.2.1.4. Exemple

Soit G un groupe. Alors G et $\{e\}$ sont des sous-groupes de G. Tout sous-groupe de G, distinct de G et $\{e\}$ s'appelle un **sous-groupe propre** de G.

3.2.1.5. Exemple

$\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-groupes propres du groupe additif $\mathbb{R}$.

3.2.1.6. Exemple

Soit $G = \mathbb{Z}$ et soit n un entier fixé. L'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupes de $\mathbb{Z}$. Réciproquement, si H est un sous-groupe de $\mathbb{Z}$, nous allons montrer qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Si $H = \{0\}$ l'assertion est évidente car H est alors l'ensemble des multiples de 0. Supposons donc que $H \neq \{0\}$. Soit $x \in H \cap \mathbb{Z}^*$; alors $-x \in H$, donc H contient des éléments strictement positifs. $H \cap \mathbb{N}^*$, partie non vide de $\mathbb{N}$, contient un plus petit élément que nous notons n. Nous allons montrer que $H = n\mathbb{Z}$.

La relation $n \in H$ entraîne $n\mathbb{Z} \subset H$ puisque H est stable pour l'addition et le passage à l'opposé.

Montrons que, réciproquement, tout élément de H appartient à $n\mathbb{Z}$. Pour tout $x \in H$, effectuons la division euclidienne de x par n :

$$x = nq + r \quad \text{avec} \quad 0 \leq r < n \quad \text{et} \quad q \in \mathbb{Z}.$$

On a $r = x - nq \in H$ puisque $x \in H$ et $nq \in n\mathbb{Z} \subset H$. Comme n est le plus petit élément positif de H et puisque $0 \leq r < n$, on a nécessairement $r = 0$ et $x = nq \in n\mathbb{Z}$, c'est-à-dire $H \subset n\mathbb{Z}$, ce qui achève la démonstration.

3.2.2. SOUS-GROUPE ENGENDRÉ PAR UNE PARTIE

3.2.2.1. Théorème

Soient G un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de G. Alors $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G.

Démonstration. H n'est pas vide puisque les sous-groupes H_i contiennent tous l'élément neutre e de G et par suite $e \in H$. Soient x et y deux éléments de H. Pour tout $i \in I$, $x \in H_i$ et $y \in H_i$, donc $xy^{-1} \in H_i$. Par suite $xy^{-1} \in H$ et H est bien un sous-groupe de G.

3.2.2.2. Exemple

La réunion de deux sous-groupes n'est un sous-groupe que si l'un d'eux est inclus dans l'autre. En effet si $x \in H_1 - H_2$ et $y \in H_2 - H_1$, alors $xy \notin H_1 \cup H_2$.

Soient G un groupe et A une partie de G. Il existe des sous-groupes de G contenant A (par exemple G lui-même). L'intersection de tous ces sous-groupes

est, d'après le Théorème 3.2.2.1, un sous-groupe de G contenant A et c'est le plus petit, au sens de l'inclusion. On l'appelle le **sous-groupe de G engendré par A** et on le note $[A]_G$ ou $[A]$.

3.2.2.3. Théorème

Soient G un groupe et A une partie de G. Alors $[A]$ est l'ensemble des produits finis d'éléments de G dont les termes ou leurs inverses sont dans A.

Démonstrations. Désignons par H l'ensemble des éléments x de G qui peuvent s'écrire

$$x = x_1\, x_2 \ldots x_p, \quad \text{avec } x_i \in A \text{ ou } x_i^{-1} \in A \text{ pour tout } i,$$

en convenant que $H = \{e\}$ si $A = \emptyset$.

Nous allons montrer que H est un sous-groupe de G contenant A et que tout sous-groupe de G qui contient A contient nécessairement H.

En prenant $p = 1$, on voit que $A \subset H$.

Si $A \neq \emptyset$ et si $a \in A$, $aa^{-1} = e \in H$, donc $H \neq \emptyset$ si $A \neq \emptyset$ et $H = \{e\}$ si $A = \emptyset$.

Si $x = x_1\, x_2 \ldots x_p$ et $y = y_1\, y_2 \ldots y_s$ appartiennent à H, avec $x_i \in A$ ou $x^{-1} \in A$ pour tout i et $y_j \in A$ ou $y_j^{-1} \in A$ pour tout j, on a

$$xy^{-1} = x_1\, x_2 \ldots x_p\, y_s^{-1} \ldots y_1^{-1} \in H.$$

Donc H est un sous-groupe de G contenant A.

Soit K un sous-groupe de G contenant A. Pour toute famille finie $(x_1, \ldots, x_p)$ d'éléments de A, $x_1^{-1}, \ldots, x_p^{-1}$ sont aussi des éléments de K ; il en est de même de tout produit de la forme $x_1 \cdot x_2 \ldots x_p$, avec $x_i \in A$ ou $x_i^{-1} \in A$.

Par conséquent tout sous-groupe de G qui contient A contient aussi H qui est bien le plus petit sous-groupe de G contenant A.

Par exemple si $A = \{x\}$ où $x \in G$, le sous-groupe de G engendré par x est le sous-goupe

$$H = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\},$$

où x^p es défini pour tout $x \in G$ et pour tout entier relatif p par :

$$x^p = x \ldots x \ (p \text{ fois}),\ x^{-p} = (x^{-1})^p = x^{-1} \ldots x^{-1} \ (p \text{ fois}) \text{ et } x^0 = e.$$

On appelle **ordre de x**, l'ordre du sous-groupe H engendré par x.

Le sous-groupe H engendré par x est abélien car $x^m \cdot x^n = x^{m+n}$ quels que soient $m, n \in \mathbf{Z}$.

3.2.2.4. Définition

Soit G un groupe. On dit qu'un sous-ensemble A de G est une **partie génératrice** *de G lorsque $[A] = G$.*

Si G admet une partie génératrice finie, on dit que G est un **groupe de type fini.**

On dit qu'un groupe G est **cyclique** *lorsqu'il peut être engendré par un seul élément x ; on dit alors que x est un* **générateur** *de G.*

D'après ce qui précède, tout groupe cyclique est abélien et de type fini.

3.3. Morphismes de groupes

3.3.1. DÉFINITIONS. EXEMPLES

3.3.1.1. Définition

Soient G et G' deux groupes. On appelle **morphisme** *ou* **homomorphisme** *de G dans G', toute application $f : G \longrightarrow G'$ telle que, pour tout $x \in G$ et pour tout $y \in G$, on ait :*

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

Si de plus f est bijectif, on dit que f est un **isomorphisme** et on dit alors que les groupes G et G' sont **isomorphes**.

Si $G = G'$ on dit que f est un **endomorphisme** ; un endomorphisme bijectif s'appelle un **automorphisme**.

3.3.1.2. Exemples

a) L'ensemble $\mathbb{R}_+^*$ des nombres réels strictement positifs est un groupe multiplicatif. L'application $x \longmapsto e^x$ est un homomorphisme du groupe additif $\mathbb{R}$ dans le groupe multiplicatif $\mathbb{R}_+^*$, car $e^{x+y} = e^x \cdot e^y$.

On sait d'après le cours d'analyse, que la fonction exponentielle est un isomorphisme de $\mathbb{R}$ sur $\mathbb{R}_+^*$, l'isomorphisme réciproque étant la fonction logarithmique $x \longmapsto \ln(x)$.

b) Soient G un groupe et a un élément de G. L'application $n \longmapsto a^n$, de $\mathbf{Z}$ dans G, est un morphisme du groupe additif $\mathbf{Z}$ dans G car $a^{m+n} = a^m a^n$.

3.3.1.3. Exemple

Soit G un groupe. Pour tout $a \in G$, l'application f_a de G dans G définie par

$$f_a(x) = axa^{-1}$$

est un automorphisme de G. On a en effet

$$f_a(xy) = axya^{-1} = (axa^{-1})\,(aya^{-1}) = f_a(x)\, f_a(y)$$

quels que soient $x, y \in G$ et f_a est un homomorphisme.

Montrons que f_a est bijectif. Pour tout $y \in G$, on a $f_a(x) = y$ avec $x = a^{-1}ya$, donc f_a est surjectif. f_a est aussi injectif car l'équation $axa^{-1} = aya^{-1}$ admet la solution unique $x = y$.

Les automorphismes de la forme f_a s'appellent les **automorphismes intérieurs de** G.

Les automorphismes intérieurs de G se réduisent à l'application identique si G est abélien.

3.3.2. PROPRIÉTÉS DES MORPHISMES DE GROUPES

Nous allons énoncer quelques propriétés des morphismes de groupes. Certaines ne sont que des rappels du Chapitre 2.

3.3.2.1. Théorème

Soient G, G' et K trois groupes, f un morphisme de G dans G' et g un morphisme de G' dans K. Alors

a) *gof est un morphisme de G dans K.*

b) *Si f est un isomorphisme de G sur G', l'application réciproque f^{-1} est un isomorphisme de G' sur G.*

La démonstration est identique à celle du Théorème 2.3.2.1.

3.3.2.2. Théorème

Soit f un homomorphisme d'un groupe G dans un groupe G'. Alors

a) *Si e est l'élément neutre de G et e' l'élément neutre de G', on a $f(e) = e'$.*

b) *Si $x \in G$, on a $f(x^{-1}) = \big(f(x)\big)^{-1}$.*

c) *L'image par f de tout sous-groupe de G est un sous-groupe de G'.*

d) *L'image réciproque par f de tout sous-groupe de G' est un sous-groupe de G.*

Démonstration.

a) Pour tout $x \in G$, on a

$$f(x) = f(xe) = f(x)\, f(e),$$

d'où
$$f(e) = \big(f(x)\big)^{-1}\ f(x) = e'$$

b) De même pour tout $x \in G$, on a

$$f(x)\, f(x^{-1}) = f(xx^{-1}) = f(e) = e'$$
$$f(x^{-1})\, f(x) = f(x^{-1}x) = f(e) = e';$$

donc
$$f(x^{-1}) = \big(f(x)\big)^{-1}.$$

c) Soit H un sous-groupe de G et soit $H' = f(H)$. H' est non vide car $e' = f(e) \in f(H)$.

Si $u, v \in H'$, il existe $x, y \in H$ tels que $u = f(x)$ et $v = f(y)$; alors

$$uv^{-1} = f(x)\ \left(f(y)\right)^{-1} = f(x)\ f(y^{-1}) = f(xy^{-1}).$$

Comme $xy^{-1} \in H$, puisque H est un sous-groupe de G, on voit que $uv^{-1} \in H'$ et H' est un sous-groupe de G'.

d) Soit B' un sous-groupe de G' et soit $B = f^{-1}(B')$.

On a $e \in B$, car $f(e) = e' \in B'$, donc $B \neq \emptyset$. Si $x \in B$ et $y \in B$, on a par définition de l'image réciproque $f(x) \in B'$ et $f(y) \in B'$. On en déduit :

$$f(xy^{-1}) = f(x)\ f(y^{-1}) = f(x)\ \left(f(y)\right)^{-1} \in B'$$

car B' est un sous-groupe de G'. Donc $xy^{-1} \in B$, ce qui achève la démonstration du théorème.

Le théorème 3.3.2.2 montre que si f est un homomorphisme de G dans G', alors $f(G)$ est un sous-groupe de G' ; ce sous-groupe s'appelle l'**image** de f et on le note $\mathrm{Im}(f)$.

De même l'ensemble $f^{-1}\left(\{e'\}\right)$ formé des $x \in G$ tels que $f(x) = e'$ est un sous-groupe de G ; on l'appelle le **noyau de** f et on le note $\mathrm{Ker}(f)$.

3.3.2.3. Remarque

D'après le Théorème 3.3.2.2, **c)**, l'image aHa^{-1} d'un sous-groupe H par un automorphisme intérieur f_a est un sous-groupe de G. Tout sous-groupe de la forme aHa^{-1}, avec $a \in G$, est dit **conjugué** de H.
vspace-0.5mm

3.3.2.4. Théorème

Soient G et G' deux groupes et soit f un homomorphisme de G dans G'. Pour que f soit injectif, il faut et il suffit que $\mathrm{Ker}(f) = \{e\}$.

Démonstration. Supposons que f soit injectif. Comme $e \in \mathrm{Ker}(f)$, s'il existait un autre élément $x \in \mathrm{Ker}(f)$, on aurait $f(x) = e' = f(e)$, d'où $x = e$ puisque f est injectif ; donc $\mathrm{Ker}(f) = \{e\}$.

Réciproquement, supposons que $\mathrm{Ker}(f) = \{e\}$ et soient $x, y \in G$ tels que $f(x) = f(y)$. Cette relation entraîne

$$f(x)\ f(y)^{-1} = f(x)\ f(y^{-1}) = f(xy^{-1}) = f(y)\ f(y)^{-1} = e' ;$$

donc $xy^{-1} \in \mathrm{Ker}(f) = \{e\}$, d'où $xy^{-1} = e$, c'est-à-dire $x = y$ et f est injectif.

3.4. Groupes-quotients

3.4.1. CLASSES MODULO UN SOUS-GROUPE

3.4.1.1. Théorème

Soient G un groupe et H un sous-groupe de G. Alors :

a) *La relation $x\mathcal{R}y$ si et seulement si $x^{-1}y \in H$ est une relation d'équivalence sur G.*

b) *La classe de x modulo $\mathcal{R}$ est l'ensemble xH.*

Démonstration.

a) Pour tout $x \in G$, on a $x^{-1}x = e \in H$; donc la relation $\mathcal{R}$ est réflexive.

Si $x^{-1}y \in H$, alors $(x^{-1}y)^{-1} \in H$, c'est-à-dire $y^{-1}x \in H$. Donc $x\mathcal{R}y$ implique $y\mathcal{R}x$ et $\mathcal{R}$ est symétrique.

Si $x^{-1}y \in H$ et $y^{-1}z \in H$, alors $(x^{-1}y)\,(y^{-1}z) \in H$, c'est-à-dire $x^{-1}z \in H$. Donc $x\mathcal{R}y$ et $y\mathcal{R}z$ impliquent $x\mathcal{R}z$ et la relation $\mathcal{R}$ est transitive, ce qui démontre a).

b) Par définition, la classe de $x \in G$ est l'ensemble de $y \in G$ tels que $x^{-1}z \in H$. Posons $x^{-1}y = z$; alors $y = xz$ avec $z \in H$, donc $y \in xH$.

Réciproquement, si $y \in xH$, on a $y = xz$ avec $z \in H$, donc $x^{-1}y = x^{-1}xz = z \in H$.

La classe de x est bien l'ensemble xH.

3.4.1.2. Remarque

Si on remplace la relation $x^{-1}y \in H$ par la relation $yx^{-1} \in H$, on obtient un théorème analogue au Théorème 3.4.1 mais l'ensemble xH est remplacé par Hx. Cette remarque nous amène à poser la définition suivante.

3.4.1.3. Définition

L'ensemble xH s'appelle une **classe à gauche modulo** H ; *l'ensemble Hx s'appelle une* **classe à droite modulo** H.

L'ensemble des classes xH (resp. Hx) modulo H se note G/H (resp. $H\backslash G$).

Donc $\quad G/H = \{xH : x \in G\} \quad$ et $\quad H\backslash G = \{Hx : x \in G\}$.

Lorsque G est abélien, les classes à gauche coïncident avec les classes à droite. Dans ce cas on note $x + H$ la classe de x.

3.4.1.4. Exemple

Prenons pour G le groupe additif $\mathbf{Z}$ et pour H le sous-groupe $n\mathbf{Z}$, où n est un entier strictement positif fixé. La relation d'équivalence s'écrit ici

$$y - x \in n\mathbf{Z} \quad \text{ou} \quad x \equiv y \pmod{n}.$$

La classe d'équivalence d'un élément $x \in \mathbf{Z}$ est

$$\dot{x} = \{..., x - 2n, x - n, x, x + n, ...\}.$$

L'ensemble quotient est noté $\mathbf{Z}/n\mathbf{Z}$.

3.4.1.5. Théorème

Soient G un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.

Démonstration. Remarquons d'abord que pour toute classe à gauche xH modulo H, l'application $y \longmapsto xy$ de H dans xH est bijective. Cette application est injective car si $xy_1 = xy_2$ avec $y_1, y_2 \in H$ alors puisque x^{-1} existe, on a $x^{-1}(xy_1) = x^{-1}(xy_2)$ d'où $y_1 = y_2$; elle est surjective par définition même des classes d'équivalence.

Donc H étant fini puisque G l'est, chaque classe xH possède autant d'éléments que H. Comme les classes xH forment une partition de G, le nombre d'éléments de G est égal au produit du nombre d'éléments de H par le nombre de classes xH distinctes.

3.4.1.6. Corollaire

Soit G un groupe fini d'ordre p premier. Alors les seuls sous-groupes de G sont $\{e\}$ et G lui-même.

3.4.2. GROUPES-QUOTIENTS

3.4.2.1. Définition

On dit qu'un sous-groupe H d'un groupe G est **distingué**, *ou* **normal**, *ou* **invariant** *si pour tout $x \in G$, on a $xH = Hx$.*

Autrement dit H est un sous-groupe distingué de G si et seulement si la classe à gauche de tout $x \in G$ coïncide avec sa classe à droite.

Il est clair que dans un groupe abélien tout sous-groupe est distingué.

Le résultat suivant donne une caractérisation des sous-groupes distingués.

3.4.2.2. Théorème

Soient G un groupe et H un sous-groupe de G. Les conditions suivantes sont équivalentes.

a) *H est distingué.*

b) *Pour tout $x \in G$, on a $xHx^{-1} = H$.*

c) *Pour tout $x \in G$, on a $xHx^{-1} \subset H$.*

Démonstration. Il est clair que **a)** $\Longleftrightarrow$ **b)** et **b)** $\Longrightarrow$ **c)**. Il reste donc à montrer que **c)** $\Longrightarrow$ **a)**. Supposons la condition **c)** vérifiée. Pour tout $x \in G$, on a alors

$$xH(x^{-1}x) \subset Hx, \quad \text{i.e.} \quad xH \subset Hx.$$

En changeant x en x^{-1} dans la relation $xHx^{-1} \subset H$, il vient $x^{-1}Hx \subset H$, d'où comme précédemment, $Hx \subset xH$; par suite on a $xH = Hx$ et le théorème est démontré.

Soient G un groupe et H un sous-groupe distingué de G. Nous allons voir que l'ensemble quotient G/H peut être muni d'une structure de groupe.

3.4.2.3. Théorème

Soient G un groupe et H un sous-groupe distingué de G. La relation d'équivalence $x\mathcal{R}y$ si et seulement si $x^{-1}y \in H$ est compatible avec la loi de G et l'ensemble quotient G/H, muni de la loi quotient, est un groupe appelé **groupe-quotient** *de G par H. Si, de plus, G est abélien, alors G/H est abélien.*

Démonstration. Montrons tout d'abord que la relation $\mathcal{R}$ est compatible avec la multiplication de G, c'est-à-dire que les relations $x\mathcal{R}x'$ et $y\mathcal{R}y'$ impliquent $(xy)\mathcal{R}(x'y')$, ou encore que $x^{-1}x' \in H$ et $y^{-1}y' \in H$ impliquent $(xy)^{-1}(x'y') \in H$.

Des relations $x^{-1}x' \in H$ et $y^{-1}y' \in H$, on déduit qu'il existe $h,\ k \in H$ tels que $x' = xh$ et $y' = yk$.

Alors $\quad (xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = y^{-1}x^{-1}xhyk = y^{-1}hyk.$

Comme H est un sous-groupe distingué, $y^{-1}hy \in H$ et puisque $k \in H$, $y^{-1}hyk \in H$ car H est stable pour la loi de G.

On peut donc définir une loi quotient (notée encore multiplicativement) dans G/H, en posant

$$(xH)(yH) = (xy)H$$

quels que soient $\dot{x} = xH \in G/H$ et $\dot{y} = yH \in G/H$, le résultat ne dépendant pas des représentants choisis dans $\dot{x}$ et dans $\dot{y}$ (voir le Théorème 2.2.6.3).

Il est clair que si G est abélien, alors

$$(xH)(yH) = (yH)(xH).$$

Montrons que G/H, muni de la loi quotient est un groupe. On a

$$\begin{aligned}[(xH)(yH)](zH) &= ((xy)H)(zH) = [(xy)z]H = [x(yz)]H \\ &= (xH)[(yz)H] = (xH)[(yH)(zH)]\end{aligned}$$

quels que soient $x, y, z \in G$, d'où l'associativité de la loi quotient.

La classe $eH = H$ est l'élément neutre car pour tout $x \in G$, on

$$(xH)\,(eH) = (xe)H = xH = (ex)H = (eH)\,(xH).$$

Enfin, l'inverse de la classe xH est la classe $x^{-1}H$. En effet, on a

$$(xH)\,(x^{-1}H) = (xx^{-1})H = eH = (x^{-1}x)H = (x^{-1}H)\,(xH),$$

ce qui achève la démonstration du théorème.

Notons que, par définition de la multiplication dans G/H, l'application canonique $\pi : G \longrightarrow G/H$ est un homomorphisme de groupes car

$$\pi(xy) = (xy)H = (xH)\,(yH) = \pi(x)\,\pi(y);$$

c'est pourquoi, on dit parfois que π est **l'homomorphisme canonique**. On notera également que H est le noyau de π car pour tout $x \in H$, on a $\pi(x) = xH = H$.

3.4.2.4. Remarque

Il est clair que H est un sous-groupe distingué d'un groupe G si et seulement si on a $\sigma_a(H) = H$ pour tout automorphisme intérieur σ_a de G, ce qui justifie la terminologie « sous-groupe invariant ».

3.4.2.5. Théorème

Soit f un morphisme du groupe G dans le groupe G'. Alors $N = \mathrm{Ker}(f)$ est un sous-groupe distingué de G.

Démonstration. Nous savons déjà (Théorème 3.3.2.2) que N est un sous-groupe de G. Quel que soit $x \in G$ et quel que soit $h \in N$, on a

$$f(xhx^{-1}) = f(x)\,f(h)\,f(x^{-1}) = f(x)\,e'\,f(x)^{-1} = e',$$

où e' désigne l'élément neutre de G'.

Donc $xNx^{-1} \subset N$ et par suite, N est un sous-groupe distingué de G.

3.4.3. DÉCOMPOSITION CANONIQUE D'UN HOMOMORPHISME

Nous avons vu au Chapitre 1 (Théorème 1.4.2.6) comment décomposer une application. Dans le cas des morphismes de groupes, on peut préciser un peu mieux les choses.

3.4.3.1. Théorème

Soient G et G' deux groupes, f un homomorphisme de G dans G', π l'homomorphisme canonique de G sur $G/\mathrm{Ker}(f)$ et j l'injection canonique

de $f(G)$ dans G'. Alors il existe un isomorphisme unique $\overline{f}$ du groupe-quotient $G/\mathrm{Ker}(f)$ sur le sous-groupe $f(G)$ de G' tel que $f = j o \overline{f} o \pi$.

Démonstration. La décomposition canonique se fait, dans le cas général, en considérant la relation d'équivalence associée à f : $x \mathcal{R} y$ si et seulement si $f(x) = f(y)$. Ici, cette relation devient

$$\begin{aligned} x \mathcal{R} y &\iff f(x) = f(y) \\ &\iff e' = f(x)^{-1} f(x) = f(x)^{-1} f(y) = f(x^{-1}) f(y) = f(x^{-1} y). \end{aligned}$$

Donc $$x \mathcal{R} y \iff x^{-1} y \in \mathrm{Ker}(f).$$

On reconnaît la relation d'équivalence modulo le sous-groupe $\mathrm{Ker}(f)$. On obtient donc la bijection $\overline{f} : G/\mathrm{Ker}(f) \longrightarrow f(G)$ définie par

$$\overline{f}(\overline{x}) = f(x)$$

pour tout $\overline{x} \in G/\mathrm{Ker}(f)$, où $\overline{x}$ désigne la classe de x (Théorème 1.4.2.6).

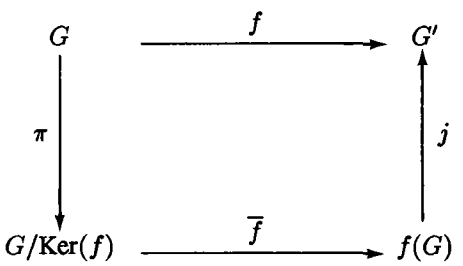
Comme $\mathrm{Ker}(f)$ est un sous-groupe distingué de G, $G/\mathrm{Ker}(f)$ est un groupe. L'application canonique π et l'injection canonique j sont des homomorphismes de groupes. $\overline{f}$ est aussi un homomorphisme car on a, quels que soient $\overline{x}, \overline{y} \in G/\mathrm{Ker}(f)$,

$$\overline{f}(\overline{x}\,\overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x) f(y) = \overline{f}(\overline{x})\,\overline{f}(\overline{y}).$$

Ainsi $\overline{f}$ est un homomorphisme bijectif, c'est-à-dire un isomorphisme de $G/\mathrm{Ker}(f)$ sur $f(G)$. La factorisation canonique de f s'écrit

$$f = j o \overline{f} \, o \, \pi$$

et on a le diagramme



3.4.3.2. Exemple

Soit n un entier ≥ 1. Alors, comme $n\mathbf{Z}$ est un sous-groupe abélien, donc distingué de $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$ est un groupe abélien pour la loi quotient $\overline{x} + \overline{y} = \overline{x} + \overline{y}$, où $\overline{x}$ désigne la classe de x.

Montrons que la restriction π_n de l'homomorphisme canonique π à l'ensemble $\{0, 1, ..., n-1\}$ est une bijection.

La relation $\pi_n(x) = \pi_n(y)$ avec $0 \leq x \leq n-1$ et $0 \leq y \leq n-1$ implique

$$\pi(x-y) = 0 \quad \text{et} \quad x - y \in n\mathbf{Z}.$$

Or le seul multiple de n dans l'intervalle $[0, n-1]$ est 0 ; donc $x - y = 0$, i.e. $x = y$, donc π_n est injective.

Montrons que π_n est surjective. Soit $\overline{x} \in \mathbf{Z}/n\mathbf{Z}$ et soit x un représentant de $\overline{x}$. La division euclidienne de x par n donne :

$$x = nq + r \quad \text{avec} \quad 0 \leq r < n.$$

D'où, puisque $n\mathbf{Z}$ est le noyau de π, et que $nq \in n\mathbf{Z}$,

$$\pi(x) = \pi(nq) + \pi(r) = \pi(r) = \pi_n(r),$$

ce qui montre que π_n est surjective, donc bijective.

Le groupe quotient $\mathbf{Z}/n\mathbf{Z}$ contient donc n éléments, à savoir $\pi(0), \pi(1), \ldots, \pi(n-1)$. On dit que $\mathbf{Z}/n\mathbf{Z}$ est le **groupe des entiers modulo** n.

Pour abréger, nous noterons $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ les éléments de $\mathbf{Z}/n\mathbf{Z}$, $n \geq 1$.

Dressons par exemple la table d'addition du groupe $\mathbf{Z}/4\mathbf{Z}$.

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

A l'intersection de la ligne $\overline{n}$ et de la colonne $\overline{m}$ figure l'élément $\overline{n} + \overline{m}$.

3.4.3.3. Exemple

Soit $\mathbf{U}$ le groupe multiplicatif des nombres complexes de module 1. L'application $f \longmapsto e^{ix}$ de $\mathbb{R}$ dans $\mathbf{U}$ est un homomorphisme surjectif dont le noyau est le groupe $2\pi\mathbf{Z}$. Le groupe quotient $\mathbb{R}/2\pi\mathbf{Z} = \mathbf{T}$ s'appelle le **tore à une dimension** ou encore le **groupe des nombres réels modulo** 2π. D'après le Théorème 3.4.3.1, $\mathbb{R}/2\pi\mathbf{Z}$ est isomorphe à $\mathbf{U}$.

3.4.4. APPLICATION AUX GROUPES CYCLIQUES

3.4.4.1. Théorème

Soit G un groupe cyclique.

a) *Si G est infini, il est isomorphe à $\mathbf{Z}$.*

b) *Si G est fini d'ordre n, il est isomorphe au groupe additif $\mathbf{Z}/n\mathbf{Z}$.*

Démonstration.

a) Soit x un générateur de G; tout élément de G est donc de la forme x^k avec $k \in \mathbf{Z}$. Il en résulte que l'homomorphisme $f : \mathbf{Z} \longrightarrow G$ défini par $f(n) = x^n$ est surjectif. Son noyau est un sous-groupe de $\mathbf{Z}$, donc de la forme $a\mathbf{Z}$ avec $a \geq 0$ (Exemple 3.2.1.7). D'après le Théorème 3.4.3.1, G est isomorphe au groupe quotient $\mathbf{Z}/\mathrm{Ker}(f)$.

Si G est infini, il en est de même de $\mathbf{Z}/\mathrm{Ker}(f)$, ce qui exige $a = 0$; alors (Thorème 3.3.2.4), f est injectif, donc f est bijectif, et le groupe G est isomorphe à $\mathbf{Z}$.

b) Si G est fini, d'ordre n, $\mathbf{Z}/\mathrm{Ker}(f)$ est aussi d'ordre n, ce qui exige $a = n$, donc G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

Dans ce cas, on a $G = \{x^0 = e, x, x^2, ..., x^{n-1}\}$.

3.4.4.2. Corollaire

Soient G un groupe et x un élément de G. Les propriétés suivantes sont équivalentes :

a) *x est d'ordre fini m.*

b) *m est le plus petit entier naturel non nul tel que $x^m = e$.*

Démonstration. a) $\Longrightarrow$ **b)** Considérons le morphisme $f : \mathbf{Z} \longrightarrow G$ utilisé précédemment. Soit $H = \mathrm{Im}(f)$ le sous-groupe de G engendré par x. Par hypothèse H est fini. Le noyau de f est un sous-groupe de $\mathbf{Z}$, donc de la forme $p\mathbf{Z}$, p étant le plus petit élément positif non nul de $\mathrm{Ker}(f)$. D'après le Théorème 3.4.3.1, H est isomorphe à $\mathbf{Z}/p\mathbf{Z}$, ce qui exige $p = m$ et m est le plus petit élement positif non nul de $\mathrm{Ker}(f)$, c'est-à-dire le plus petit entier naturel non nul tel que $x^m = e$.

b) $\Longrightarrow$ **a)** Par hypothèse m est le plus petit élément positif non nul de $\mathrm{Ker}(f)$. Donc $\mathrm{Ker}(f) = m\mathbf{Z}$ et H est isomorphe à $\mathbf{Z}/m\mathbf{Z}$, donc est d'ordre fini m.

3.4.4.3. Corollaire

Soit G un groupe fini d'ordre n. Alors, on a $x^n = e$ pour tout $x \in G$.

Démonstration. Soit $x \in G$ et soit H le sous-groupe de G engendré par x. L'ordre m de H est fini puisque H est un sous-groupe du groupe fini G. Donc (Théorème 3.4.1.5) il existe un entier p tel que $n = mp$. Comme $x^m = e$, il vient $x^n = (x^m)^p = e^p = e$.

3.4.4.4. Corollaire

Tout groupe G d'ordre p premier est cyclique ; il est engendré par l'un quelconque de ses éléments autre que l'élément neutre e.

Démonstrations. Soient x un élément de G distinct de e et H le sous-groupe de G engendré par x. Alors (Corollaire 3.4.1.6), $H = \{e\}$ ou $H = G$; comme $x \neq e$, on a nécessairement $H = G$. Donc G est cyclique. D'après le Théorème 3.4.4.1, G est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

3.5. Groupes symétriques

3.5.1. GÉNÉRALITÉS

Rappelons que si E est un ensemble ayant n éléments, l'ensemble $\mathcal{S}(E)$ des permutations de E, muni de la composition des applications est un groupe ayant $n!$ éléments.

3.5.1.1. Théorème

Soient E et F deux ensembles, et f une bijection de E sur F. Alors l'application $\Psi : \mathcal{S}(E) \longrightarrow \mathcal{S}(F)$ définie par $\Psi(h) = fohof^{-1}$ est un isomorphisme de groupes.

Démonstrations. Il est clair que $\emptyset(h) \in \mathcal{S}(F)$ pour tout $h \in \mathcal{S}(E)$. D'autre part, on a

$$\emptyset(hoh') = fo(hoh')of^{-1} = (fohof^{-1}) \, o \, (foh'of^{-1}) = \emptyset(h) \, o \, \emptyset(h').$$

Enfin $\emptyset$ est bijective car tout élément h' de $\mathcal{S}(F)$ est l'image d'un élément et d'un seul de $\mathcal{S}(E)$, à savoir $f^{-1}oh'of$.

Si n est un entier positif, nous noterons $\mathbb{N}_n$ l'intevalle $[1, n]$. Donc si E est un ensemble fini, de cardinal n, il existe une bijection de E sur $\mathbb{N}_n$ et d'après le théorème précédent, $\mathcal{S}(E)$ est isomorphe au groupe symétrique $\mathcal{S}_n$ d'ordre n. Cette remarque permet de ne s'intéresser qu'au groupe $\mathcal{S}_n$.

Notation. Si $\sigma \in \mathcal{S}_n$, on convient d'écrire

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}. \tag{3.5.1}$$

On appelle **permutation circulaire** la permutation

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ 2 & 3 & \ldots & 1 \end{pmatrix}$$

où chaque élément sauf n, a pour image par τ le suivant, l'image de n étant 1.

3.5.1.2. Théorème

Le groupe $\mathcal{S}_n$ n'est pas commutatif si $n \geq 3$.

Démonstration. Il suffit d'exhiber deux éléments de $\mathcal{S}_n$ qui ne commutent pas.

Considérons les deux permutations σ et σ' suivantes qui laissent invariants tous les éléments de $[1, n]$ autres que a, b et c.

$$\sigma = \begin{pmatrix} a & b & c & x & \dots & z \\ b & a & c & x & \dots & z \end{pmatrix}, \quad \sigma' = \begin{pmatrix} a & b & c & x & \dots & z \\ c & b & a & x & \dots & z \end{pmatrix}$$

On a

$$\sigma o \sigma' = \begin{pmatrix} a & b & c & x & \dots & z \\ c & a & b & x & \dots & z \end{pmatrix}$$

$$\sigma' o \sigma = \begin{pmatrix} a & b & c & x & \dots & z \\ b & c & a & x & \dots & z \end{pmatrix},$$

donc $\sigma o \sigma' \neq \sigma' o \sigma$.

3.5.2. TRANSPOSITIONS

3.5.2.1. Définition

Soit n un entier naturel ≥ 2. On dit qu'une permutation $\tau \in \mathcal{S}_n$ est une **transposition** *s'il existe deux entiers distincts i et j de $\mathbb{N}_n$ tels que*

$$\tau(i) = j, \quad \tau(j) = i \quad \text{et} \quad \tau(k) = k \quad \text{pour} \quad k \neq i \quad \text{et} \quad k \neq j.$$

On note τ_{ij} la transposition qui échange i et j et qui laisse fixes les autres éléments de $\mathbb{N}_n$.

On remarquera que si τ est une transposition alors $\tau o \tau = Id_{\mathbb{N}_n}$, i.e. $\tau = \tau^{-1}$.

3.5.2.2. Théorème

Si $n \geq 2$, tout élément de $\mathcal{S}_n$ peut s'écrire comme composé de transpositions.

Démonstrations. Nous allons démontrer ce résultat par récurrence sur n.

Si $n = 2$, $\mathcal{S}_2$ contient les deux éléments

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{et} \quad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

e est l'application identique de $\mathbb{N}_2$, τ est une transposition et on a

$$e = \tau o \tau.$$

Supposons le théorème vrai pour tout élément de $\mathcal{S}_{n-1}$ et démontrons-le pour $\mathcal{S}_n$.

Soit σ une permutation de $\mathbb{N}_n$ et soit i un élément quelconque de $\mathbb{N}_n$. Posons

$$A = \mathbb{N}_n - \{i\}.$$

A contient $n-1$ éléments. Il y a deux éventualités, ou $\sigma(i) = i$, ou $\sigma(i) \neq i$.

a) $\sigma(i) = i$.

Alors la restriction σ' de σ à A est une permutation de A. D'après l'hypothèse de récurrence, il existe des transpositions $\sigma_1, \sigma_2, \ldots, \sigma_p$ dans $\mathcal{S}_{n-1}$ telles que

$$\sigma' = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_p.$$

Posons

$$\tau_j(x) = \begin{cases} \sigma_j(x) & \text{si} \quad x \in A \\ i & \text{si} \quad x = i \end{cases}$$

Comme les σ_j sont des éléments de $\mathcal{S}_{n-1}$, les τ_j sont des transpositions, éléments de $\mathcal{S}_n$. On a alors

$$\sigma = \tau_1 \circ \tau_2 \circ \ldots \tau_p$$

et σ est bien la composée de transpositions $\tau_j \in \mathcal{S}_n$.

b) $\sigma(i) = j \neq i$.

Soit $\tau \in \mathcal{S}_n$ la transposition de $\mathbb{N}_n$ qui échange i et j et qui laisse fixes tous les autres éléments de $\mathbb{N}_n$. Alors $\tau \circ \sigma \in \mathcal{S}_n$ et on a

$$(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \tau(j) = i.$$

D'après le premier cas, il existe des transpositions $\tau_1, \tau_2, \ldots, \tau_p$ dans $\mathcal{S}_n$ telles que

$$\tau \circ \sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_p.$$

En composant à gauche par $\tau = \tau^{-1}$, il vient

$$\sigma = \tau \circ \tau_1 \circ \ldots \circ \tau_p \quad \text{et le théorème est démontré.}$$

3.5.2.3. Remarque

La décomposition de $\sigma \in \mathcal{S}_n$ en produit de transpositions n'est pas unique. Par exemple si

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

on a $$\sigma = \tau_{2,3} \circ \tau_{1,3} \circ \tau_{2,3} = \tau_{1,2} \circ \tau_{2,3}.$$

Cependant, nous allons voir que si σ est fixé, la parité du nombre de ces transpositions dans une décomposition quelconque de σ est entièrement définie par σ.

3.5.3. SIGNATURE D'UNE PERMUTATION

3.5.3.1. Définition

Soit σ un élément de $\mathcal{S}_n$. On dit qu'un couple (i, j) d'éléments de $\mathbb{N}_n$ est une **inversion** *pour σ ou une σ-***inversion** *si $i < j$ et si $\sigma(i) > \sigma(j)$.*

3.5.3.2. Exemple

Soit

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

un élément de $\mathcal{S}_4$. Les couples (1,2), (1,3) et (1,4) sont des σ-inversions.

Soit σ une permutation de $\mathbb{N}_n$. Désignons par $I(\sigma)$ le nombre total de σ-inversions. Notons

$$\Delta = \prod_{i<j} (j - i)$$

le produit de toutes les différences $j - i$ avec $i < j$. On a

$$i \in \{1, 2, ..., n-1\} \quad \text{et} \quad j \in \{2, 3, ..., n\}.$$

Notons de même

$$\Delta_\sigma = \prod_{i<j} (\sigma(j) - \sigma(i))$$

le produit de toutes les différences $\sigma(j) - \sigma(i)$ avec $i < j$. Puisque σ est une bijection, chaque facteur de Δ se retrouve au signe près une fois et une seule dans Δ_σ et on a

$$\Delta_\sigma = (-1)^{I(\sigma)} \Delta. \tag{3.5.2}$$

L'application $\sigma \longmapsto \varepsilon(\sigma) = (-1)^{I(\sigma)}$ de $\mathcal{S}_n$ dans le groupe multiplicatif $\{-1, 1\}$ s'appelle **la signature de la permutation** σ.

Si $\varepsilon(\sigma) = +1$, on dit que la permutation σ est **paire.**

Si $\varepsilon(\sigma) = -1$, on dit que la permutation σ est **impaire.**

3.5.3.3. Exemple

Parité d'une transposition.

Soit τ la transposition qui échange les éléments i et j de $\mathbb{N}_n$ et laisse fixes les autres. On peut l'écrire, en supposant $i < j$:

$$\tau = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$$

Les couples (a, b) tels que $a < b$ et $\tau(a) > \tau(b)$ sont :

$$(i, i+1),\ (i, i+2),\ \dots,\ (i, j-1),\ (i, j)$$

$$(i+1, j),\ (i+2, j),\ \dots,\ (j-1, j).$$

Le nombre total d'inversions pour τ est donc

$$I(\tau) = 2(j - i) - 1$$

qui est un nombre impair, d'où $\varepsilon(\tau) = -1$.

Le théorème suivant donne les propriétés essentielles de la signature d'une permutation.

3.5.3.4. Théorème

Soient σ et π des éléments de $\mathcal{S}_n$. On a :

$$\varepsilon(Id) = 1, \quad \varepsilon(\sigma o \pi) = \varepsilon(\sigma)\,\varepsilon(\pi), \quad \varepsilon(\sigma^{-1}) = \varepsilon(\sigma).$$

Démonstration. On a

$$I(Id) = 0, \quad \text{d'où} \quad \varepsilon(Id) = (-1)^{I(Id)} = 1.$$

Si σ et π sont des permutations, nous avons d'après (3.5.2) :

$$\Delta_{\sigma o \pi} = (\Delta_\pi)_\sigma = \varepsilon(\sigma)\Delta_\pi = \varepsilon(\sigma)\,\varepsilon(\pi)\Delta.$$

Comme d'autre part,

$$\Delta_{\sigma o \pi} = \varepsilon(\sigma \circ \pi)\Delta,$$

il vient

$$\varepsilon(\sigma o \pi) = \varepsilon(\sigma)\,\varepsilon(\pi).$$

On en déduit $\varepsilon(\sigma)\,\varepsilon(\sigma^{-1}) = \varepsilon(\sigma \circ \sigma^{-1}) = \varepsilon(Id) = 1$.

Comme $\big(\varepsilon(\sigma)\big)^2 = 1$, on a

$$\varepsilon(\sigma^{-1}) = 1/\varepsilon(\sigma) = \big(\varepsilon(\sigma)\big)^2/\varepsilon(\sigma) = \varepsilon(\sigma).$$

3.5.3.5. Remarque

Le Théorème 3.5.3.4 signifie que l'application $\sigma \longmapsto \varepsilon(\sigma)$ est un homomorphisme de $\mathcal{S}_n$ sur le groupe multiplicatif $\{-1, 1\}$. Le noyau de cet homomorphisme est un sous-groupe de $\mathcal{S}_n$ appelé **groupe alterné d'ordre** n. On le note $\mathcal{A}_n$.

3.5.3.6. Remarque

Nous savons que toute permutation σ est un produit de transpositions et que cette décomposition n'est pas unique. Si

$$\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_s = t_1 \circ t_2 \circ \ldots \circ t_r$$

où les τ_i et τ_j sont des transpositions, alors d'après l'Exemple 3.5.3.3 et le Théorème 3.5.3.4, nous avons

$$\varepsilon(\sigma) = (-1)^s \quad \text{et} \quad \varepsilon(\sigma) = (-1)^r,$$

d'où $(-1)^s = (-1)^r$. Donc s et r sont tous les deux pairs ou tous les deux impairs.

Ainsi, lorsqu'on décompose une permutation en produits de transpositions, le nombre de ces transpositions est toujours soit pair soit impair.

3.6. Groupes opérant sur un ensemble

3.6.1. DÉFINITION. EXEMPLES

3.6.1.1. Définition

Soient G un groupe et X un ensemble. On dit que G **opère à gauche** *sur X, si l'on s'est donné une application $(g.x) \longmapsto g.x$ de $G \times X$ dans X satisfaisant aux conditions suivantes :*

a) $(g_1\, g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ *quels que soient* $g_1, g_2 \in G$ *et* $x \in X$;

b) $e \cdot x = x$ *quel que soit* $x \in X$.

On définirait de même la notion de groupe **opérant à droite** sur l'ensemble X.

Pour tout $g \in G$, soit $\varphi(g)$ l'application $x \longmapsto g \cdot x$ de X dans X.

D'après **a)**, on a $\varphi(g_1\, g_2) = \varphi(g_1)\, o\, \varphi(g_2)$; d'après **b)**, on a $\varphi(e) = Id_X$. Il en résulte que $\varphi(g)\, o\, \varphi(g^{-1}) = \varphi(g^{-1})\, o\, \varphi(g) = Id_X$, donc que $\varphi(g)$ est bijective pour tout $g \in G$. Donc φ est un homomorphisme de G dans le groupe des permutations de X.

Réciproquement, soit G un groupe, X un ensemble et φ un homomorphisme de G dans $\mathcal{S}(X)$. Pour $g \in G$ et $x \in X$, posons $g \cdot x = \varphi(g)(x)$. Alors les conditions **a)** et **b)** ci-dessus sont vérifiées.

En effet, puisque φ est un homomorphisme, on a :

$$\begin{aligned}(gg') \cdot x &= .\varphi(gg')(x) = \left[\varphi(g)\, o\, \varphi(g')\right](x) \\ &= \varphi(g)\left[\varphi(g')(x)\right] = g \cdot (g' \cdot x)\end{aligned}$$

quels que soient $g, g' \in G$ et $x \in X$.

De même on a :

$$e \cdot x = \varphi(e)(x) = Id_X(x) \qquad \text{pour tout } x \in X.$$

On peut donc définir l'action d'un groupe G dans un ensemble X par la donnée d'un homomorphisme de G dans $\mathcal{S}(X)$.

Dans la suite de ce paragraphe, nous nous intéressons uniquement aux groupes opérant à gauche sur un ensemble.

On dit que G **opère transitivement** sur X, si quels que soient x et y dans X, il existe $g \in G$ tel que $y = g \cdot x$. On dit alors que X est un **espace homogène.**

3.6.1.2. Exemple

On peut faire opérer G sur lui-même à l'aide des **translations à gauche**

$$(s, x) \longmapsto sx,$$

où à l'aide des **translations à droite.**

$$(s, x) \longmapsto xs.$$

3.6.2. SOUS-GROUPE D'ISOTROPIE. ORBITES

Soit G un groupe opérant à gauche sur l'ensemble X, et soit $x_0 \in X$. L'ensemble H_{x_0} des $g \in G$ tels que $g \cdot x_0 = x_0$ est un sous-groupe de G. En effet si $g_1, g_2 \in H_{x_0}$, on a

$$(g_1 g_2) \cdot x_0 = g_1 \cdot (g_2 \cdot x_0) = g_1 \cdot x_0 = x_0,$$

donc $g_1 g_2 \in H_{x_0}$.

Si $g \in H_{x_0}$, on a

$$g^{-1} \cdot x_0 = g^{-1} \cdot (g \cdot x_0) = (g^{-1} g) \cdot x_0 = e \cdot x_0 = x_0,$$

donc $g^{-1} \in H_{x_0}$. Enfin $H_{x_0} \neq \emptyset$ car $e \in H_{x_0}$ d'après **b).**

3.6.2.1. Définition

Soient G un groupe opérant à gauche sur l'ensemble X et soit $x_0 \in X$. On appelle **stabilisateur** *de x_0 dans G ou* **sous-groupe d'isotropie** *de x_0, le sous-groupe H_{x_0} des $g \in G$ tels que $g \cdot x_0 = x_0$.*

3.6.2.2. Théorème

Soit G un groupe opérant à gauche sur l'ensemble X. Pour $x, y \in X$, la relation binaire « il existe $g \in G$ tel que $y = g \cdot x$ » est une relation d'équivalence dans X. On appelle **orbite** *ou* **trajectoire** *de x suivant G, et on note $G \cdot x$, la classe d'équivalence de $x \in X$, pour cette relation.*

Démonstration. Pour tout $x \in X$, on a $x = e \cdot x$, donc la relation est réflexive.

Si $y = g \cdot x$, alors on a :

$$g^{-1}y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x,$$

donc la relation est symétrique.

Enfin, si $y = g \cdot x$ et $z = g' \cdot y \quad (g \in G,\ g' \in G)$, on a :

$$z = g' \cdot (g \cdot x) = (g'g) \cdot x,$$

donc la relation est transitive.

Notons que le groupe G opère transitivement sur l'ensemble X si et seulement si la seule orbite suivant G est X.

3.6.2.3. Exemple

Soient G un groupe, H un sous-groupe de G et G/H l'ensemble des classes à gauche $\dot{x} = xH$ modulo H. On vérifie facilement que G opère transitivement à gauche sur G/H par l'application

$$(s, xH) \longmapsto (sx)H.$$

Autrement dit, G/H est un espace homogène. Inversement, on a le résultat suivant.

3.6.2.4. Théorème

Soient G un groupe et X un espace homogène de G. Il existe un sous-groupe H de G et une application bijective f de G/H sur X tels que, quels que soient $s, g \in G$, on ait :

$$sf(gH) = f\left((sg)H\right).$$

Démonstration. Soit x_0 un point fixé de X et soit H le stabilisateur de x_0. Définissons une application f de G/H dans X en posant

$$f(sH) = sx_0, \quad s \in G.$$

Cette définition est justifiée car si s_1 et s_2 appartiennent à la même classe modulo H, i.e. si $s_2^{-1}s_1 \in H$, alors $s_1x_0 = s_2x_0$.

Si $sx_0 = gx_0$, alors $g^{-1}sx_0 = x_0$ et $g^{-1}s \in H$, donc $sH = gH$, ce qui prouve que f est injective.

D'autre part, pour tout $x \in X$, il existe par hypothèse un $s \in G$ tel que $x = sx_0 = f(sH)$; donc f est surjective, donc f est bijective et on a :

$$sf(gH) = f\left((sg)H\right).$$