Chapitre
Algèbre générale

1 Ensemble

On appelle ensemble une collection d'objets non ordonnés. On peut définir un ensemble de deux manières différentes :
- Par **extension** : on définit l'ensemble en donnant la liste de tous ses éléments mis entre accolades. On peut toute fois se permettre des pointillés si ceux ci ne sont pas trop ambigue. Par exemple : $E = \{1, 2, 3, \ldots, 9\}$.
- Par **compréhension** : On définit l'ensemble en décrivant ses éléments comme éléments d'un ensemble déjà défini vérifiant une certaine propriété. Par exemple l'ensemble E ci-dessus peut s'écrire $E = \{n \in \mathbb{N}, 1 \leq n \leq 9\}$.

Dans tout le chapitre, $\emptyset$ désigne l'ensemble vide, c'est-à-dire l'ensemble ne contenant aucun élément.

Définition 1.1. *Soit E un ensemble et x un élément, on notera $x \in E$ pour x appartient à E et $x \notin E$ pour x n'appartient pas à E.*
Soient A et B deux ensembles, on dira que A est inclus dans B ou B contient A et on notera $A \subset B$ ou $B \supset A$ (respectivement) si

$$x \in A \Longrightarrow x \in B$$

On dira que A et B sont égaux et on notera $A = B$ si et seulement si $A \subset B$ et $B \subset A$.

Remarque 1.1. *Si A est inclus dans B on dira que A est un sous ensemble de B ou encore A est une partie de B.*

Exemples :
- $2 \in \mathbb{N}$, $\sqrt{3} \notin \mathbb{Q}$, $(2, 1) \in \{(x, y) \in \mathbb{R}^2, x \geq y\}$.
- $\mathbb{Q} \subset \mathbb{R}$, $\{1, 2\} \not\subset \{1, 3, 5\}$.

Définition 1.2. *Soient E un ensemble et A un sous ensemble de E. Alors il existe un unique ensemble $C_E(A)$ appelé complémentaire de A dans E vérifiant :*

$$\forall x \in E, (x \in C_E(A)) \Longrightarrow (x \notin A).$$

Remarque 1.2. *Lorsqu'il n'y a pas d'ambiguité sur l'ensemble E on écrira A^c au lieu de $C_E(A)$.*

Exemples
$C_E(\emptyset) = E, \quad C_{\mathbb{Z}}(\mathbb{N}) = \{n \in \mathbb{Z}, n < 0\}, \quad \{(x,y) \in \mathbb{R}^2, x \geq y\}^c = \{(x,y) \in \mathbb{R}^2, x < y\}.$

Définition 1.3. *Soient A et B deux ensembles, on note alors :*
- *l'intersection de A et B, et l'on note $A \cap B$, l'ensemble défini par :*

$$(x \in A \cap B) \text{ si et seulement si } x \in A \text{ et } x \in B.$$

- *l'union de A et B, et l'on note $A \cup B$, l'ensemble défini par :*

$$(x \in A \cup B) \text{ si et seulement si } x \in A \text{ ou } x \in B.$$

- *$A \setminus B$, la différence entre A et B, l'ensemble défini par :*

$$(x \in A \setminus B) \text{ si et seulement si } (x \in A \text{ et } x \notin B).$$

Enfin, on dira que A et B sont disjoints si $A \cap B = \emptyset$.

Remarque 1.3. *Si A et B sont définis par compréhension, $A = \{x \in E, P(x)\}$ et $B = \{x \in E, Q(x)\}$ on a :*

$$A \cap B = \{x \in E, P(x) \text{ et } Q(x)\}, \quad A \cup B = \{x \in E, P(x) \text{ ou } Q(x)\}$$

Exemple
Si $A = \{1,2,3\}, \quad B = \{3,4,5\}$ on a $A \cap B = \{3\}$ et $A \cup B = \{1,2,3,4,5\}$.

Définition 1.4. *Soit E un ensemble, il existe un ensemble formé de toutes les parties de l'ensemble E, noté $\mathcal{P}(E)$.*

Exemples
- $\emptyset \in \mathcal{P}(E)$ et $E \in \mathcal{P}(E)$.
- $\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$.

Définition 1.5. *Soit E un ensemble, on appelle partition de E une partie $\mathcal{A}$ de $\mathcal{P}(E)$ telle que :*
- *$\forall x \in E, \exists A \in \mathcal{A}$ tel que $x \in A$.*
- *$\emptyset \notin \mathcal{A}$.*
- *$\forall (A,B) \in \mathcal{A}^2$ tels que $A \neq B$, on a $A \cap B = \emptyset$.*

Exemples
- Les nombres pairs et les nombres impairs forment une partition des nombres naturels.
- Soit E un ensemble et A une partie non vide de E, alors $\{A, A^c\}$ forme une partition de E.

Proposition 1.1. *Soient E un ensemble et A, B, C trois parties de E. On a alors les propriétés suivantes :*
- $(A^c)^c = A$.
- $(A \cup B) \cup C = A \cup (B \cup C)$. ***(associativité)***
- $(A \cup B) \cup C = A \cup (B \cup C)$. ***(associativité)***
- $A \cup B = B \cup A$ *et* $A \cap B = B \cap A$. ***(commutativité)***
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. ***(Distributivité de $\cup$ par rapport à $\cap$)***
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. ***(Distributivité de $\cap$ par rapport à $\cup$)***
- $(A \cap B)^c = A^c \cup B^c$ *et* $(A \cup B)^c = A^c \cap B^c$.
- $A \subset B \Longrightarrow B^c \subset A^c$.

Définition 1.6. *Soient E et F deux ensembles, le* ***produit cartésien*** *de E et F noté $E \times F$ est l'unique ensemble défini par :*

$$E \times F = \{(a, b), \quad a \in E, \quad b \in F\}.$$

Remarque 1.4. *Si $E = F$ on écrira E^2 au lieu de $E \times E$.*
On peut étendre la définition à un nombre fini d'ensemble :

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n), a_1 \in A_1, \quad a_2 \in A_2, \quad \ldots, \quad a_n \in A_n\}.$$

Si $A_1 = A_2 = \cdots = A_n = A$, on notera encore A^n au lieu de $A \times A \times \cdots \times A$.
Attention on a en général $A \times B \neq B \times A$.

Exemple
$\{0, 1\} \times \{a, b, c\} = \{(0, a), (0, b), (0, c), (1, a), (1, b), (1, c)\}$.

2 Application

2.1 Définitions

Définition 2.1. *Soient E et F deux ensembles. On appelle* ***application*** *f de E vers F la donnée d'un* ***ensemble de départ*** *E, d'****un ensemble d'arrivée*** *F tels que et pour tout $x \in E$, il existe un unique $y = f(x) \in F$* ***image*** *de x par cette application. Une application sera généralement notée*

$$\begin{aligned} f : & E \longrightarrow F \\ & x \longrightarrow f(x) \end{aligned}$$

On appelle ***graphe*** *de f et on note Γ_f la partie de $E \times F$ définie par : $\Gamma_f = \{(x, y) \in E \times F \text{ tel que } y = f(x)\}$.*
On appelle ***image de f*** *et on note Imf la partie de F définie par $Imf = \{y \in F \text{ tel que } \exists x \in E, y = f(x)\}$*
Soit $(x, y) \in E \times F$, on dit que x est un ***antécédent*** *de y par f si et seulement si $y = f(x)$.*
On note E^F ou $\mathcal{F}(E, F)$ l'ensemble de toutes les applications de E dans F.

Exemple
L'application identité sur E

$$\begin{aligned} id_E : & E \longrightarrow E \\ & x \longrightarrow id_E(x) = x \end{aligned}$$

Proposition 2.1. *Soient f et g deux applications, on dit que f est égale à g et on note $f = g$ si f et g ont leurs ensembles de départ et d'arrivée égaux et si $\forall x \in E, f(x) = g(x)$.*

Définition 2.2. *Soient E,F et G trois ensembles et $f \in E^F, g \in F^G$. On définit alors l'application, $h \in E^G$, composée de f et g par :*

$$\forall x \in E, h(x) = g\left(f(x)\right).$$

On note $h = g \circ f$.

Proposition 2.2. *Soient E,F,G et H quatres ensembles et $f \in E^F, g \in F^G, h \in G^H$. On a alors la propriété d'associativité suivante :*

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

Remarque 2.1. *ATTENTION! La composition n'est pas commutative on a* ***pas*** *en général $f \circ g = g \circ f$ Par exemple si*

$$\begin{aligned} f : & \mathbb{R} \longrightarrow \mathbb{R} \\ & x \longrightarrow x^2 \end{aligned} \qquad \begin{aligned} g : & \mathbb{R} \longrightarrow \mathbb{R} \\ & x \longrightarrow x + 1 \end{aligned}$$

2.2 Injections, surjections, bijections

Définition 2.3. *Soient E et F deux ensembles et $f : E \mapsto F$, alors*
- *On dit que f est* ***injective*** *si $\forall y \in F$, il existe au plus un antécédent de y par f.*
- *On dit que f est* ***surjective*** *si $\forall y \in F$, il existe au moins un antécédent de y par f.*
- *On dit que f est* ***bijective*** *si elle est injective et surjective, c'est-à-dire si $\forall y \in F, \exists! x \in E$ tel que $f(x) = y$.*

Exemples   Soient $E = \{0, 1, \ldots, 4\}$ et f l'application définie par

$$\begin{aligned} f :&\mathbb{N} \longrightarrow E \\ &n \longrightarrow r_5(n) \end{aligned}$$

où $r_5(n)$ est le reste de la division euclidienne de n par 5. Alors f est une application surjective.

Soit E un ensemble et $A \subset E$, alors l'application i_A définie par

$$\begin{aligned} i_A :&A \longrightarrow E \\ &x \longrightarrow x \end{aligned}$$

est injective. L'application i_A est appelée **injection canonique de A dans E**.

Soit $P = \{n \in N, \text{ tel que } \exists k \in \mathbb{N}, \quad n = 2k\}$, alors l'application :

$$\begin{aligned} h :&P \longrightarrow \mathbb{N} \\ &n \longrightarrow n/2 \end{aligned}$$

est bijective.

Proposition 2.3. *Avec les notations précédentes, on a*
- *f est injective $\iff \forall (x_1, x_2) \in E^2, \quad f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$.*
- *f est injective $\iff \forall (x_1, x_2) \in E^2, \quad x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)$.*
- *f est surjective $\iff \forall y \in F, \exists x \in E, y = f(x)$.*
- *f est surjective $\iff \forall y \in F, \exists! x \in E, y = f(x)$.*

Remarque 2.2. *Si $f : E \mapsto F$ est une application non injective (resp. non surjective), on peut la rendre injective (resp. surjective) en réduisant son espace de départ (resp. d'arrivée). Par exemple si $f : E \mapsto F$ est une application quelconque alors $f : E \mapsto Imf$ est surjective. Soit $A \subset E$ et $B \subset deF$, on note $f|_A$ l'application $f : A \mapsto F$ restreinte au départ à A, et $f|^B$ l'application $f : E \mapsto B$ l'application restreinte à l'arrivée à B.*

Proposition 2.4. *Soit $f : E \mapsto F$ une application, on a alors :*

$$f \text{ est surjective } \iff Imf = F$$

Proposition 2.5. *Soient* $f : E \mapsto F$ *et* $g : F \mapsto G$ *deux applications, on a :*
- f *et* g *injectives* $\Longrightarrow g \circ f$ *injective.*
- f *et* g *surjectives* $\Longrightarrow g \circ f$ *surjective.*
- f *et* g *bijectives* $\Longrightarrow g \circ f$ *bijective.*

Définition 2.4. *Soit* $f : E \mapsto F$ *une application bijective. Il existe une unique application, notée* f^{-1}*, appelée* ***application réciproque de*** f *telle que :*

$$f^{-1} : F \mapsto E$$

$$f^{-1} \circ f = id_E, \qquad f \circ f^{-1} = id_F$$

Proposition 2.6. *Soient* $f : E \mapsto F$ *et* $g : F \mapsto G$ *deux applications bijectives, on a alors :* f^{-1} *est bijective* $(f^{-1})^{-1} = f$ *et* $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Définition 2.5. *Soient* $f : E \mapsto F$*,* $A \subset E, B \subset F$*, on définit alors :*
- ***L'image de A par f****, le sous ensemble de* F *noté* $f(A)$ *défini par* $f(A) = \{y \in F | \exists x \in A \text{ tel que } f(x) = y\}$.
- ***L'image réciproque de B par f****, le sous ensemble de* E *noté* $f^{-1}(B)$ *défini par* $f^{-1}(B) = \{x \in E | f(x) \in B\}$.

Remarque 2.3. ***ATTENTION!!!!*** *L'écriture* $f^{-1}(B)$ *ne signifie* ***pas*** *que* f *est bijective. Par exemple, prenons* $f : \mathbb{R} \mapsto \mathbb{R}$ *définie par* $f(x) = x^2$ *alors* f *n'est pas bijective néanmoins nous pouvons calculer* $f^{-1}([1, 2]) = \{x \in \mathbb{R} | x^2 \in [1, 2]\} = [1, \sqrt{2}]$.

3 Relations Binaires

3.1 Définitions

Définition 3.1. *Soit E un ensemble non vide, on appelle* ***relation binaire*** *sur E une application qui à chaque couple $(x, y) \in E^2$ associe une valeur de vérité : vrai ou faux. Soit $(x, y) \in E^2$ et $\mathcal{R}$ une relation binaire, si la valeur associé au couple (x, y) est vrai on écrira $x\mathcal{R}y$.*

Exemple
Si $E = \mathbb{N} \setminus \{0\}$ on peut définir la relation :

$$x\mathcal{R}y \Longleftrightarrow x \text{ divise } y.$$

De sorte que $2\mathcal{R}6$, mais $non(6\mathcal{R}2)$.

Définition 3.2. *Soient E un ensemble non vide et $\mathcal{R}$ une relation binaire sur E. On dit que :*
- *$\mathcal{R}$ est* ***réflexive*** *si et seulement si $\forall x \in E, x\mathcal{R}x$.*
- *$\mathcal{R}$ est* ***symétrique*** *si et seulement si $\forall (x, y) \in E^2, x\mathcal{R}y \Longleftrightarrow y\mathcal{R}x$*
- *$\mathcal{R}$ est* ***antisymétrique*** *si et seulement si $\forall (x, y) \in E^2, (x\mathcal{R}y \text{ et } y\mathcal{R}x) \Longrightarrow x = y$*
- *$\mathcal{R}$ est* ***transitive*** *si et seulement si $\forall (x, y, z) \in E^3, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Longrightarrow x\mathcal{R}z$.*

Exemple
La relation de l'exemple précédent est réflexive, non symétrique, antisymétrique et transitive.

3.2 Relation d'équivalence

Définition 3.3. *Soient E un ensemble et $\mathcal{R}$ une relation binaire sur E, on dit que $\mathcal{R}$ est une* ***relation d'équivalence*** *si $\mathcal{R}$ est réflexive, symétrique et transitive.*

Exemples
L'égalité est une relation d'équivalence dans n'importe quel ensemble.
Soit U_0 l'ensemble des suites ne s'annulant pas. Alors la relation d'équivalence des suites et une relation d'équivalence.
Pour les mots, "être un anagramme de" est une relation d'équivalence.

Définition 3.4. *Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E, on appelle* ***classe d'équivalence de x (modulo $\mathcal{R}$)*** *l'ensemble $\overline{x}$ défini par $\overline{x} = \{y \in E | x\mathcal{R}y\}$. Si $\overline{x}$ est une classe d'équivalence et $y \in \overline{x}$ on a $\overline{x} = \overline{y}$. Enfin on dira que x est un* ***représentant*** *de $\overline{x}$*

Exemple
Si on considère la relation d'équivalence sur les mots *"être un anagramme de"* on a alors

$$\overline{ET} = \{ET, TE\}, \quad \overline{MOT} = \{MOT, MTO, OMT, OTM, TOM, TMO\}$$

Définition 3.5. *Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E, on appelle* ***ensemble quotient de** E **par** $\mathcal{R}$* *l'ensemble des classe d'équivalence modulo $\mathcal{R}$. On le note $E/\mathcal{R}$.*

Proposition 3.1. *Pour toute relation d'équivalence $\mathcal{R}$ sur E, les classes d'équivalences forment une partition de E.*

Pour finir cette partie nous allons étudier un exemple important. Soit $n \in \mathbb{Z}$, considérons la relation d'équivalence sur $\mathbb{Z}$

$$x\mathcal{R}y \Longleftrightarrow \exists k \in \mathbb{Z}, \quad x - y = nk.$$

Vérifions qu'il s'agit bien d'une relation d'équivalence :

- **Réflexivité** : Soit $x \in \mathbb{Z}$ alors $x - x = 0 = n \cdot 0$ donc $x\mathcal{R}x$.
- **Symétrie** : Soit $(x, y) \in \mathbb{Z}^2$ on a alors

$$x\mathcal{R}y \Longleftrightarrow \exists k \in \mathbb{Z} x - y = nk \Longleftrightarrow \exists k \in \mathbb{Z} y - x = -nk \Longleftrightarrow \exists k' \in \mathbb{Z} x - y = nk' \Longleftrightarrow y\mathcal{R}x.$$

- **transitivité** : Soit $(x, y, z) \in \mathbb{Z}^3$ tel que $x\mathcal{R}y$ et $y\mathcal{R}z$, il existe donc k et k' tels que $x - y = nk$ et $y - z = nk'$ et donc $x - z = x - y + y - z = nk + nk' = n(k + k')$ et donc $x\mathcal{R}z$.

Cette relation d'équivalence est appelée congruence modulo n, si deux entiers x et y sont en relation on dira qu'ils sont congrus modulo n et on notera

$$x \equiv y \pmod{n}$$

Les classes d'équivalences pour la relation de congruence modulo n sont de la forme :

$$\overline{x} = \{\ldots, x - 3n, x - 2n, x - n, x, x + n, x + 2n, x + 3n, \ldots\} = x + n\mathbb{Z}.$$

par exemple pour $n = 3$, on a $\overline{0} = \{\ldots - 6, -3, 0, 3, 6, \ldots\} = \overline{3}$.

Soit $x \in \mathbb{Z}$, on peut trouver un représentant de $\overline{x}$ entre 0 et $n-1$, en effectuant la divisions euclidienne de x par n, en effet on sait qu'il existe $(q, r) \in \mathbb{Z}$ tel que :

$$x = qn + r, \qquad 0 \leq r \leq n - 1,$$

de sorte que x et r sont dans la même classe d'équivalence et donc $\overline{x} = \overline{r}$.

Enfin l'ensemble quotient $\mathbb{Z}/\mathcal{R}$ est l'ensemble des classes d'équivalence modulo n on le note $\mathbb{Z}/n\mathbb{Z}$, on peut donner une représentation simple de $\mathbb{Z}/n\mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

3.3 Relation d'ordre

Définition 3.6. *Soient E un ensemble et $\mathcal{R}$ une relation binaire sur E, on dit alors que*
- *$\mathcal{R}$ est une **relation d'ordre** si $\mathcal{R}$ est réflexive, antisymétrique et transitive.*
- *$(E, \mathcal{R})$ est un **ensemble ordonné** si $\mathcal{R}$ est une relation d'ordre.*
- *$\mathcal{R}$ est une **relation d'ordre total** si $\forall (x, y) \in E^2, x\mathcal{R}y$ ou $y\mathcal{R}x$.*
- *$(E, \mathcal{R})$ est un **ensemble totalement ordonnée** si $\mathcal{R}$ est total.*
- *$\mathcal{R}$ est une **relation d'ordre partiel** si $\mathcal{R}$ n'est pas total.*

Exemples
- $(\mathbb{R}, \leq)$ est ensemble totalement ordonné.
- Soit E l'ensemble des mots, l'ordre du dictionnaire est appelé ordre lexicographique ou alphabétique. E muni de cette relation d'ordre est un ensemble totalement ordonné.
- $(\mathcal{P}(E), \subset)$ est un ensemble partiellement ordonné.

Définition 3.7. *Soient $(E, \mathcal{R})$ un ensemble ordonné, $A \subset E$ et $(M, m) \in E^2$. On dit que :*
- *M **est un majorant de A** si et seulement si $\forall x \in A, x\mathcal{R}M$.*
- *M **est un minorant de A** si et seulement si $\forall x \in A, m\mathcal{R}x$.*

On note $Maj(A)$, (resp $Min(A)$) l'ensemble des majorants (resp. minorants) de A.
On dira que x est le plus grand élément ou le maximum de A noté $max(A)$, (resp. le plus petit élément ou le minimum de A noté $min(A)$), si $x \in A \cap Maj(A)$ (resp. $x \in A \cap Min(A)$).

Exemples
- Pour $(\mathbb{R}, \leq)$, 3 est un majorant de $[0, 1]$.
- Pour $(\mathbb{R}, \geq)$, -1 est un majorant de $[0, 1]$.

Remarque 3.1.
1. *Si x est un majorant de A et $x\mathcal{R}y$, alors par transitivité de $\mathcal{R}$, y est aussi un majorant, ainsi il n'y a pas unicité du majorant en général.*
2. *Un sous ensemble A ne possède pas forcément de plus grand élément, par exemple pour $(\mathbb{R}, \leq)$, considérons $A = [0, 1[$ alors $Maj(A) =]1, +\infty[$ et $A \cap Maj(A) = \emptyset$.*

Définition 3.8. *Soient $(E, \mathcal{R})$ un ensemble ordonné et $A \subset E$ alors :*
- *A **est une partie majorée de E** si et seulement si A possède un majorant.*
- *A **est une partie minorée de E** si et seulement si A possède un minorant.*
- *A **est une partie bornée de E** si et seulement si A est majorée et minorée.*

Définition 3.9. *Soient $(E, \mathcal{R})$ un ensemble ordonné et $A \subset E$ non vide. Si $Maj(A)$ possède un plus petit élément, celui-ci s'appelle **borne supérieure de A** et se note* $\sup(A)$. *De même on définit la borne inférieure de A notée* $\inf(A)$ *comme étant le plus grand élément de $Min(A)$.*

Exemples
- Pour $(\mathbb{R}, \leq)$, on a $\sup[0, 1[= 1$.
- Pour $(\mathcal{P}(E), \subset)$ on a $\sup\{A, B\} = A \cup B$.

Proposition 3.2. *Soient $(E, \mathcal{R})$ un ensemble ordonné et $A \subset E$ non vide. On a alors l'équivalence suivante :*

$$M = \sup(A) \iff \begin{array}{c} M \in Maj(A) \\ \forall M' \in Maj(A), M\mathcal{R}M'. \end{array}$$

4 Groupes

Définition 4.1. *Une* ***loi de composition interne*** $*$ *est une application*

$$\begin{aligned} E \times E &\longrightarrow E \\ (x, y) &\longrightarrow x * y \end{aligned}$$

Exemple
- Pour $E = \mathbb{N}$, on dispose des lois fondamentales $+, \times$.
- Soit E un ensemble, on dispose dans $\mathcal{P}(E)$ des lois $\cup, \cap$.

Définition 4.2. *Soit G un ensemble muni d'une loi de composition interne $*$. On dit que $(G, *)$ est un* ***groupe*** *si et seulement si :*
- *$*$ est associative : $\forall (x, y, z) \in G^3, \quad (x * y) * z = x * (y * z)$.*
- *$*$ possède un élément neutre $e \in G$: $\forall x \in G, x * e = e * x = x$.*
- *Tout élément de G possède un symétrique : $\forall x \in G, \exists y \in G$ tel que $x * y = y * x = e$.*

Si de plus $*$ est commutative, c'est-à-dire si $\forall (x, y) \in G^2, x * y = y * x$, G est appelé ***groupe commutatif*** *ou* ***groupe abélien****.*

4.1 Définitions

4.2 Morphismes

5 Anneaux

5.1 Définitions

5.2 Morphismes

6 Corps