Chapitre 1
Rappels et compléments de "théorie" des ensembles

I Relation d'équivalence

Définition I.1.
Soit X un ensemble et R une relation binaire sur X.
On dit que R est d'équivalence si:

- *$\mathcal{R}$ est reflexive ($\forall x \in X, x\mathcal{R}x$)*
- *$\mathcal{R}$ est symétrique ($\forall (x,y) \in X^2, x\mathcal{R}y \iff y\mathcal{R}x$)*
- *$\mathcal{R}$ est transitive ($\forall (x,y,z) \in X^3, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \implies x\mathcal{R}z$)*

Exemple:

1. Soit P une partition de X.
   On associe à P la relation $\mathcal{R}_P$ définie par:
   $x\mathcal{R}_P y$ ssi x et y appartiennent à la même partie de P.
2. Soit $f : X \longrightarrow Y$ une application.
   La relation $\mathcal{R}_f$ définie par:
   $x\mathcal{R}_f y \iff f(x) = f(y)$
   est une relation d'équivalence.

□

Définition I.2.
Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble X.
On appelle classe d'équivalence d'un élément x de X l'ensemble des éléments qui sont en relation avec x.
Noté $\bar{x}$ ou $[x]_{\mathcal{R}}$ ou $\dot{x}$
$\bar{x} = \{y \in X, x\mathcal{R}y\}$

Propriété I.3.

- *Les classes d'équivalence des éléments de X forment une partition de X. on la note $X/\mathcal{R}$*
- *La relation d'équivalence associée à cette partition est $\mathcal{R}$*
- *L'application $\pi : X \longrightarrow X/\mathcal{R}$ est une surjection (appelée surjection canonique) et $x \longmapsto \bar{x}$ la relation associée à π est $\mathcal{R}$.*

Démonstration:

- $X/\mathcal{R} = \{\bar{x}, x \in X\}$
- – Soit $C \in X/\mathcal{R}$.
  Il existe $x \in X$ tel que $C = \bar{x}$.
  On a : $x \in C$. Donc $C \neq \varnothing$.
  – $\forall x \in X, x \in \bar{x}$
  Donc $\bigcup_{C \in X/\mathcal{R}} C = X$.
  – Soient $C_1, C_2 \in X/\mathcal{R}$.
  Supposons $C_1 \cap C_2 \neq \varnothing$.
  Soient $x_1, x_2 \in X$ tels que $C_1 = \bar{x}_1$ et $C_2 = \bar{x}_2$.
  Soit $x \in C_1 \cap C_2$.
  Comme $x \in C_1$, on a $x\mathcal{R}x_1$.
  De même : $x\mathcal{R}x_2$.
  On en déduit, pour tout $y \in X$,
  $y \in C_1 \implies y\mathcal{R}x$
  $\implies y\mathcal{R}x_2$
  $\implies y \in C_2$
  C'est à dire $C_1 \subset C_2$. De même $C_2 \subset C_1$.
- Soient $x, y \in X$
  $x\mathcal{R}y \implies x \in \bar{y}$
  $\implies \bar{x} \subset \bar{y}$
  De même, $x\mathcal{R}y \implies \bar{y} \subset \bar{x}$
  Donc $\bar{x} = \bar{y}$.
  Réciproquement, $\bar{x} = \bar{y} \implies x\mathcal{R}y$
  Ainsi:
  $x\mathcal{R}y \iff \bar{x} = \bar{y}$
  $\iff \exists C \in X/\mathcal{R}, x \in C$ et $y \in C$

- Immédiat:
  - π est surjective car $\bar{x} = \pi(x)$
  - $x\mathcal{R}_\pi y \iff {}_{\text{def}}\pi(x) = \pi(y)$
    $\iff \bar{x} = \bar{y}$
    $\iff x\mathcal{R}y$

□

Définition I.4.
Soit R une relation d'équivalence définie sur X et $f\colon X \longrightarrow Y$.
On dit que f est compatible avec $\mathcal{R}$
si les conditions équivalentes suivantes sont satisfaistes :

i $\forall x, y \in X, x\mathcal{R}y \implies f(x) = f(y)$

ii *Il existe $g\colon X/\mathcal{R} \longrightarrow Y$ telle que $f = g \circ \pi$.*
Dans ce cas, g est unique et s'appelle l'application quotient (de f par $\mathcal{R}$).

Démonstration:

- $[ii \implies i]$ Supposons l'existence de g telle que $f = g \circ \pi$.
  Alors, pour tout $x, y \in X$,
  $xRy \implies \pi(x) = \pi(y)$
  $\implies g \circ \pi(x) = g \circ \pi(y)$
  $\implies f(x) = f(y)$
- $[i \implies ii]$ Supposons 'i'.
  Soit $C \in X/\mathcal{R}$.
  Pour $x, y \in C$, on a $x\mathcal{R}y$ donc $f(x) = f(y)$.
  Ainsi: $f(x)$ ne dépend pas du choix de x dans C.
  On peut donc poser $g(C) = f(x)$, où x est un élément quelconque de C.
  Ceci définit g de $X/\mathcal{R}$ dans Y et on a:
  $\forall x \in X, g(\bar{x}) = f(x)$
  ie: $g \circ \pi(x) = f(x)$

□

Exemple:

Soient $n, m \in \mathbb{N}^*$.
À quelles conditions existe-t-il une application $g\colon \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ vérifiant $\forall x \in \mathbb{Z}, g([x]_n) = [x]_m$?
Une telle application g existe ssi:
$\forall x, y \in \mathbb{Z}, x \equiv y[n] \implies \pi_m(x) = \pi_m(y)$
Ou encore : $\forall x, y \in \mathbb{Z}, x \equiv y[n] \implies x \equiv y[m]$
ou encore : $\forall z \in \mathbb{Z}, n|z \implies m|z$
Ce qui est vrai ssi $m|n$. □

Définition I.5.
Soit $\mathcal{R}$ une relation d'équivalence sur X et $*$ une loi de composition interne sur X.
On dit que $*$ est compatible avec $\mathcal{R}$
si les propriétés équivalentes suivantes sont vérifiées :

i $\forall x, x', y, y' \in X, (xRx' \text{ et } y\mathcal{R}y') \implies (x * y)\mathcal{R}(x' * y')$

ii Il existe une loi $\bar{*}$ sur $X/\mathcal{R}$ vérifiant :
$\forall x, y \in X, \bar{x}\bar{*}\bar{y} = \overline{x * y}$

Démonstration:

Exercice □

Exemple:

Les lois $+$ et $\times$ de $\mathbb{Z}$ sont compatibles avec $\equiv_n$ (où $n \in \mathbb{N}^*$)
Soient $x, x', y, y' \in \mathbb{Z}$.
Supposons $\begin{cases} x \equiv x'[n] \\ y \equiv y'[n] \end{cases}$
Alors:
$(x' + y') - (x + y) = \underbrace{(x' - x)}_{\in n\mathbb{Z}} + \underbrace{(y' - y)}_{\in n\mathbb{Z}}$
Donc $x' + y' \equiv x + y[n]$
De même $x'y' - xy = \underbrace{(x' - x)}_{\in n\mathbb{Z}} y' + x \underbrace{(y' - y)}_{\in n\mathbb{Z}} \in n\mathbb{Z}$
Donc $x'y' \equiv xy[n]$ □

Remarque I.6.
Plutôt que d'utiliser les lois quotient $\bar{*}$ et $\bar{+}$,
on préfère travailler dans $\mathbb{Z}$ modulo n ($3+2 \equiv 1[4] \iff \bar{3}^4 \bar{+} \bar{2}^4 = \bar{1}^4$)

Remarque I.7.
Soit $*$ une loi compatible avec $\mathcal{R}$ (d'équivalence).
$\bar{*}$ hérite d'un grand nombre de propriétés que $*$ possède (peut-être)

- *$*$ commutative $\implies$ $\bar{*}$ commutative*
- *e neutre pour $*$ $\implies$ $\bar{e}$ neutre pour $\bar{*}$*
- *$*$ distributive sur $\perp$ (qui elle aussi passe au quotient) $\implies$ $\bar{*}$ distributive sur $\bar{\perp}$*
- *Si x est inversible pour $*$, il existe y tel que $x * y = e$ et $y * x = e$.*
  Alors $\bar{x}$ est inversible pour $\bar{*}$.
  Noter en particulier que si $(X, *)$ est un groupe, $(X/\mathcal{R}, \bar{*})$ l'est aussi.
  Si $(X, \perp, *)$ est un anneau, $(X/\mathcal{R}, \bar{\perp}, \bar{*})$ l'est aussi.

II Relation d'ordre

Définition II.1.
Une relation $\mathcal{R}$ sur un ensemble X est dite d'ordre si:

- *Elle est refléxive ($\forall x, x\mathcal{R}x$)*
- *Elle est antisymétique($\forall x, y, (x\mathcal{R}y$ et $y\mathcal{R}x) \implies x = y$)*
- *Elle est transitive*

En outre, une relation d'orde $\mathcal{R}$ est dite totale si
$\forall x, y \in X, x\mathcal{R}y$ ou $y\mathcal{R}x$

Exemple:

- $(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq)$ Mais pas $(\mathbb{C}, \leq)$!!!
- Ordre lexicographique
- L'égalité sur $\{0, 1\}$ est une relation d'ordre non totale.

□

Définition II.2.
Soient $(X, \leq), (Y, \preceq)$ *deux ensembles ordonnés, et* $f : X \longrightarrow Y$.
On dit que f *est croissante si* $\forall x, y \in X, x \leq y \implies f(x) \preceq f(y)$.

Exercice:

Si f est bijective et croissante, f^{-1} est-elle nécessairement croissante ?
Non ($f : (\{0,1\}, =) \longrightarrow (\{0,1\}, \leq)$)
Mais oui si la première relation est totale. □

Définition II.3.
Soit $(X, \leq)$ *un ensemble ordonné,*
$A \subset X$ *et* $a \in X$

1. *On dit que* a *majore* A *si :* $\forall x \in A, x \leq a$
2. *On dit que* a *est le plus grand élément de* A *si* $a \in A$ *et* a *majore* A
3. a *est la borne supérieure de* A *si* a *est le plus petit des majorants de* A
4. a *est un élément maximal de* A *si* $a \in A$ *et* $\forall x \in A, a \leq x \implies x = a$

Exercice:

Donner le graphe de C dans $\mathcal{P}(a, b, c)$ □

III Dénombrabilité

Définition III.1.

- *Un ensemble* A *est dit dénombrable s'il existe une bijection de* $\mathbb{N}$ *dans* A
- *Un ensemble fini ou dénombrable est dit au plus dénombrable*

Exemple:

- $\mathbb{N}$ est dénombrable
- $\mathbb{Z}$ est dénombrable (Exercice : expliciter une bijection de $\mathbb{N}$ dans $\mathbb{Z}$)
- $\mathbb{N}^2$ est dénombrable (Exercice : expliciter une bijection de $\mathbb{N}^2$ dans $\mathbb{N}$)
- $\mathbb{R}$ n'est pas dénombrable
  Soit en général $a : \mathbb{N} \longrightarrow \mathbb{R}$ une suite de réels. Montrons qu'elle n'est pas surjective.
  Soit $\alpha_0 < \beta_0$ tels que $a_0 \notin [\alpha_0, \beta_0]$
  Puis α_1, β_1 tels que $\alpha_0 \leq \alpha_1 < \beta_1 \leq \beta_0$ et $a_1 \notin [\alpha_1, \beta_1]$
  En poursuivant ainsi, on construit deux suites $(\alpha_k)_k$, $(\beta_k)_k$ telles que
  $\forall k, \alpha_k \leq \alpha_{k+1} < \beta_{k+1} \leq \beta_k$
  $\forall k, a_k \notin [\alpha_k, \beta_k]$
  Comme $(\alpha_k)_k$ est croissante majorée (par β_0), elle converge. De même, $(\beta_k)_k$ converge.
  Posons $u = \lim\limits_{k \to +\infty} \alpha_k, v = \lim\limits_{k \to +\infty} \beta_k$
  On a :
  $$\forall k, \begin{cases} \alpha_k \leq u \leq v \leq \beta_k \\ a_k \notin [\alpha_k, \beta_k] \end{cases}$$
  Donc $\forall k, a_k \notin [u, v]$; a n'est pas surjective.

□

Propriété III.2.

1. *Une partie d'un ensemble dénombrable est au plus dénombrable.*
2. *L'image injective d'un ensemble dénombrable est dénombrable.*
3. *Soit $f : X \longrightarrow Y$ une application.*
   - *Si f est injective et Y est dénombrable alors X est au plus dénombrable*
   - *Si f est surjective et X dénombrable alors Y est au plus dénombrable*
4. *Un produit d'ensembles deux ensembles dénombrables est dénombrable.*
5. *Une réunion au plus dénombrable d'ensemble au plus dénombrables est au plus dénombrable.*

Démonstration:

1. Soit X dénombrable et $Y \subset X$
   Soit $\varphi : \mathbb{N} \longrightarrow X$ une bijection
   φ induit une bijection de $A = \varphi^{-1}(Y)$ dans Y.
   Il suffit de prouver que A est au plus dénombrable
   Supposons A non fini.

   - A est une partie non vide de $\mathbb{N}$
     Donc A admet une plus petit element
     Posons $a_0 = min(A)$
   - $A \setminus \{a_0\} \neq \varnothing$ car A est infini.
     On peut donc poser $a_1 = min(A \setminus \{a_0\})$

   Et on construit ainsi par récurrence une suite $(a_k)_k$ en posant à chaque étape $a_{k+1} = min(A \setminus \{a_0, ..., a_k\})$

   - On a clairement $\forall k, a_k < a_{k+1}$
   - Soit $x \in A$
     Comme $a_0 \leq x$ et $(a_k)_k$ est croissante, il existe k tel que $a_k \leq x < a_{k+1}$
     Si on avait $x \neq a_k$, on aurait $x \in A \setminus \{a_0, ..., a_k\}$ et $x < a_{k+1}$, ce qui contredit la définition de a_{k+1}
     Donc $a : \mathbb{N} \longrightarrow A$ est une bijection

2. Évident

3. Soit $f : X \longrightarrow Y$

   - Si f est injective et Y dénombrable, alors f induit une bijection de X dans $f(X)$ qui est au plus dénombrable en tant que partie de Y.
     Donc X est au plus dénombrable
   - Si f est surjective et X dénombrable alors Y est au plus dénombrable
   - Si f est surjective et X dénombrable, il existe une application $g : Y \longrightarrow X$ telle que $\forall y \in Y, f(g(y)) = y$ (il suffit de choisir pour chaque $y \in Y$ un antécedent $g(y)$ de y)
     g est injective car : $\forall y, z, g(y) = g(z) \implies f(g(y)) = f(g(z))$
     $\implies y = z$
     Puisque X est dénombrable, Y l'est aussi.

□

Remarque III.3.
Une telle application g, associée à une surjection f s'appelle une section de f (le terme section a une origine géométrique)

Démonstration:

4. Soit X et Y dénombrables et $\varphi\colon \mathbb{N} \longrightarrow X$, $\psi\colon \mathbb{N} \longrightarrow Y$ deux bijections.
   L'application $\varphi \times \psi\colon \mathbb{N}^2 \longrightarrow X \times Y$ est une bijection.
   $$(k,l) \longmapsto (\varphi(k), \psi(l))$$
   Comme $\mathbb{N}^2$ est dénombrable, $X \times Y$ l'est aussi.

□

Remarque III.4.
Le produit cartésien d'une famille quelconque d'ensembles au plus dénombrables n'est pas forcément dénombrable.

Exemple:

$X = \{0,1\}^{\mathbb{N}}$ n'est pas dénombrable.
Soit en effet $a\colon \mathbb{N} \longrightarrow X$ une application
Soit $b \in X$ définie par : $b_k = 1 - a_k(k)$.
On a : $\forall k, b_k \neq a_k(k)$
Donc $b \neq a_k$; b n'appartient pas à l'image de a. □

Démonstration:

5. Soit $(A_i)_{i\in I}$ une famille au plus dénombrable d'ensembles au plus dénombrables.
   Montrons que $\bigcup_{i\in I} A_i$ est au plus dénombrable.
   $\bigcup_{i\in I}\{i\}\times A_i$
   Soit $\psi\colon I \longrightarrow \mathbb{N}$ une injection et, pour $i\in I$, $\varphi_i\colon A_i \longrightarrow \mathbb{N}$ une injection
   $G\colon \bigcup_{i\in I}\{i\}\times A_i \longrightarrow \mathbb{N}\times\mathbb{N}$ est une injection.
   $(i,x) \longmapsto (\psi(i),\varphi_i(x))$
   $\mathbb{N}\times\mathbb{N}$ dénombrable et G est injective entraine $\bigcup_{i\in I}\{i\}\times A_i$ au plus dénombrable.
   Puisque $\bigcup_{i\in I}\{i\}\times A_i \longrightarrow \bigcup_{i\in I}\times A_i$ est surjective, $\bigcup_{i\in I} A_i$ est au plus dénombrable.
   $(i,x) \longmapsto x$

□

Exercice:

1. Montrer que $\mathbb{Q}$ est dénombrable
   $\mathbb{Z}\times\mathbb{N}^* \longrightarrow \mathbb{Q}$ surjective
   $(p,q) \longmapsto \dfrac{p}{q}$
   Or $\mathbb{Z}\times\mathbb{N}^*$ est dénombrable, donc $\mathbb{Q}$ aussi.

2. L'ensemble des suites presques nulles à valeurs dans $\mathbb{Z}$ (noté $\mathbb{Z}^{(\mathbb{N})}$).
   $A_r = \{u\in\mathbb{Z}^{(\mathbb{N})}, \forall k\geq r, u_k = 0\}$.
   On a $\mathbb{Z}^{(\mathbb{N})} = \bigcup_{r\in\mathbb{N}^*} A_r$.
   $\forall r\in\mathbb{N}^*, A_r \simeq \mathbb{Z}^r$.
   Donc A_r est dénombrable et $\mathbb{Z}^{(\mathbb{N})}$ aussi.

3. $\mathcal{P}(\mathbb{N})$?
   $\{0,1\}^{\mathbb{N}} \longrightarrow \mathcal{P}(\mathbb{N})$ est une bijection.
   $f \longmapsto \{x\in\mathbb{N}, f(x)=1\}$
   Donc $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable.

□

Remarque III.5.
On peut montrer que quelque soit l'ensemble X, il n'existe pas de bijection de X dans $\mathcal{P}(X)$.
Soit en effet $\varphi : \mathcal{P}(X) \longrightarrow X$ une application.
Posons $A = \{x \in X, x \notin \varphi(x)\}$.
Soit $a \in X$ tel que $\varphi(a) = A$
$a \in A \iff a \notin \varphi(a)$
$\iff a \notin A$

Exercice:

4. $z \in \mathbb{C}$ est dit algébrique s'il existe $P \in \mathbb{Z}[X] \setminus \{0\}$ tel que $P(z) = 0$
   L'ensemble des nombres algébriques est il dénombrable ?
   C'est : $\bigcup_{P \in \mathbb{Z}[x] \setminus \{0\}} \{z \in \mathbb{C}, P(z) = 0\}$ donc il est dénombrable

□

Remarque III.6.
L'ensemble des nombres algébriques est un corps. C'est non trivial.
2 démos possibles :

- *"À la main"*
- *Avec un peu d'algèbre linéaire*

IV Notion de conjugaison

Soient X, X', Y, Y' des ensembles et $\varphi : X \longrightarrow X'$ et $\psi : Y \longrightarrow Y'$ des bijections.
φ et ψ permettent de voir X et X' commes "copies" l'un de l'autre, idem pour Y et Y'.
À toute application $f : X \longrightarrow Y$ correspond donc une application $f' : X' \longrightarrow Y'$ qu'on appelle conjuguée de f par (φ, ψ).
$f' = \psi \circ f \circ \varphi^{-1}$
Cas particulier important :
$$\begin{cases} Y = X \\ Y' = X' \\ \varphi = \psi \end{cases}$$

Exemple:

1. E plan euclidien orienté
   - f =rotation d'ange de mesure θ
     $\varphi \in O^+(E)$
     Alors $\varphi \circ f \circ \varphi^{-1}$ est une rotation d'angle θ
     Donc $\varphi \circ f \circ \varphi^{-1} = f$
     Si $\varphi \in O^-(E)$: $\varphi \circ f \circ \varphi^{-1} = f^{-1}$ car φ "renverse l'orientation"
   - s_Δ =symétrie orthogonale par rapport à Δ
     $\varphi \in O(E)$, $\varphi \circ s_\Delta \circ \varphi^{-1} = s_{\varphi(\Delta)}$
2. S_n = groupe des permutations de $[\![1, n]\!]$
   $c = (a_1, ..., a_s)$ cycle.
   $\sigma \in S_n : \sigma \circ c \circ \sigma^{-1} = (\sigma(a_1), ..., \sigma(a_s))$

□