Université de Caen Normandie

Département d'informatique

Structures algébriques pour l'informatique

12 mars 2018

Table des matières

Chapitre 1

Préliminaires

1.1 Ensembles

1.1.1 Définition

Un *ensemble* est une collection d'objets (de nombres, de personnes, etc.).

Exemples

- $A = \{1, 2, 3, 4\}$;
- $X = \{*, a, b\}$;
- $\mathbb{N}$ (entiers naturels) ;
- $\mathbb{Z}$ (entiers relatifs) ;
- $\mathbb{Q}$ (fractions rationnelles) ;
- $\mathbb{R}$ (réels) ;
- $\mathbb{C}$ (complexes).

Soit X un ensemble. On note $x \in X$ (x appartient à X ou encore x est un élément de X) un élément x d'un ensemble X.

1.1.2 Sous-ensemble

Un *sous-ensemble* (ou une partie) d'un ensemble X est un ensemble S tel que :

$$x \in S \to x \in X$$

On note $S \subset X$ $\left\{ \begin{array}{l} S \text{ est un sous-ensemble de } X \\ S \text{ est inclus dans } X \end{array} \right.$

Une stratégie pour montrer que deux ensembles X et Y sont égaux est de montrer que $X \subset Y$ et que $Y \subset X$.

$$X = Y \text{ si et seulement si } \left\{ \begin{array}{l} X \subset Y \\ Y \subset X \end{array} \right.$$

1.1.3 Ensemble des parties d'un ensemble

L'ensemble de toutes les parties (ou sous-ensembles) de X est l'ensemble, généralement noté $\mathcal{P}(X)$, dont les éléments sont les sous-ensembles de X.

Exemple 1 Soit $X = \{1, 2, 3\}$ un ensemble de trois éléments. L'ensemble de tous les sous-ensembles de X est :

$$\mathcal{P}(X) = \{\{1, 2, 3\}, \varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$$

Remarque si X a n éléments, $\mathcal{P}(X)$ a 2^n éléments *(ici $2^3 = 8$ éléments)*.

1.1.4 Produit cartésien

Le *produit cartésien* de deux ensembles X et Y est l'ensemble de tous les couples (x, y) tels que $x \in X$ et $y \in Y$. Il est noté $X \times Y$.

$$X \times Y = \{(x, y) \colon x \in X \text{ et } y \in Y\}$$

Exemple 1 Soit l'ensemble $X = \{1, 2, 3\}$ et l'ensemble $Y = \{a, b\}$. Le produit cartésien de ces deux ensembles est :

$$X \times Y = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$

Remarque si X a n éléments et Y a m éléments, $X \times Y$ a nm éléments.

$$\text{⚠ } (x, y) = (x', y') \Leftrightarrow x = x' \text{ et } y = y'$$

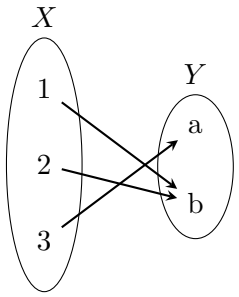
1.1.5 Ensemble des parties d'un produit cartésien

Une application f d'un ensemble X dans un ensemble Y noté $f \colon X \to Y$ est la donnée d'un sous-ensemble Γ de $X \times Y$, tel que pour tout $x \in X$, il existe un unique élément y tel que $(x, y) \in \Gamma$.

f est donc la donnée $\begin{cases} X \text{ un ensemble de départ} \\ Y \text{ un ensemble d'arrivée} \\ \Gamma \text{ appelé graphe de l'application } \Gamma \subset X \times Y \end{cases}$

Exemple 1 Soit l'ensemble $X = \{1, 2, 3\}$ et l'ensemble $Y = \{a, b\}$. Un sous-ensemble Γ de $X \times Y$ est :

$$\Gamma = \{(1, b), (2, b), (3, a)\}$$

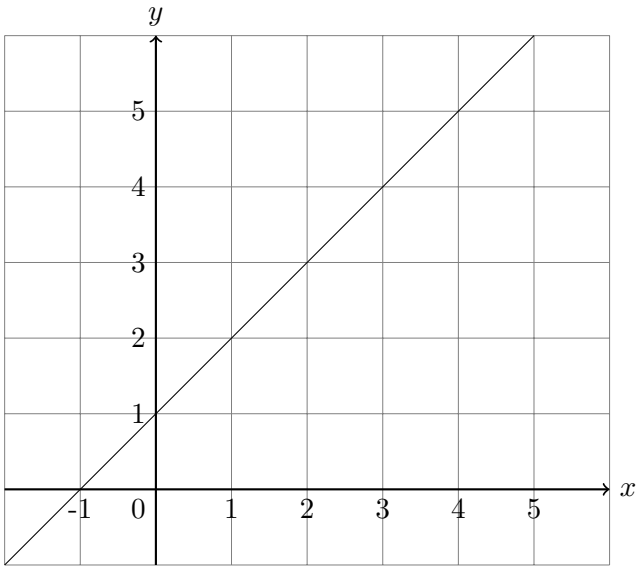


Soit $x \in X$, l'unique élément y tel que $(x, y) \in \Gamma$ est appelé image de x. Il est noté $f(x)$, on note également $x \mapsto y$.

$$\Gamma = \{(x, f(x)) \colon x \in X\}$$

Si $y = f(x)$, alors x est appelé un antécédent de y par f.

Exemple 2 Soit $f \colon \begin{cases} \mathbb{N} \to \mathbb{N} \\ x \mapsto x + 1 \end{cases}$



Deux applications f et g sont égales ($f = g$) si et seulement si elles ont le même ensemble de départ, le même ensemble d'arrivée et le même graphe.

⚠ Toute construction ne définit pas une application.

Exemple 3 $g\left(\frac{p}{q}\right) = pq$

g ne définit pas une application de Q dans Q.

$$g\left(\frac{1}{2}\right) = 2, \quad g\left(\frac{2}{4}\right) = 8$$

Mais $f\left(\frac{p}{q}\right) = 2\frac{p}{q}$ définit bien une application de Q dans Q.

1.2 Injection, surjection, bijection

1.2.1 Injection

Une application $f\colon X \to Y$ est *injective* si et seulement si tout élément de Y a au plus un antécédent (zéro ou un) par f.

$$f\colon X \to Y \text{ est injective} \begin{cases} \text{si et seulement si } \begin{cases} x \in X \\ x' \in X \end{cases} \quad x \neq x' \Rightarrow f(x) \neq f(x') \\ \\ \text{si et seulement si } f(x) = f(x') \Rightarrow x = x' \end{cases}$$

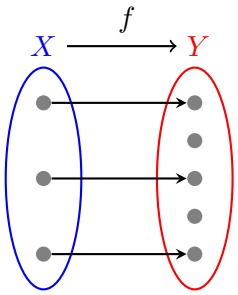


FIGURE 1.1 – Injection

1.2.2 Surjection

Une application $f\colon X \to Y$ est *surjective* si et seulement si tout élément de Y a au moins un antécédent par f.

$$f : \begin{cases} \mathbb{R} \to \mathbb{R} & f \text{ n'est pas injective} \\ x \mapsto x^2 & f \text{ n'est pas surjective} \end{cases}$$

$$g : \begin{cases} \mathbb{R} \to \mathbb{R}_+ & g \text{ n'est pas injective} \\ x \mapsto x^2 & g \text{ est surjective} \end{cases}$$

$$h : \begin{cases} \mathbb{R}_+ \to \mathbb{R}_+ & h \text{ est injective} \\ x \mapsto x^2 & h \text{ est surjective} \end{cases}$$

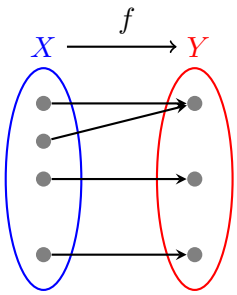


FIGURE 1.2 – Surjection

1.2.3 Bijection

Une application $f : X \to Y$ est *bijective* si et seulement si f est injective et surjective.

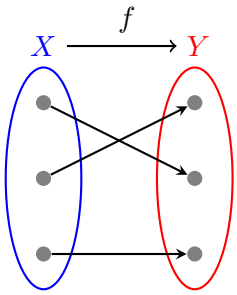


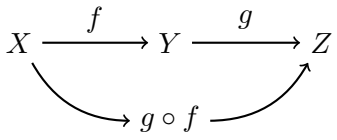
FIGURE 1.3 – Bijection

Remarque si X et Y sont des ensembles finis et que $\begin{cases} X \text{ a } n \text{ éléments (on note} |X|) \\ Y \text{ a } m \text{ éléments (on note} |Y|) \end{cases}$

— Si $|Y| > |X|$ on **ne peut pas** avoir de surjection de X dans Y.
— Si $|Y| < |X|$ on **ne peut pas** avoir d'injection de X dans Y.

Soient $f : X \to Y$ et $g : Y \to Z$ deux applications.

On définit alors $g : f : X \to Z$ tel que pour tout $x \in X$, $g \circ f(x) = g(f(x))$



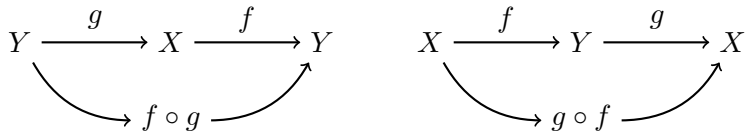
1.2.4 Application identité

On appelle l'*application identité* l'application qui n'a aucun effet lorsqu'elle est appliquée à un élément : elle renvoie toujours la valeur qui est utilisée comme argument.

$$\mathrm{id}_X : X \to X \text{ et pour tout } x \in X, \mathrm{id}_X(x) = x$$

$$\mathrm{id}_X : \begin{cases} X & \to & X \\ x & \mapsto & x \end{cases} \qquad \mathrm{id}_X \text{ est bijective.}$$

Soit $f : X \to Y$ une application. S'il existe $g : Y \to X$ tel que $g \circ f = \mathrm{id}_X$ alors g est appelée l'application réciproque de f (noté f^{-1}).



Proposition 1 $f : X \to Y$ est bijective si et seulement si f a une application réciproque g.

Soit $y \in Y$. Comme f est bijective, il existe un unique élément $x \in X$ tel que $y = f(x)$. On pose $x = g(y)$.

On a aussi défini $g : Y \to X$

On obtient $\begin{cases} \forall x \in X,\ g(f(x)) = x \\ \forall y \in Y,\ f(g(y)) = f(x) = y \end{cases}$

Montrer que f est injective.

Soient x et x' deux éléments de X tels que $f(x) = f(x')$. On a donc $g(f(x)) = g(f(x'))$ et $x = x'$.

f est aussi surjective : pour tout $y \in Y$, $g(y)$ est un antécédent de y car $f(g(y)) = y$

Pour montrer qu'une application est bijective, deux stratégies :
- Montrer que f est injective et surjective.
- Montrer que f admet une application réciproque.

Exemple 1 Soient $f : \begin{cases} \mathbb{N} \to \mathbb{N} \\ x \mapsto x+1 \end{cases}$ et $g : \begin{cases} \mathbb{N} \to \mathbb{N} \\ x \mapsto \begin{cases} 0 \text{ si } x = 0 \\ x - 1 \text{ si } x \geq 1 \end{cases} \end{cases}$

f est-elle bijective ? (g est-elle l'application réciproque de f ?)

Soit $x \in \mathbb{N}$, $\begin{cases} g(f(x)) = g(x+1) = x + 1 - 1 = x \\ g \circ f = \mathrm{id}_X \end{cases}$

Mais $f \circ g = \mathrm{id}_{\mathbb{N}}$?

$$f \circ g(0) = f(g(0)) = f(0) = 1$$
Donc $f \circ g \neq \mathrm{id}_{\mathbb{N}}$

g non injective, mais surjective.

Exemple 2 Si $\begin{cases} f\colon X \to Y \\ g\colon Y \to X \end{cases}$ et $g \circ f = \mathrm{id}_X$, alors f est injective et g est surjective.

Soit X un ensemble. On note $\mathcal{F}(X)$ ou X^X, l'ensemble des applications de X dans X (exemple : si $|X| = 3$, $\left|X^X\right| = |X|^{|X|}$).

Sur $\mathcal{F}(X)$, on définit une « opération interne ».

Si $f \in \mathcal{F}(X)$ et $g \in \mathcal{F}(X)$, $\quad f \circ g \in \mathcal{F}(X)$ *($f \circ g$ est toujours bien définie)*

1.3 Associativité

Une loi de composition interne ou loi interne $\circ$ sur un ensemble X est dite *associative* si pour tous f, g, et h dans X :

$$f \circ (g \circ h) = (f \circ g) \circ h$$

Soit $x \in X$. $\quad (f \circ g) \circ h(x) = f \circ g(h(x)) = f(g(h(x)))$

id_X est un élément neutre : $f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f$

$\forall x \in X$,

$$\begin{aligned} f \circ \mathrm{id}_X(x) = f(\mathrm{id}(x)) = f(x) \\ f \circ \mathrm{id} = f \\ \mathrm{id}_X \circ f(x) = \mathrm{id}_X(f(x)) = f(x) \\ \mathrm{id}_X \circ f = f \end{aligned}$$

Note : en général $f \circ g \neq g \circ f$

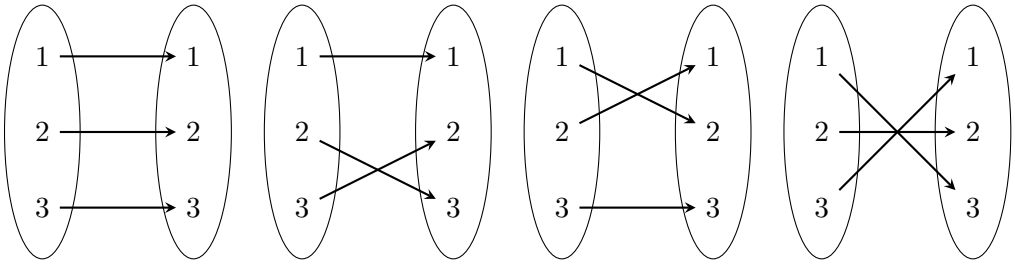
Exemple 1

$$\begin{aligned} g \circ f(x) = g(f(x)) = g(x^2) = x^2 + 1 \\ f \circ g(x) = f(g(x)) = f(x+1) = (x+1)^2 = x^2 + 2x + 1 \end{aligned}$$

$$g \circ f \neq f \circ g$$

Soit S_X l'ensemble des bijections de X dans X

$X = \{1, 2, 3\}$



0 est associative et 1_X est l'élément neutre et chaque élément de f de S_X admet un élément réciproque g tel que $f \circ g = g \circ f = \mathrm{id}_X$

1.4 Image directe et image réciproque

1.4.1 Image directe

L'*image directe* d'un sous-ensemble A de X par une application $f\colon X \to Y$ est le sous-ensemble de Y formé des éléments qui ont, par f, au moins un antécédent appartenant à A :

$$f(A) = \{f(x) \mid x \in A\} = \{y \in Y \mid \exists a \in A, y = f(a)\}$$

Exemple 1 Soit $f\colon \{1,2,3\} \to \{a,b,c,d\}$ une application définie par $f(1) = a$, $f(2) = c$, $f(3) = d$. L'image directe de $\{2,3\}$ par f est $f(\{2,3\}) = \{c,d\}$ tandis que l'image de f est $\{a,c,d\}$.

1.4.2 Image réciproque

L'*image réciproque* d'une partie B d'un ensemble Y par une application $f\colon X \to Y$ est le sous-ensemble de X constitué des éléments dont l'image par f appartient à B :

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}$$

Exemple 1 Soit $f\colon \{1,2,3\} \to \{a,b,c,d\}$ une application définie par $f(1) = a$, $f(2) = c$, $f(3) = d$. L'image réciproque de $\{a,b\}$ par f est $f^{-1}(\{a,b\}) = \{1\}$.

Remarque on peut avoir $f^{-1}(B) = \varnothing$.

1.5 Relation binaire

1.5.1 Définition

Une *relation binaire* $\mathcal{R}$ entre deux ensembles X et Y est un sous-ensemble du produit cartésien $X \times Y$, soit une collection de couples dont la première composante est dans X et la seconde dans Y.

Exemple Soient $X = \{1,2,3\}$ et $Y = \{a,b\}$. Alors $\mathcal{R} = \{(1,a),(1,b),(2,b)\}$.

On définit une relation binaire $\mathcal{R}$ sur un ensemble X pour un sous-ensemble de $X \times X$.

Exemple Soit $X = \{1, 2, 3\}$. Alors $\mathcal{R} = \{(1,2), (1,3), (2,3), (1,1), (2,2), (3,3)\}$

Lorsque $(x, y) \in \mathcal{R}$, on note $x\mathcal{R}y$. Sur l'exemple ci-dessus, on a :

$$\begin{array}{ccc} 1\mathcal{R}1 & 2\mathcal{R}2 & 3\mathcal{R}3 \\ 1\mathcal{R}2 & 1\mathcal{R}3 & 2\mathcal{R}3 \end{array}$$

De la même façon, "$\leq$" est une relation binaire finie sur $\mathbb{Z}$.

1.5.2 Relation sur (ou dans) un ensemble

1.5.2.1 Réflexivité

La relation $\mathcal{R}$ sur X est dite *réflexive* si tout élément de X est en relation avec lui-même, c'est-à-dire si :

$$\forall x \in X, \quad x\mathcal{R}x$$

1.5.2.2 Symétrie

La relation $\mathcal{R}$ est *symétrique* si :

$$\forall (x, y) \in X, \quad x\mathcal{R}y \Rightarrow y\mathcal{R}x$$

1.5.2.3 Transitivité

La relation $\mathcal{R}$ sur X est *transitive* si, lorsqu'un premier élément de X est en relation avec un deuxième élément lui-même en relation avec un troisième, le premier élément est aussi en relation avec le troisième, c'est-à-dire si :

$$\forall x, y, z \in X, \quad (x\mathcal{R}y \wedge y\mathcal{R}z) \Rightarrow x\mathcal{R}z$$

1.5.3 Relation d'équivalence

Une relation $\mathcal{R}$ est une *relation d'équivalence* si elle est réflexive, symétrique et transitive.

Exemple 1 Soit $X = \{\textit{étudiants dans l'amphi}\}, \quad x, y \in X$.

$$x\mathcal{R}y \Leftrightarrow x \textit{ et } y \textit{ ont le même âge}$$

$\mathcal{R}$ est clairement réflexive, symétrique et transitive donc c'est bien une relation d'équivalence.

1.5.4 Classe d'équivalence

La *classe d'équivalence* de x, notée $[x]$ *(ou parfois* $\overline{x}$*)* est par définition :

$$[x] = \{y \in X \mid x\mathcal{R}y\}$$

Remarque Une relation d'équivalence est souvent notée "$\equiv$" (au lieu de $\mathcal{R}$).

Il est clair que :

$$x \equiv y \Leftrightarrow [x] = [y]$$

Supposons que $x \equiv y$. On va montrer que $[x] \subset [y]$.

Soit $z \in [x]$, on a donc $x \equiv z$, or $x \equiv y$ (par symétrie $y \equiv x$). De $y \equiv x$ et $x \equiv z$, on déduit par transitivité $y \equiv z$ ou encore $z \in [y]$. De la même façon, $[y] \subset [x]$. Finalement, on a bien $[x] = [y]$.

Réciproquement si $[x] = [y]$, en particulier $x \in [x] = [y]$. Comme $x \in [y]$ on a donc bien $x \equiv y$.

1.5.5 Ensemble quotient

Étant donnée une relation d'équivalence $\equiv$ sur X, l'*ensemble quotient* de X par la relation $\equiv$, noté $X/\equiv$, est le sous-ensemble de $\mathcal{P}(X)$ des classes d'équivalence :

$$X/\equiv \; = \; \{[x] \in \mathcal{P}(X) \mid x \in X\}$$

Exemple 1 Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, n) tel que :

$$a = qb + n \quad \text{avec } a \leq n \leq b \text{ (où } q\text{=quotient et } n\text{=reste).}$$

$X = \mathbb{Z}$. Prenons $n = 5$ ($7 \equiv 12$). $x\mathcal{R}y \Leftrightarrow x$ et y ont le même reste dans la division entière par n.

$\mathcal{R}$ est clairement réflexive, symétrique et transitive. C'est donc une relation d'équivalence (on les notera dorénavant "$\equiv$").

Quelles sont les classes d'équivalence ? Quel est l'ensemble $\mathbb{Z}/\equiv$?

— $[0]$ = l'ensemble des multiples de 5

— $[1] = \{x \in \mathbb{Z} \mid x = 5q + 1 \text{ avec } q \in \mathbb{Z}\}$

— $[2] = \{x \in \mathbb{Z} \mid \exists q \in \mathbb{Z} \quad x = 5q + 2\}$

— $[3] = \{x \in \mathbb{Z} \mid \exists q \in \mathbb{Z} \quad x = 5q + 3\}$

— $[4] = \{x \in \mathbb{Z} \mid \exists q \in \mathbb{Z} \quad x = 5q + 4\}$

Ici $\mathbb{Z}/\equiv$ a exactement 5 éléments. 0 est le représentant de $[0]$, un autre représentant possible est 10.

On constate sur cet exemple que les classes d'équivalence sont non vides et deux à deux disjointes.

Par exemple : $[0] \cap [1] = \varnothing$.

Plus généralement $0 \leq i \leq j \leq 4$ $[i] \cap [j] = \varnothing$.

De plus, la réunion des classes d'équivalence forme $\mathbb{Z}$ tout entier.

$$[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$$

1.5.5.1 Partition

L'ensemble des classes d'équivalence forme une *partition* de X. On dit que l'ensemble des classes d'équivalence forme une *partition* de $\mathbb{Z}$.

Définition Soit X un ensemble et $A_1, A_2, \ldots, A_n, \ldots$ une famille de sous-ensembles de X.

$$A_i \subset X$$

On dit que cette famille forme une partition de X si et seulement si :

— $\forall i \quad A_i \neq \varnothing$

— $\forall (i,j) \quad i \neq j \quad A_i \cap A_j \neq \varnothing$

— $A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots = X$

Exemple 1 $\mathbb{Z}$ $\left.\begin{array}{l} A_0 : \text{entiers pairs} \\ A_1 : \text{entiers impairs} \end{array}\right\}$ cas précédent avec $n = 2$.

Exemple 2
$X = \{1,2,3,4,5\}$
$A_1 = \{1,2,4\}, A_2 = \{3\}, A_3 = \{5\}$

A_1, A_2 et A_3 forment une partition de X.

$$\begin{array}{ccccc} 1 \equiv 1 & 2 \equiv 2 & 3 \equiv 3 & 4 \equiv 4 & 5 \equiv 5 \\ & 1 \equiv 2 & 2 \equiv 4 & 1 \equiv 4 & \end{array}$$

Proposition 1 Si $\equiv$ est une relation d'équivalence sur X, alors les classes d'équivalence de $\equiv$ forment une partition de X.

Réciproquement, étant donné une partition de X, il existe une unique relation d'équivalence telle que les éléments de la partition soient les classes d'équivalence de $\equiv$.

Par définition d'une relation d'équivalence $\equiv$, $\forall x \in X, x \in [x]$. Donc $[x] \neq \varnothing$ ($[x]$ est non vide).

Supposons $[x] \cap [y] \neq \varnothing \mid \exists z \in [x] \cap [y]$. On a donc $x \equiv z$ et $z \equiv y$.

— Par transitivité, $x \equiv y$ dans $[x] = y$.

— Par contraposée, si $[x] \neq [y]$ alors $[x] \cap [y] = \varnothing$.

— Par définition on a $X = \bigcup\limits_{x \in X} \{x\}$ or $\{x\} \subset [x]$ donc $X = \bigcup\limits_{x \in X} [x]$.

Réciproquement, soit $(A_i)_{i \in I}$ une partition de X.

On définit par $x \equiv y$ si et seulement si $\left\{\begin{array}{l} x \text{ et } y \text{ appartiennent au même élément de la partition} \\ \exists i \in I \mid x, y \in A_i \end{array}\right.$

et on vérifie que $\equiv$ est une relation d'équivalence.

Pour $n \in \mathbb{N}^*$, on note $\mathbb{N}_n$ pour $\{1, \ldots, n\}$.

Exemple $\mathbb{N}_1 = \{1\}$; $\mathbb{N}_2 = \{1,2\}$; $\mathbb{N}_5 = \{1,2,3,4,5\}$ ($[\![1,5]\!]$)

1.5.5.2 Surjection canonique

Soit $\equiv$ une relation d'équivalence définie sur un ensemble E. On note $E/\equiv$ l'ensemble des classes d'équivalence de E.

$$\varphi \begin{cases} E & \to & E/\equiv \\ x & \mapsto & [x] \text{ (la classe de } x) \end{cases}$$

φ est clairement surjective. Elle est appelée la **surjection canonique** de E dans $E/\equiv$.

1.6 Ensemble fini, infini, dénombrable

1.6.1 Ensemble fini

On dit qu'un ensemble X est *fini* si et seulement si il existe une bijection de X dans $\mathbb{N}_n$ pour un certain n (c'est-à-dire qu'il existe $n \in \mathbb{N}$ tel que X soit en bijection avec $\mathbb{N}_n$).

Exemple 1 Soit $X = \{\circ, *, \star\}$. X est fini car il existe une bijection de X dans $\{1, 2, 3\}$.

$$\begin{array}{ccc} X & \to & \{1,2,3\} \\ \circ & \mapsto & 1 \\ * & \mapsto & 2 \\ \star & \mapsto & 3 \end{array}$$

1.6.2 Ensemble infini

Un ensemble *infini* est un ensemble qui n'est pas fini, c'est-à-dire qu'il n'y a aucun moyen de « compter » les éléments de cet ensemble à l'aide d'un ensemble borné d'entiers (c'est-à-dire que pour tout $n \in \mathbb{N}$, X n'est pas en bijection avec $\mathbb{N}_n$).

Un ensemble en bijection avec un ensemble infini est donc infini.

1.6.3 Ensemble dénombrable

Un ensemble X est dit dénombrable s'il existe une bijection de X dans $\mathbb{N}$.

Exemple 1 L'ensemble des entiers pairs

$$\varphi : \begin{cases} \{\textit{Entiers pairs}\} & \to & \mathbb{N} \\ x & \mapsto & \dfrac{x}{2} \end{cases}$$

φ est une bijection car $\phi : \begin{cases} \mathbb{N} & \to & \{\textit{Entiers pairs}\} \\ x & \mapsto & 2x \end{cases}$

$\varphi \circ \phi = \mathrm{id}_{\mathbb{N}}$ et $\phi \circ \varphi = \mathrm{id}_{\textit{Entiers pairs}}$

On montre que $\mathbb{N}^2$ est dénombrable (plus généralement $\mathbb{N}^k$ est dénombrable).

Soit $\varphi \begin{cases} \mathbb{N}^2 \to \mathbb{N} \\ (x, y) = y + (1 + 2 + \ldots + (x, y)) \end{cases}$

On dit qu'un ensemble est au plus dénombrable si il est fini ou dénombrable. On a tout sous-ensemble dénombrable est au plus dénombrable.

1.7 Exemples de "structures algébriques"

1.7.1 Préliminaires

Soit E un ensemble. On appelle *opération (élémentaire) binaire interne* sur E une application de $E \times E$ dans E.

Exemple 1 $*: \left\{ \begin{array}{ccc} E \times E & \to & E \\ (x,y) & \mapsto & z = *(x,y) \end{array} \right.$ $*(x,y)$ sera noté $x * y$.

1.7.2 Propriétés remarquables d'une opération interne

1.7.2.1 Associativité

Une opération interne sur un ensemble E est dite **associative** si et seulement si :

$$\forall (x,y,z) \in E \quad (x * y) * z = x * (y * z) = x * y * z$$

Notation Il existe deux notations usuelles pour une opération : $\times$ et $+$.

Si l'opération est associative :

$$\begin{array}{l} x + x + \ldots + x \text{ est noté } nx. \\ \underbrace{x \times x \times \ldots \times x}_{n \text{ fois}} \text{ est noté } x^n. \end{array}$$

1.7.2.2 Commutativité

Une opération interne sur un ensemble E est dite **commutative** si et seulement si :

$$\forall (x,y) \in E^2 \quad x * y = y * x$$

Notation Usuellement, $+$ est gardé pour les opérations commutatives, et $\times$ (noté ".") pour les autres.

1.7.2.3 Élément neutre

Une opération interne sur un ensemble E admet un **élément neutre** e si et seulement si :

$$\forall x \in E \quad x * e = e * x = x$$

Notation Pour $+$ lorsqu'il y a un élément neutre, il est 0_E.
Pour $\times$ lorsqu'il y a un élément neutre, il est 1_E.

1.7.2.4 Élément symétrique

Un élément $x \in E$ admet un **élément symétrique** $x' \in E$ si et seulement si :

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

Notation Pour $+$, x' est noté $(-x)$.
Pour $\times$, x' est noté x^{-1}.

1.7.2.5 Clôture

On dit qu'une partie A d'un ensemble E est **stable** (ou close) pour une opération définie sur E si cette opération, appliquée à des éléments de A, produit un élément de A.

Soit $S \subset E$. On dit que S est **stable** pour $*$ si et seulement si :

$$\forall (x, y) \in S \times S \quad x * y \in S$$

1.7.2.6 Distributivité

On dit qu'une opération interne $*$ est **distributive** par rapport à une autre opération interne T dans un ensemble E si et seulement si :

$$\forall (x, y, z) \in E^3 \quad x * (y \, T \, z) = (x * y) \, T \, (x * z)$$

1.7.2.7 Sous-structure

Soit E muni d'opérations élémentaires ayant une structure. Soit $S \subset E$. On dit que S, muni d'opérations de E, est une *sous-structure* de E si et seulement si (S, opération élémentaire) garde la même structure que (E, opération élémentaire).

Condition nécessaire (pas forcément suffisante) : il faut que S soit stable pour toutes les opérations. On parle alors des *opérations induites* sur S.

1.7.2.8 Morphismes

Soit (E, opération) et (E', opération) où E et E' ont les mêmes opérations.

Une application $f \colon E \to E'$ est un morphisme de la structure si elle est compatible avec les opérations. Si $*$ est une opération et si $(x, y) \in E^2$:

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

et les éléments neutres devant être conservés.

1.8 Définitions

1.8.1 Monoïde

Un *monoïde* est un ensemble E muni d'une opération interne associative admettant un élément neutre.

Exemples

1. Soit E l'ensemble des mots (finis) sur l'alphabet $\{0, 1\}$ muni de la concaténation (l'élément neutre est le mot vide). (E, *concaténation*) est un monoïde non commutatif.
2. $(\mathbb{N}, +)$: l'élément neutre est 0.
3. Soit E un ensemble non vide et E^E (l'ensemble des applications de E dans E), muni de $\circ$ (la composition). L'élément neutre est id_E :

$$\begin{array}{rll} & (f \circ g) \circ h & = f \circ (g \circ h) \\ \forall x \in E & ((f \circ g) \circ h)(x) & = (f \circ g)(h(x)) \\ & & = f(g(h(x))) \end{array}$$
$$\text{de même } f \circ (g \circ h))(x) = f(g \circ h(x)) = f(g(h(x)))$$

1.8.2 Groupe

Un *groupe* est un ensemble E muni d'une opération interne associative admettant un élément neutre et tel que tout élément de E admet un élément symétrique. $(E, \circ)$ est donc un monoïde où chaque élément admet un élément symétrique.

1. L'exemple 1 n'est pas un groupe.
2. L'exemple 2 $(\mathbb{N}, +)$ n'est pas un groupe.
3. $(E^E, \circ)$ n'est pas un groupe (toute application non-bijective n'a pas d'élément symétrique)
   L'ensemble des bijections de E dans E, noté σ_E, muni de la composition est un groupe. $(\sigma_E, \circ)$ est un groupe.
   - $\mathcal{M}_2(\mathbb{R})$: l'ensemble des matrices carrées 2×2 à coefficients dans $\mathbb{R}$
   - $\mathcal{M}_2(\mathbb{R}, x)$ n'est pas un groupe
   - $\mathcal{M}_2(\mathbb{R}, +)$ est un groupe (élément neutre $0_{\mathcal{M}_2(\mathbb{R})}$)
   - $\mathcal{M}_2(\mathbb{Z}, +)$ est un groupe
4. $(\mathbb{R}^5, +)$ est un groupe. L'élément neutre est $(0, 0, 0, 0, 0)$.
   $(\mathbb{Z}^2, +)$ est un groupe. L'élément neutre est $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$.
5. $\left(\left\{ \begin{bmatrix} x & y \\ z & t \end{bmatrix} \quad (x, y, z, t) \in \mathbb{R}^4 \text{ et } xt - zy \neq 0 \right\}, X \right)$ est un groupe. L'élément neutre est $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
6. $\left\{ \begin{bmatrix} x & y \\ z & t \end{bmatrix} \quad (x, y, z, t) \in \mathbb{Z}^4 \text{ avec } |xt - zy| = 1 \right\}$ est un groupe.

1.8.3 Anneau

Un ensemble E muni de deux opérations $+$ et $\times$ telles que $(E, +)$ est un *groupe commutatif* (c'est-à-dire l'opération $+$ est commutative). L'élément neutre est noté 0_E.

$\times$ est associative et admet un élément neutre (i.e. $(E, \times)$ est un monoïde). L'élément neutre est noté 1_E).

$\times$ est distributive par rapport à l'addition.

Exemples

1. $(\mathbb{Z}, +, .)$
2. $(\mathcal{M}_2(\mathbb{R}), +, .)$: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ est l'élément neutre pour $+$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est l'élément neutre

pour $\times$

3. $(E = \{f : \mathbb{R} \to \mathbb{R}\}, +, .)$ est un anneau où $(f+g)(x) := f(x) + g(x) \quad \forall x \in \mathbb{R}$
$(f.g)(x) := f(x).g(x) \quad \forall x \in \mathbb{R}$

1.8.4 Corps

$(K, +, \circ)$ est un corps si $\begin{cases} (i) & (K, +, \circ) \text{ est un anneau} \\ (ii) & \forall x \in K \backslash \{0_K\},\ x \text{ admet un élément symétrique pour } X \end{cases}$

(ii) $\Leftrightarrow (K\{0_E\}, X)$ est un groupe.

Exemples : $(\mathbb{Q}, +, X)$; $(\mathbb{C}, X, .)$; $(\mathbb{R}, +, X)$

1.9 "Sous-structure"

1.9.1 Sous-monoïde

Un sous-monoïde d'un monoïde $(E, .)$ est un sous-ensemble S de E vérifiant :

— $\forall (x, y) \in S \quad x.y \in S$ (stable)

— $1_E \in S$

1.9.2 Sous-groupe

Soit H un sous-ensemble de G. On dit que $(H, *)$ est un sous-groupe de $(G, *)$ si :

— $\forall (x, y) \in H^2 \quad x, y \in H$

— $1_G \in H$

— $\forall x \in H \quad x' \in H$

1.9.3 Sous-anneau

Soit $(A, +, .)$ un anneau, $S \subset A$.
$(S, +, .)$ est un sous-anneau si et seulement si :

— $(S, +)$ est un sous-groupe

— $1_A \in S$

— $\forall (x, y) \in S^2 \quad x, y \in S$

1.10 Morphismes

On suppose que E et E' sont deux exemples d'une même structure (par exemple E et E' deux monoïdes, E et E' deux groupes, E et E' deux anneaux ou E et E' deux corps).

On appelle ici $*_1, *_2$ les opérations de la structure.

Un morphisme de E dans E' est une application qui "conserve les lois de la structure", i.e. qui est compatible avec les opérations de la structure et qui conserve les constantes de la structure.

$$f : \begin{cases} E & \to & E' \\ x & \mapsto & x' \end{cases} \qquad \begin{matrix} f(x *_1 y) = f(x) *_1 f(y) \\ f(x *_2 y) = f(x) *_2 f(y) \end{matrix}$$

1.10.1 Monoïde

Soit $(E, .)$ et $(E', .)$ deux monoïdes. $f : E \to E'$ est un morphisme de monoïde si et seulement si :

$$\forall (x, y) \in E^2 \quad \begin{array}{l} f(x, y) = f(x)f(y) \\ f(1_E) = 1_{E'} \end{array}$$

1.10.2 Groupe

Soit $(G, .)$ et $(G', .)$ deux groupes. $f : G \to G'$ est un morphisme de groupe si et seulement si :

$$\forall (x, y) \in G^2 \quad f(x, y) = f(x)f(y) \tag{1.1}$$

Si (1.1) vérifié, alors :

$$\forall (x, y) \in G^2 \quad \begin{array}{rl} f(1_E) & = f(1_E \cdot 1_E) \\ & = f(1_E) \cdot f(1_E) \end{array}$$

$f(1_E) = f(1_E) \cdot f(1_E)$ or $f(1_E)$ est un élément de E' et E' est un groupe. Donc il existe un élément symétrique pour $f(1_E)$ qui est noté $(f(1_E))^{-1}$.

$$\begin{array}{rl} f(1_E)(f(1_E))^{-1} & = f(1_E) \cdot f(1_E)(f(1_E))^{-1} \\ 1_{E'} & = f(1_E) \cdot 1_{E'} \\ 1_{E'} & = f(1_E) \end{array}$$

1.10.3 Anneau

$f : A_1 \to A_2$ est un morphisme d'anneau si et seulement si :

$$\forall (x, y) \in A^2 \quad \left\{ \begin{array}{rl} f(x + y) & = f(x) \oplus f(y) \\ f(x \cdot y) & = f(x) \odot f(x) \\ f(1_{A_1}) & = 1_{A_2} \end{array} \right.$$

Soient $(K_1, +, \cdot)$ et $(K_2, \oplus, \odot)$ deux corps. $f : K_1 \to K_2$ est un morphisme de corps si et seulement si :

$$\forall (x, y) \in K^2 \quad \left\{ \begin{array}{rl} f(x + y) & = f(x) \oplus f(y) \\ f(x \cdot y) & = f(x) \odot f(x) \end{array} \right.$$

Un morphisme entre deux exemples d'une structure est un morphisme bijectif dont la fonction réciproque est aussi un morphisme.

Un morphisme de E dans E est un **endomorphisme**.

Un morphisme bijectif de E dans E est un **automorphisme**.

Chapitre 2

Langages et monoïdes

2.1 Définitions

Soit Σ un alphabet (fini). Σ^* est l'ensemble des mots finis sur Σ (un élément de Σ^* est une séquence finie d'éléments de Σ). On a déjà vu que (Σ, concaténation) est un monoïde.

$$L \subset \Sigma^* \text{ est ici appelé un langage sur } \Sigma.$$

Exemple Soit $\Sigma = \{0, 1\}$.

$$L_1 = \{\varepsilon, 0001, 110\}$$
$$L_2 = \{\omega \in \Sigma^*,\ \omega \text{ a autant de 0 que de 1}\}$$
$$L_3 = \{\omega \in \Sigma^*,\ \omega \text{ ne contient que des 1}\}$$

On peut définir des opérations sur les langages :

— $L_1 \cup L_2$

— $L_1 \cap L_2$

— $\Sigma^* \backslash L_1$

— $L_1 \backslash L_2$

— $L_1 L_2 = \{\omega_1\omega_2 \mid \omega_1 \in L_1 \text{ et } \omega_2 \in L_2\}$

2.2 Automates

Un *automate fini déterministe* est un automate fini dont les transitions à partir de chaque état sont déterminées de façon unique par le symbole d'entrée.

Un automate fini est un quintuplet $\mathcal{A} = (Q, \Sigma, \rho, i, F)$ où :

— Q est un ensemble fini, appelé ensemble des états,

— Σ est un alphabet,

— ρ est une partie de $Q \times \Sigma \times Q$ appelée ensemble des transitions,

— i est une partie de Q appelée ensemble des états initiaux,

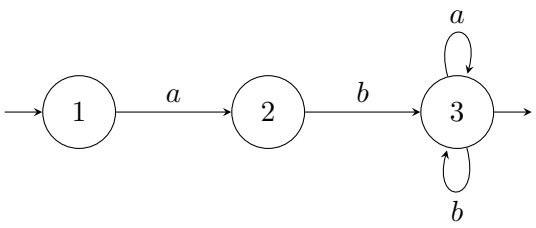
— F est une partie de Q appelée ensemble des états finaux.

2.2.1 Représentation graphique

Un automate fini, déterministe ou non, est représenté par un graphe dont les sommets sont les états, et les arcs sont les transitions. C'est donc un graphe orienté, étiqueté aux arcs par des lettres de l'alphabet. Une symbolique spéciale distingue les états initiaux et terminaux : un état initial est marqué par une flèche entrante, un état terminal par une flèche sortante ou par un double cercle.

Deux manières de représenter les automates : table de transitions et graphe de transitions.

Exemple 1 L'automate ci-dessous est composé de trois états ; l'état 1 est le seul état initial, distingué par une flèche entrante, l'état 3 est le seul état terminal, distingué par une flèche sortante. C'est un automate déterministe. Il reconnaît les mots, sur deux lettres a et b, qui commencent par ab. La fonction de transition est donnée par sa table de transitions. L'absence de flèche est représentée par un tiret : la présence d'un tiret montre que la fonction de transition est partielle.



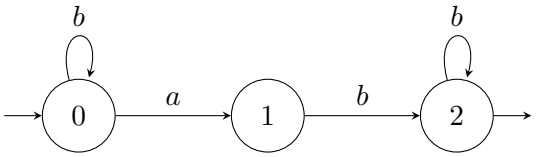
	a	b
1	2	-
2	-	3
3	3	3

FIGURE 2.1 – Graphe et table de transitions de l'automate

Exemple 2

$Q = \{0, 1, 2\}$ $\quad i = 0$

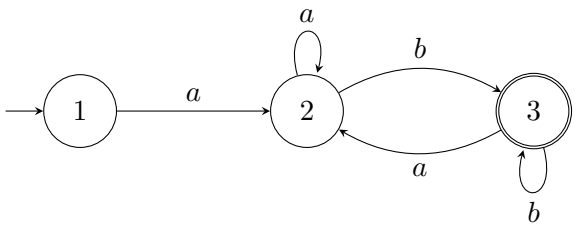
$\Sigma = \{a, b\}$ $\quad F = \{2\}$



	a	b
0	1	0
1	-	2
2	-	2

FIGURE 2.2 – Graphe et table de transitions de l'automate

Exemple 3 Soit l'automate ci-dessous. Les mots reconnus par cet automate sont ab, aab, abb, $aaab$, $aabb$, $abab$, $abbb$, etc. et plus généralement tous les mots commençant par a et finissant par b.



Une transition $(p, a, q) \in R$ est souvent écrite sous la forme $p \xrightarrow{a} q$, empruntée à la représentation graphique. Un *chemin* est une suite de flèches consécutives, notée :

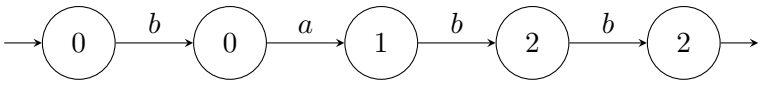
$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \longrightarrow \cdots \xrightarrow{a_n} q_n$$

Sa longueur est le nombre n de ses transitions, son *étiquette* (ou trace) est le mot $a_1 a_2 \cdots a_n$ formé des étiquettes de ses arcs.

On dit qu'un chemin est *réussi* lorsque $q_0 \in i$ et $q_k \in F$. Un mot est *reconnu* lorsqu'il est l'étiquette d'un chemin réussi. Le langage *accepté* ou *reconnu* par l'automate est l'ensemble des mots qu'il reconnaît.

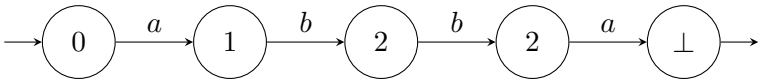
Exemple 4

— Calcul sur le mot *babb* :



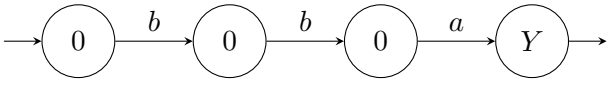
babb est reconnu.

— Calcul sur le mot *abbaab* :



On est dans un état de blocage. *abbaab* n'est pas reconnu.

— Calcul sur le mot *bba*



bba n'est pas reconnu.

Exemple 5 Soit $L = \{\omega \in \{a, b\}^*,\ \omega \text{ contenant le sous-mot } abba\}$.
Construisons un automate qui reconnaît L.

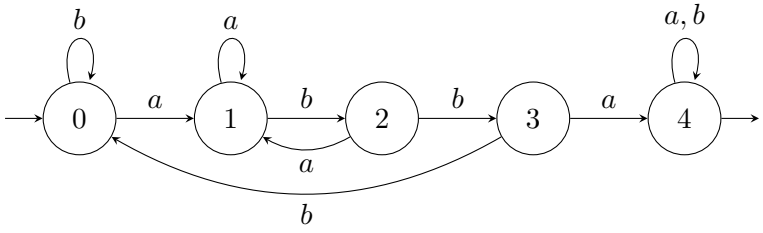


FIGURE 2.3 – Graphe de transitions

	a	b
0	1	0
1	1	2
2	1	3
3	4	0
4	4	4

TABLE 2.1 – Table de transitions

$Q_E = \{0, 1, 2, 3, 4\}$, $\Sigma_E = \{a, b\}$, $i = 0$, $F = \{4\}$ et $\rho\colon Q \times \Sigma \to Q$ est ici une application. On dit que l'automate est complet.

Remarque On peut toujours compléter un automate fini déterministe non complet pour avoir un automate complet en y ajoutant un "état puits" forcément non final.

2.2.2 Reconnaissance par morphisme

Soit $\varphi\colon \Sigma^* \to M$ où M est un monoïde fini et φ un morphisme de monoïde. On dit que $L \subset \Sigma^*$ est reconnu par le morphisme φ si et seulement si :

$$L = \varphi^{-1}(\varphi(L))$$

On dit que L est reconnu par le monoïde fini M s'il existe un morphisme $\varphi\colon \Sigma^* \to M$ qui reconnaît L. $L \subset \Sigma^*$ est reconnaissable par morphisme s'il existe un monoïde fini qui reconnaît L.

Pour un langage $L \subset \Sigma^*$, on a défini deux notions :

— être reconnu par un automate ;

— être reconnu par un morphisme.

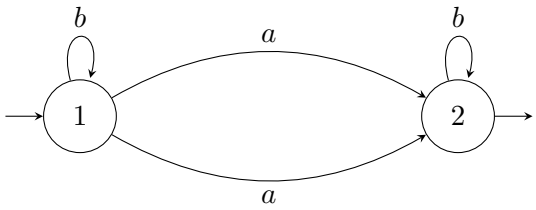
Nous allons montrer que les deux notions sont les mêmes.

2.2.3 Monoïde de transition d'un automate

Soit $\mathcal{A}(Q, \Sigma, \varphi, i, F)$ un automate fini déterministe complet. Soit l'alphabet de l'Exemple 5 début de l'alphabet φ_a de Q dans Q.

Le monoïde de transition de $\mathcal{A}(Q, \Sigma, \varphi, i, F)$ est le sous-monoïde de l'ensemble des applications de Q dans Q engendré par $(\varphi_a), a \in \Sigma$.
Remarque l'ensemble Q^Q (l'ensemble des applications de Q dans Q) muni de la loi de composition est un monoïde. a est une opération binaire et id_Q est l'élément neutre.

Soit $F = \{\varphi_a : a \in \Sigma\}$. On appelle le sous-monoïde engendré par F l'intersection du sous-monoïde de Q^Q qui contient F.



$$\{1,2\} \to \{1,2\} \quad \{1,2\} \to \{1,2\}$$
$$\varphi_a \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \end{cases} \qquad \varphi_b \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \end{cases}$$

Les langages reconnus par automates (finis déterministes complets) sont les langages reconnus par morphisme.

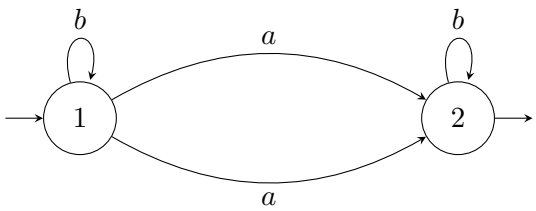
Soit L un langage défini sur un alphabet Σ ($L \subset \Sigma^*$) reconnu par un morphisme. Il existe un monoïde fini M et un morphisme de monoïde

$$\mu : \Sigma^* \to M$$

On a $\begin{cases} \mu(\varepsilon) = 1_M \\ \forall(\omega_1, \omega_2) \in (\Sigma^*)^2 \quad \mu(\omega_1\omega_2) = \mu(\omega_1)\mu(\omega_2) \end{cases}$ et $S \subset M \mid L = \mu(S)$.

Rappel :

Soit $\mathcal{A}(Q, \Sigma, \rho, i, F)$ un automate.



$Q = \{1, 2\}$
$\Sigma = \{a, b\}$
$\rho = Q \times \Sigma \to Q$
$(1, a) \mapsto 2$
$(1, b) \mapsto 1$
$(2, a) \mapsto 1$
$(2, b) \mapsto 2$

Soit $\omega \in \Sigma^*$. Le calcul de $\mathcal{A}$ sur ω :

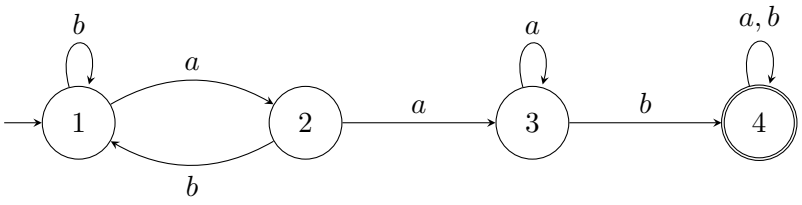
Exemple $\omega = abaab$

$$i \xrightarrow{a} 2 \xrightarrow{b} 2 \xrightarrow{a} 1 \xrightarrow{a} 2 \xrightarrow{b} 2$$

ω est accepté par $\mathcal{A}$ si le résultat du calcul de $\mathcal{A}$ sur ω se termine dans un état $q \in F$.

Soit $L \subset \Omega^*$. On dit que L est reconnu par un automate (fini, déterministe) si il existe un automate (fini, déterministe) tel que $L = \{\textit{ensemble des mots acceptés par } \mathcal{A}\}$.

Exemple 1 $L = \{$*langage des mots sur* $\{a, b\}$ *qui contiennent comme sur-mot* $aab\}$



On va construire un automate qui reconnaît le langage L : $\mathcal{A}(Q, \Sigma, \rho, i, F)$.

$$\begin{array}{l} Q = M \\ \Sigma = \Sigma \\ i = 1_M \end{array} \qquad \rho\colon \begin{array}{ccc} Q \times \Sigma & \to & Q \\ (q, a) & \mapsto & q.\mu(a) \end{array}$$

L'ensemble F des états occupants : S.
Que donne le calcul de cet automate sur le mot $\omega \in L$?

$$1_M \xrightarrow{a_1} \underbrace{1_M.\mu(a_1)}_{\mu(a_1)} \xrightarrow{a_2} \underbrace{\mu(a_1).\mu(a_2)}_{\mu(a_1,a_2)} \xrightarrow{a_3} \underbrace{\mu(a_1, a_2).\mu(a_3)}_{\mu(a_1,a_2,a_3)} \longrightarrow \cdots \longrightarrow \mu(\omega)$$

On a $\omega \in L \Leftrightarrow \omega \in \mu^{-1}(S)$. On a donc $\mu(\omega) \in S$, i.e. $\omega \in \mu^{-1}(S)$. $\mathcal{A}$ reconnaît donc bien exactement le langage L.

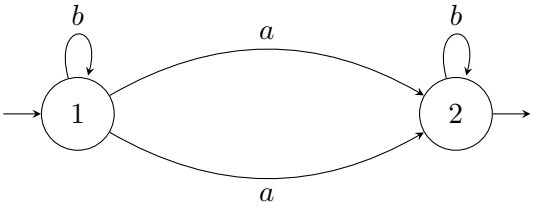
Réciproquement, soit $L \subset \Sigma^*$ un langage reconnu par un automate fini déterministe complet. L est-il reconnu par un morphisme (i.e. existe-t-il un monoïde fini (M_i), un morphisme $\mu\colon \Sigma^* \to M$ et $S \subset M \mid L = \mu^{-1}(S)$) ?

Lorsque $\mathcal{A}(Q, \Sigma, \rho, i, F)$ est fini déterministe complet, chaque lettre de Σ définit une application $\delta_a\colon Q \to Q$.

$$q \in Q \qquad \delta_a(q) = \rho(q, a)$$

Le monoïde des transitions de $\mathcal{A}$ est le sous-monoïde de $(Q^Q, \circ)$ engendré par $\{\delta_a\colon a \in \Sigma\}$.

Exemple 2



$$\delta_a : \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \end{array} \qquad \delta_b : \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 2 \end{array}$$

On définit le morphisme μ de la manière suivante :

$$\text{Pour } a \in \Sigma, \quad \mu(a) = \delta_a$$

Pour $w \in \Sigma^*$, on définit $\mu(\omega)$ de manière inductive : $\mu(a\omega) = \mu(a) \circ \mu(\omega)$

Exemple 3 Si $\omega = a_1 a_2 \mid a_1 \in \Sigma, a_2 \in \Sigma$,

$$\mu(a_1 a_2) = \delta_{a_1} \circ \delta_{a_2}$$

Plus généralement, $\mu(a_1 a_2 \dots a_n) = \delta_{a_1} \circ \delta_{a_2} \circ \cdots \circ \delta_{a_n}$.

μ ainsi défini est bien un morphisme

$$\begin{aligned} &\mu((a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_k)) \\ &= \mu(a_1 a_2 \cdots a_n b_1 b_2 \cdots b_k) \\ &= (\delta_{a_1} \delta_{a_2} \cdots \delta_{a_n} \delta_{b_1} \delta_{b_2} \cdots \delta_{b_n}) \end{aligned}$$

Il suffit alors de choisir $S = \mu(L)$ (on a bien $\omega \in L \Leftrightarrow \omega \in \mu^{-1}\mu(L)$)

Chapitre 3

Permutations sur un ensemble

3.1 Définition

Une *permutation* sur un ensemble X est une bijection de X dans X.

Exemple 1 Supposons $X = \{1, 2, 3, 4\}$, on notera une permutation $\sigma \in S_X$ de la manière suivante :

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

$$\sigma \begin{cases} X \to X \\ 1 \longmapsto 3 \\ 2 \longmapsto 2 \\ 3 \longmapsto 1 \\ 4 \longmapsto 4 \end{cases}$$

3.2 Notation

Une permutation peut se noter de plusieurs manières. La notation traditionnelle des permutations place les éléments qui vont être permutés dans l'ordre naturel sur une première ligne, et les images en correspondance, sur une deuxième ligne. Par exemple :

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

On appelle une énumération des éléments de X un arrangement :

(3 2 4 1) est un arrangement.

Tout arrangement sur X définit de manière unique une permutation sur X.

Exemple 1 L'arrangement (3 2 4 1) définit les permutations $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$.

On note S_X l'ensemble des permutations sur un ensemble X. Si $X = \{1, \ldots, n\}$, il est appelé groupe symétrique sur n éléments et on le note simplement S_n. L'ensemble S_X muni de la loi de composition des applications forme un groupe, appelé *groupe symétrique sur l'ensemble* X.

Preuve (déjà vu) : la composée de deux bijections est une bijection.

$$f \in S_X \text{ et } g \in S_X, \quad f \circ g \in S_X \Leftrightarrow \begin{cases} \exists f^{-1} \in S_X \mid (f^{-1} \circ f = f \circ f^{-1} = \mathrm{id}_X) \\ \exists g^{-1} \in S_X \mid (g^{-1} \circ g = g \circ g^{-1} = \mathrm{id}_X) \end{cases}$$

On remarque :

$$(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ f^{-1} = \mathrm{id}$$

Si f est une bijection, f^{-1} est encore une bijection.

3.2.1 Cycles

Nous allons introduire une deuxième notation pour les permutations.
α et β deux éléments de S_X, ne commutant pas. En général :

$$\alpha \cdot \beta \neq \beta \cdot \alpha$$

Soit $\{i_1, i_2, \ldots, i_r\} \subset \{1, 2, \ldots, n\}$. $\alpha \in S_n$ est appelé un *cycle* (de longueur n). Si $\alpha(i_1) = i_2, \alpha(i_2) = i_3, \ldots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1$ et $\forall j \notin \{i_1, i_2, \ldots, i_r\}, \alpha(j) = j$, on dit que α forme
Le cycle α est noté $(i_1, i_2, \ldots, i_r)$.

Exemple 1 Soit $X = \{1, 2, \ldots, 12\}$ et $\alpha = (5, 6, 9, 12)$.
Alors $\alpha(5) = 6$, $\alpha(6) = 9$, $\alpha(9) = 12$, $\alpha(12) = 5$, $\alpha(1) = 1$, $\alpha(2) = 2$ et ainsi de suite.

Un cycle de longueur 2 est appelé une *transposition*.

Exemple 2 Soit $\alpha = (1, 6)$.

$$\alpha(1) = 6 \qquad \alpha(6) = 1$$

L'ensemble des éléments déplacés par un cycle est appelé le *support* du cycle.

$$\mathrm{supp}((1, 6)) = \{1, 6\}$$

Un cycle de longueur 1 est l'identité.

$$\mathrm{supp}(\mathrm{id}) = \varnothing$$

Exemple 3 Soit α les permutations de S_9 suivantes :

$$\alpha \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}$$

On peut toujours écrire α comme produit de cycles :

$$\underbrace{(1\ 6)}_{\gamma}\underbrace{(2\ 4)}_{\delta}\underbrace{(3\ 7\ 8\ 9)}_{\mu}\underbrace{(5)}_{\text{id}}$$

Soit β les permutations de S_6 suivantes :

$$\beta \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$$

$$(1\ 3\ 2)\ (4)\ (5\ 6)$$

On va montrer que :

$$\alpha = \gamma \circ \delta \circ \mu$$

où γ est le cycle $(1, 6)$, δ est le cycle $(2, 4)$ et μ est le cycle $(3, 4, 8, 9)$.

On remarque que les supports des cycles γ, δ et μ sont deux à deux disjoints (on appelle deux cycles de supports disjoints des cycles disjoints).

Avec $\alpha(1) = 6$		Avec $\alpha(2) = 4$	
$\gamma \circ \delta \circ \mu$	$= \gamma(\delta(\mu(1)))$	$\gamma \circ \delta \circ \mu$	$= \gamma(\delta(\mu(2)))$
	$= \gamma(\delta(1))$		$= \gamma(\delta(2))$
	$= \gamma(1)$		$= \gamma(2)$
	$= 6$		$= 4$

Il en est de même pour tout $i \in \{1, 2, \ldots, 9\}$.

À partir d'une rotation en produits de cycles, on peut donc facilement obtenir la notation par table :

$$\sigma = (1\ 2)(1\ 3\ 4\ 2\ 5)(2\ 5\ 1\ 3)$$

$$1 \mapsto 3 \mapsto 4 \mapsto 4$$
$$2 \mapsto 5 \mapsto 1 \mapsto 2$$
$$3 \mapsto 2 \mapsto 5 \mapsto 5$$
$$4 \mapsto 4 \mapsto 2 \mapsto 1$$
$$5 \mapsto 1 \mapsto 3 \mapsto 3$$

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

Décomposons (par l'algorithme précédent) σ un produit de cycles : $(1\ 4)(2)(3\ 5)$. Ce produit de cycles n'est pas e même que le produit de cycles original $(1\ 2)(1\ 3\ 4\ 2\ 5)(2\ 5\ 1\ 3)$. Dans le produit obtenu par l'algorithme, on obtient toujours des cycles disjoints.

Proposition 1 α et β sont deux cycles disjoints si et seulement si i est déplacé par α, alors il est invariant par β et si j est déplacé par β, alors il est invariant par α.

Proposition 2 Deux cycles disjoints α et β commutent.

$$\alpha \cdot \beta = \beta \cdot \alpha$$

Proposition 3 Toute permutation $\alpha \in S_n$ est soit un cycle, soit un produit de cycles disjoints.

Preuve de la Proposition 2 α et β sont définis sur $\{1, \ldots, n\}$. Il suffit de montrer que pour tout $i \in \{1, \ldots, n\}$, on a $\alpha \cdot \beta(i) = \beta \cdot \alpha(i)$.

Soit $i \in \{i, \ldots, n\}$. Supposons que i n'est pas invariant par α.

$$\alpha(i) = j \quad \textit{avec } i \neq j$$

Alors j n'est également pas invariant par α (sinon, on aurait $\alpha(j) = j$ et $\alpha(i) = j$ or α est injective). Or comme α et β sont disjoints, $\beta(i) = i$ et $\beta(j) = j$.

$$\alpha(\beta(i)) = \alpha(i) = j \text{ et } \beta(\alpha(j)) = \beta(j) = j$$

Si i n'est pas invariant par β, on montre de la même façon que :

$$\alpha \cdot \beta(i) = \beta \cdot \alpha(i)$$

Si i est invariant pour α et β, on a :

$$\alpha \cdot \beta(i) = i = \beta \cdot \alpha(i)$$

Proposition 4 Toute permutation se découpe en produits de cycles disjoints. Cette décomposition est unique à l'ordre près.

Preuve : existence par récurrence sur le nombre d'éléments "déplacés" par la permutation (un élément "déplacé" est un élément qui n'est pas invariant).

Soit k le nombre d'éléments déplacés. Si $k = 0$, la permutation est l'identité (l'identité s'écrit de manière unique : $(1), (2), \ldots, (n)$).

Supposons que $k > 0$, il existe i_1 un élément déplacé. On a alors $\sigma(i_1) = i_2$ avec $i_2 \neq i_1$. On note $i_3 = \sigma(i_2)$, $i_4 = \sigma(i_3)$, et ainsi de suite. Alors il existe r tel que $i_r = i_1$.

En effet, il existe (k, l) tel que $i_k = i_l$ car $i_k \in \{1, \ldots, n\}$ et $i_l \in \{1, \ldots, n\}$.

Appelons r le plus petit indice tel que $i_r \in \{i_1, i_2, \ldots, i_{n-1}\}$. On va montrer que $i_r = i_1$. On a $i_r = \sigma(i_{r-1})$ et σ est injective. Sinon, ça veut dire que $i_r = i_l \mid l > 1$ or $\sigma(i_{l-1}) = i_l$ et $\sigma(i_r) = i_l$ et il y a 2 antécédents.

σ s'écrit sous la forme $\sigma = (i_1, i_2, \ldots, i_{r-1}) = \beta$ où β garde invariants les éléments appartenant à $\{i_1, i_2, \ldots, i_n\}$ et pour $j \notin \{i_1, i_2, \ldots, i_r\}$ on a $\beta(j) = \sigma(j)$.

Il est clair que le nombre d'éléments déplacés par β est strictement inférieur à k.

3.3 Unicité

Supposons qu'on a $\sigma = \beta_1\beta_2 \cdots \beta_t$ et $\sigma = \gamma_1\gamma_2 \cdots \gamma_s$ où les γ_i sont des cycles deux à deux disjoints. On va montrer par récurrence sur $\max(s, t)$ que les deux décompositions sont les mêmes.

Soit l_1 un élément de $\{1, 2, \ldots, n\}$ déplacé pour σ. Il existe un des cycles σ_i qui contient l_1. Sans perte de généralité (en changeant l'ordre des γ_i) on suppose que ce cycle est γ_s.

Nécessairement, il existe également un des cycles β_j qui contient i_1 (sinon i_1 serait invariant par $\beta_1, \beta_2, \ldots, \beta_t$). Sans perte de généralité (en changeant l'ordre des β_i) on suppose que ce cycle est β_t et on a donc :

$$\sigma^k(i_1) = \gamma_s^k(i_1)$$
$$\sigma^k(i_1) = \beta_t^k(i_1)$$

pour tout k.

On en déduit que $\sigma_s = \beta_t$ et on applique l'hypothèse de récurrence.

Remarque 1 Soit α un cycle de longueur n $\alpha = (i_1, i_2, \ldots, i_n)$. α est en fait de la forme $(i_1, \alpha(i_1), \alpha^2(i_1), \ldots, \alpha_{r-1}(1))$. En effet :

$$\alpha(i_2) = \alpha(\alpha(i_1)) = \alpha^2(i_1)$$
$$\alpha(i_3) = \alpha(\alpha(i_2)) = \alpha(\alpha(\alpha(i_1))) = \alpha^3(i_1)$$

Remarque 2 Soit α un cycle de longueur r $(i_1, i_2, \ldots, i_r)$.

α s'écrit aussi $(i_1, i_2, \ldots, i_r, i_1) = (i_3, i_4, \ldots, i_r, i_1, i_2) = (i_r, i_1, i_2, \ldots, i_{r-1})$.

Proposition 1 $ab \cdot x = x \cdot ab = \mathrm{id}$.

(i) Si α est un cycle de longueur r où $\alpha = (i_1, i_2, \ldots, i_{r-1}, i_r)$, alors :

$$\alpha^{-1} = (i_r, i_{r-1}, i_{r-2} \ldots, i_1)$$

(ii) Si α se décompose en produits de cycles deux à deux disjoints β_i :

$$\alpha = \beta_1 \beta_2 \ldots \beta_t$$

$$\alpha^{-1} = \beta_t^{-1} \beta_{t-1}^{-1} \ldots \beta_2^{-1} \beta_1^{-1}$$

Proposition 2 Soit γ et α deux éléments de S_n. Alors γ et $\alpha\gamma\alpha^{-1}$ ont le même type de description complète. Plus précisément, la décomposition complète de $\alpha\gamma\alpha^{-1}$ s'obtient à partir de la décomposition complète de γ, en y remplaçant chaque entier i par $\alpha(i)$.

Exemple 1

$$\gamma = (1\ 3\ 5)(2\ 4)(6) \text{ et } \alpha = (1\ 2)(4\ 5)$$

$\alpha\gamma\alpha^{-1} = (\alpha(1)\ \alpha(3)\ \alpha(5))(\alpha(2)\ \alpha(4))(\alpha(6))$
$\sigma = (2\ 3\ 4)(1\ 5)(6)$

Il faut montrer que $\sigma = \alpha\gamma\alpha^{-1}$. $\forall i \in \{1, 2, \ldots, n\}$:

$$\sigma(i) = \alpha\gamma\alpha^{-1}(i)$$

On considère deux types d'éléments j. Premier cas : j est un élément invariant par γ ($\gamma(j) = j$). On regarde comment se comportent σ et $\alpha\gamma\alpha^{-1}$ sur $\alpha(j)$. Comme 6 est

dans un cycle de longueur 1, dans la décomposition de γ, $\alpha(6)$ est dans un cycle de longueur 1 dans σ.

On a donc $\sigma(\alpha(6)) = \alpha(6)$ et $\alpha\gamma\alpha^{-1}(\alpha(6)) = \alpha\gamma(6) = \alpha(6)$ car 6 est invariant par γ.

Soit j un élément qui n'est pas invariant par γ (exemple $j = 1$).

$$j \longmapsto k$$
$$1 \longmapsto 3$$

$\sigma(\alpha(j)) = \alpha(k)$ et $\alpha\gamma\alpha^{-1}(\alpha(j)) = \alpha\gamma(j) = \alpha(k)$. Or α est une permutation, c'est-à-dire que tout i s'écrit sous la forme $\alpha(j)$.

Proposition 3 : Soit γ et β deux propositions qui ont le même type de décomposition complète.

Exemple 2

$$\gamma = (1\ 2\ 4)(3\ 5)(6\ 7)(8)$$
$$\beta = (5\ 3\ 2)(4\ 6)(1\ 8)(7)$$

Alors il existe $\alpha \in S_n$ tel que $\gamma = \alpha\beta\alpha^{-1}$. En effet, il suffit d'écrire les décompositions complètes l'une en dessous de l'autre et en déduire :

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

Proposition 4 $\forall n \leq 2,\ \forall \alpha \in S_n$, α est un produit de transpositions.

3.4 Signature

Soit $\sigma \in S_n$. La *signature* de σ, notée $\text{sgn}(\sigma)$, est définie par :

$$\text{sgn}(\sigma) = (-1)^{n-t}$$

où t est le nombre de cycles dans la décomposition complète de σ en cycles disjoints.

Exemple 1 $\sigma \in S_n, \quad \sigma = (1)(2)(3\ 4\ 5)$

$$\text{sgn}(\sigma) = (-1)^{5-3} = (-1)^2 = 1$$

Soit $\tau \in S_n$ une transposition (un cycle de longueur 2). Le nombre de cycles dans la décomposition complète de τ est :

$$1 + (n-2) = n - 1$$
$$\text{sgn}(\tau) = (-1)^{n-(n-1)} = (-1)$$

Proposition 1 Soit $\sigma \in S_n$ et $\tau \in S_n$ où τ est une transposition.

$$\text{sgn}(\tau\sigma) = -\text{sgn}(\sigma)$$

Preuve 1 On note $\tau = (a, b)$
et soit k et l deux entiers positifs $(k, l \geq 0)$
et $a, b, c_1, c_2, \ldots, c_k, d_1, d_2, \ldots, d_l$ des entiers deux à deux disjoints.

1. Premier cas : a et b sont dans le même cycle dans la décomposition de σ en cycles disjoints. Calculons le produit :

$$\underbrace{(a,b)(a,c_1,c_2,\ldots,c_k,b,d_1,d_2,\ldots,d_l)}_{\textit{cycle de } \sigma \textit{ qui contient } a \textit{ et } b}$$

$$= (ac_1c_2\ldots c_k)(bd_1d_2\ldots d_l)$$

2. Deuxième cas : a et b ne sont pas dans le même cycle dans la décomposition de σ en cycles disjoints. Calculons le produit :

$$(a,b)(a,c_1,c_2,\ldots,c_k)(b,d_1,d_2,\ldots,d_l)$$

$$= (a,c_1,c_2,\ldots,c_k,b,d_1,d_2,\ldots,d_l)$$

Comparons la décomposition complète de σ et la décomposition complète de $(\tau\sigma)$. $\tau = (a, b)$. Tous les cycles de la décomposition complète de σ qui ne contiennent ni a, ni b apparaissent également dans la décomposition de $(\tau\sigma)$.

— Si a et b sont dans le même cycle dans la décomposition complète de σ, alors ce cycle se décompose en 2 cycles dans la décomposition de $(\tau\sigma)$ (premier cas ci-dessus).

— Si a et b sont dans deux cycles disjoints dans la décomposition complète de σ, alors ces deux cycles se réunissent en un seul cycle dans la décomposition complète de $(\tau\sigma)$ (deuxième cas ci-dessus).

On en déduit donc que le nombre de cycles dans la décomposition complète de $(\tau\sigma)$ diffère de 1 du nombre de cycles dans la décomposition complète de σ.
Donc si $t =$ *nombre de cycles dans la décomposition complète de* σ, on a :

$$\text{sgn}(\tau\sigma) = \begin{cases} (-1)^{n-(t+1)} = (-1)^{n-t-1} = -\text{sgn}(\sigma) \\ (-1)^{n-(t-1)} = (-1)^{n-t+1} = -\text{sgn}(\sigma) \end{cases}$$

Proposition 2 Soit $\sigma \in S_n$ et soit $\sigma = \tau_1\tau_2\cdots\tau_k$ une décomposition de σ en produit de transpositions. On a :

$$\text{sgn}(\sigma) = (-1)^k$$

Corollaire de 2 Soit $\sigma = \tau_1\tau_2\ldots\tau_k$ avec τ_i des transpositions et $\sigma = \tau'_1\tau'_2\ldots\tau'_l$ avec τ_j des transpositions. Alors k et l sont de même parité (c'est-à-dire que tous deux sont pairs ou tous deux sont impairs.)

Preuve 2 Récurrence sur k. $\sigma = \tau_1$ et $\text{sgn}(\sigma) = (-1)^1$. La propriété est vraie au rang 0 et au rang 1.

Supposons que la propriété est vraie au rang $k-1$ et soit $\sigma = \tau_1\tau_2\ldots\tau_k = \tau_1(\tau_2\ldots\tau_k)$ d'après l'hypothèse de récurrence.

D'après la proposition précédente, $\text{sgn}(\sigma) = -\text{sgn}(\tau_2\ldots\tau_k) = -(-1)^{k-1} = (-1)^k$

3.5 Parité

3.5.1 Définition

Une permutation est dite *paire* si elle se décompose en un nombre pair de transpositions, ou encore si sa signature est égale à 1.

Une permutation est dite *impaire* si elle se décompose en un nombre impair de transpositions, ou encore si sa signature est égale à (-1).

Corollaire Soit $\alpha \in S_n$ et $\beta \in S_n$. On a :

$$\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta)$$

Preuve Soit $\alpha = \tau_1\tau_2 \dots \tau_k$ une décomposition de α en produit de transpositions et $\beta = \tau'_1\tau'_2 \dots \tau'_l$ une décomposition de β en produit de transpositions.

Alors on a $\alpha\beta = \tau_1\tau_2 \dots \tau_k\tau'_1\tau'_2 \dots \tau'_l$ est bien une décomposition de $\alpha\beta$ en produit de transpositions et on a :

$$\text{sgn}(\alpha\beta) = (-1)^{k+l} = (-1)^k(-1)^l = \text{sgn}(\alpha)\text{sgn}(\beta)$$

L'application $\text{sgn} : \left\{ \begin{array}{ccc} S_n & \to & \{-1,1\} \\ \sigma & \mapsto & \text{sgn}(\sigma) \end{array} \right.$ est un morphisme de groupe de $(S_n, \circ)$ dans $(\{-1,1\}, \times)$.

Chapitre 4

Groupe quotient

4.1 Relation d'équivalence compatible

Proposition 1 Soit $(G, \cdot)$ un groupe. Les relations d'équivalence $\mathcal{R}$ compatibles à gauche (respectivement à droite) avec la loi du groupe sont les relations de type $x\mathcal{R}y$ si et seulement si $x^{-1}y \in H$ (respectivement $xy^{-1} \in H$) où H est un sous-groupe de G.

$\mathcal{R}$ est compatible à gauche avec $(\cdot)$ si et seulement si :

$$\forall (x, y, z) \in G^3, \quad x\mathcal{R}y \Rightarrow zx\mathcal{R}zy$$

Soit $\mathcal{R}$ une relation d'équivalence compatible avec $(\cdot)$. On note H la classe de 1_G (on sait que $H \subset G$ et $H \neq \varnothing$ car $e \in H$).

Soit $(x, y) \in G^2$ tel que $x\mathcal{R}y \Rightarrow x^{-1}x\mathcal{R}x^{-1}y$. $\mathcal{R}$ est compatible à gauche $\Rightarrow 1_G\mathcal{R}x^{-1}y$.

$$x^{-1}y \in H \Leftrightarrow x^{-1}y\mathcal{R}1_G \Rightarrow x\mathcal{R}y \ (x\mathcal{R}y \Leftrightarrow x^{-1}y \in H)$$

Réciproquement : Soit H un sous-groupe de G. On pose $x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$. Montrons que $\mathcal{R}$ est une relation d'équivalence compatible avec la loi du groupe.

<u>$\mathcal{R}$ est réflexive :</u> on a bien $x\mathcal{R}y \Leftrightarrow x^{-1}x \in H$ car $1_G \in H$ qui est un sous-groupe symétrique

$$x\mathcal{R}y \Leftrightarrow x^{-1}y \in H \Leftrightarrow (x^{-1}y)^{-1} \in H \Leftrightarrow y^{-1}x \in H \Leftrightarrow y\mathcal{R}x$$

<u>$\mathcal{R}$ est transitive :</u>

$$x\mathcal{R}y \text{ et } y\mathcal{R}z \Leftrightarrow x^{-1}y \in H \text{ et } y^{-1}z \in H \Rightarrow x^{-1}yy^{-1}z = x^{-1} \in H \Leftrightarrow x\mathcal{R}z$$

$\mathcal{R}$ est bien compatible avec $(\cdot)$: Soit $(x, y) \in G^2$ et soit $z \in G$.

$$x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$$

or $x^{-1}y = x^{-1}z^{-1}zy = (zx)^{-1}zy \in H$.

Soit H un sous-groupe de G et $a \in G$. Les ensembles $aH\colon \{ah\colon h \in H\}$ (respectivement $Ha\colon \{ha\colon h \in H\}$) sont appelés les classes à gauche (respectivement les classes à droite)

selon H. Ces classes sont exactement les classes d'équivalence de $\mathcal{R}_g$ (respectivement $\mathcal{R}_d$) les relations définies par :

$$x\mathcal{R}_g\, y \Leftrightarrow x^{-1}y \in H$$

$$\textit{respectivement } x\mathcal{R}_d\, y \Leftrightarrow xy^{-1} \in H$$

Supposons que les ensembles quotients $\frac{G}{\mathcal{R}_g}$ et $\frac{G}{\mathcal{R}_d}$ sont finis (c'est-à-dire qu'il y a un nombre fini de classes d'équivalence). Alors :

$$\text{card}\left(\frac{G}{\mathcal{R}_g}\right) = \text{card}\left(\frac{G}{\mathcal{R}_d}\right)$$

et ce nombre est appelé indice de H dans G et est noté $[G\colon H]$.

L'application φ suivante est bijective :

$$\varphi\colon \begin{cases} \{aH\colon a \in G\} & \to & \{Ha\colon a \in G\} \\ aH & \mapsto & Ha \end{cases}$$

Cas important Supposons que G est un groupe fini. Alors toutes les classes à gauche (respectivement les classes à droite) sur H auront le même cardinal, qui sera le cardinal de H. En effet, φ_a définie par

$$\varphi_a\colon \begin{array}{ccc} H & \to & aH \\ h & \mapsto & ah \end{array}$$

est toujours une bijection.

Proposition 2 Soit G un groupe, H un sous-groupe de G et $g \in G$. On définit $\phi\colon H \to gH$. ϕ est une application bijective.

Preuve de 2 Soit $y \in gH \Leftrightarrow \exists h \in H$ tel que $y = gH \Leftrightarrow g^{-1}y = h \Leftrightarrow \phi(h) = y$.

Si G est un graphe fini, H et gH ont le même cardinal.

Les seules relations d'équivalence sur G compatibles à gauche sont celles définies par :

$$x \equiv y \Leftrightarrow xy^{-1} \in H$$

où H est un sous-groupe de G.

Dans ce cas, H est la classe de 1_G et les classes d'équivalence de $\equiv$ sont les ensembles gH (qu'on appelle les classe à gauche).

Remarque Soit G un groupe et H un sous-groupe de G, $(g_1, g_2) \in G^2$. Alors on a les équivalences suivantes :

$$g_1H = g_2H \Leftrightarrow H_{g_1}^{-1} = H_{g_2}^{-1}$$

$$\Leftrightarrow g_1H \cap g_2H \neq \varnothing \Leftrightarrow g_1H \subset g_2H \Leftrightarrow g_2H \subset g_1H$$

$$g_1 \in g_2H \Leftrightarrow g_2 \in g_1H \Leftrightarrow g_1g_2^{-1} \in H$$

Exemple 1 On choisit $G = S_3$, $H = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$.

On a les classes à gauche selon H :

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

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

On a les classes à droite selon H :

$$H(\mathrm{id}) = H(1\ 2\ 3) = (1\ 3\ 2) = H$$

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

⚠ En général, les classes à gauche sont différentes des classes à droite.

Exemple 2 On choisit $G = S_3$, $H = \{\mathrm{id}, (1\ 2)\}$.

On a les classes à gauche selon H :

— $(\mathrm{id})H = (1\ 2)H = H$

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

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

On a les classes à droite selon H :

— $H(\mathrm{id}) = H(1\ 2) = H$

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

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

4.2 Récapitulatif

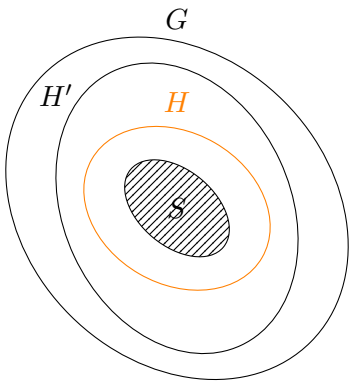
Récapitulatif sur la notion de sous-groupe engendré par un ensemble $S \subset G$. Soit G un groupe et S un sous-ensemble de G.

Proposition et définition Il existe un plus petit sous-groupe de G (pour l'inclusion) contenant S. Ce sous-groupe est appelé le sous-groupe engendré par S. Il est noté $\langle S \rangle$.

Preuve Comme $S \subset G$, il existe toujours un sous-groupe de G qui le contient : G lui-même. On sait que l'intersection d'une famille de sous-groupe de G est encore un sous-groupe G. L'intersection de tous les sous-groupes de G qui contiennent S est donc un sous-groupe. C'est bien le plus petit pour l'inclusion.

Remarque Dire que $H = \langle S \rangle$ est le plus petit sous-groupe contenant S signifie :

$$\forall H' \text{ sous-groupe de } G \text{ tel que } S \subset G,\ H \subset H'.$$



Exemple 1 Montrer que l'intersection d'une famille de sous-groupe de G est un sous-groupe de G.

Rappel : Soit $H \subset G$. H est un sous-groupe si et seulement si $H \neq \varnothing$ et $\forall (x,y) \in H, \quad xy^{-1} \in H$.

Proposition 1 Soit G un groupe et $S \subset G$.

$$\langle S \rangle = \{y \in G : \exists (x_1, x_2, \ldots, x_n) \in S^n \mid y = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}\}$$

avec $\varepsilon_1 = \pm 1$.

Preuve On a bien $S \subset \langle S \rangle$.
Soit $\omega_1 \in S$ et $\omega_2 \in S$. Exemple :

$$\omega_2 = x_1^{-1} x_2^{-1} x_3^{-1} x_4^{-1}$$
$$\omega_2^{-1} = x_4^1 \; x_3^{-1} x_2^1 \; x_1^{-1}$$

Cas particulier important $S = \{a\}$ $\langle S \rangle$ est appelé un groupe, $\langle \{a\} \rangle$ est noté $\langle a \rangle$. On dit qu'il est monogène et s'il est fini on dit qu'il est cyclique. $|\langle a \rangle|$ est appelé l'ordre de a, noté $\mathrm{ord}(a)$, si $\langle a \rangle$ est fini. Si $\langle a \rangle$ est infini, on dit que a est d'ordre infini.

Proposition 2 Soit G un groupe fini. $\mathrm{ord}(a) = \min\{k \in \mathbb{N}^* \mid a^k = 1_G\}$.

Preuve de 2 Considérons les puissances successives positives de :

$$1_G = a^0, a^1, a, a^2, a^3, \ldots$$

Remarque $\langle a \rangle = \{a^1 : i \in \mathbb{Z}\}$ d'après la Proposition 2.

Il en existe une infinité qui sont des éléments de G. Or G est fini. Donc nécessairement il existe $i \neq j$ avec $a^i = a^j$.

Soit k le premier entier positif pour lequel on se répète :

$$\exists j \text{ où } 0 \leq j < k \mid a^k = a^j$$
$$a^k = a^j \Leftrightarrow a^k a^{-j} = a^j a^{-j} \Leftrightarrow a^{k-j} = 1_G = a^0$$

$0 \leq k - j \leq k$ et on a une répétition en a^{k-j}. On a donc $j = 0$ sinon $k - j < k$ et x avec la définition de k.

Définition Pour un groupe fini G, le cardinal du groupe est aussi appelé ordre de G, noté $\text{ord}(G)$. ($\text{ord}(G) = |G|$)

Corollaire 1 Soit G un groupe fini et $a \in G$. $\text{ord}(a)$ divise $|G|$. ($\text{ord}(a) = |\langle a \rangle|$ et le théorème de Lagrange dit que : H sous-groupe de G, $|H|$ divise $|G|$)

Corollaire 2 Soit G un groupe et $a \in G$.

$$\exists k \in \mathbb{N} \mid a^{|G|} = 1_G$$

En effet, $|G| = k \cdot \text{ord}(a)$ (Lagrange)

$$a^{|G|} = a^{k \cdot \text{ord}(a)} = \left(a^{\text{ord}(a)}\right)^k = (1_G)^k = 1_G$$

Corollaire 3 Soit G un groupe fini avec $|G| = p$ où p est un nombre premier. G est cyclique et $\forall g \in G$, $g \neq 1_G$, $G = \langle g \rangle$. (G est engendré par tout élément autre que 1_G)

Preuve de 3 Soit $x \neq 1_G$ (il en existe car $|G| = p > 1$)

$$1 < \text{ord}(a) \text{ et } \text{ord}(x) \text{ divise } p \Rightarrow \text{ord}(x) = p$$

4.2.1 Exemple important

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

Notation Si le groupe est noté additivement, les classes à gauche selon H sont notées $g + H$ et les classes à droite selon H sont notées $H + g$.

Proposition 1 Les seuls sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z} = \{nk\}$. |

Les classes à gauche selon un sous-groupe $n\mathbb{Z}$ sont les mêmes que les classes à droite (car $+$ est commutatif dans $\mathbb{Z}$). Il s'agit des ensembles $r + n\mathbb{Z}$.

Les relations d'équivalence associées au sous-groupe $n\mathbb{Z}$ sont ici :

$$x \equiv y \Leftrightarrow x - y \in n\mathbb{Z}$$

$$\Leftrightarrow x + y \text{ est multiple de } n$$

$$\Leftrightarrow \ x \text{ et } y \text{ ont le même reste dans la division par } n$$

Donc $\mathbb{Z}$ est ici partitionné en exactement n classes :

$$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + \mathbb{Z}$$

(car le reste dans la division par n ne peut être que $0, 1, \ldots, n-1$)

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$