CHAPITRE 1

RAPPELS SUR LES ENSEMBLES ET FONCTIONS

Nous rappelons ici quelques notions de base de la théorie des ensembles et les notations utilisées. Nous définirons les ensembles et les notions de fonctions, relations, opérations qui sont fondamentales dans toute la suite.

1.1 Ensembles

Soit E un *ensemble* et e un *élément*, $e \in E$ signifie que e est un élément qui est dans l'ensemble E et se lit e appartient à E. La négation de cette relation, c'est-à-dire e n'appartient pas à E, s'écrit $e \notin E$. L'ensemble vide est un ensemble qui ne contient aucun élément, il est noté $\emptyset$.

A, B étant deux ensembles, on dit que A est un sous-ensemble de B ou une partie de B ou encore que A est inclus dans B, et on note $A \subseteq B$, si et seulement si tout élément de A appartient à B. La négation de $A \subseteq B$ s'écrit $A \nsubseteq B$ et ne veut pas du tout dire $B \subseteq A$. On peut remarquer que $A = B$ si et seulement si $A \subseteq B$ et $B \subseteq A$, c'est-à-dire si et seulement si A et B ont les mêmes éléments. Si $A \subseteq B$ mais que $A \neq B$, on écrit $A \subsetneq B$. Enfin, on note $\mathcal{P}(E)$ l'ensemble des parties de E ; donc $A \subseteq E$ si et seulement si $A \in \mathcal{P}(E)$. Remarquons que les ensembles $\emptyset$ et E sont toujours des éléments de $\mathcal{P}(E)$.

EXEMPLE 1.1 Soit $E = \{0, 1\}$. $\mathcal{P}(E) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

On appelle *produit cartésien* de deux ensembles E et F l'ensemble des couples formés d'un élément de E et d'un élément de F : $E \times F = \{(x, y) \,/\, x \in E \text{ et } y \in F\}$. Le produit cartésien se généralise à une famille finie d'ensembles :

$$E_1 \times \cdots \times E_n = \{(x_1, \ldots, x_n) \,/\, x_1 \in E_1, \ldots, x_n \in E_n\}$$

Finalement, on note $E^n = E \times \cdots \times E$ le produit cartésien de E par lui-même n fois, pour $n \geq 1$. E^n peut être défini récursivement par : $E_1 = E$ et $E^n = E \times E^{n-1}$.

1.1.1 Réunion, intersection, différence, complémentaire, partition

On suppose dans toute la suite que l'on travaille dans un ensemble référentiel E. Soient A, B deux parties de E. On définit :

- l'*intersection* de A et B : $A \cap B = \{e \in E \,/\, e \in A \text{ et } e \in B\}$,
- l'*union* de A et B : $A \cup B = \{e \in E \,/\, e \in A \text{ ou } e \in B\}$,
- la *différence* de A et B : $A \setminus B = \{e \in E \,/\, e \in A \text{ et } e \notin B\}$,
- le *complémentaire* de A dans E, noté $\overline{A}$ ou A^c : $\overline{A} = E \setminus A = \{e \in E \,/\, e \notin A\}$,
- la *différence symétrique* de A et B : $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

On dit que deux ensembles A et B de E sont *disjoints* si et seulement si $A \cap B = \emptyset$.

Exemple 1.2 1. $\overline{E} = \emptyset$, et $\overline{\emptyset} = E$. 2. $A \cap \emptyset = \emptyset$, $A \cup E = E$, $A \triangle E = \overline{A}$. 3. $A \cap A = A \cup A = A \cup \emptyset = A \triangle \emptyset = A \cap E = A$. 4. $A \setminus B = A \cap \overline{B}$. 5. $A \setminus A = A \triangle A = \emptyset$.

Les lois de Morgan permettent de calculer le complémentaire d'une union et d'une intersection : $\overline{A \cup B} = \overline{A} \cap \overline{B}$ et $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

L'union et l'intersection sont des opérations associatives et commutatives . Elles sont de plus distributives l'une par rapport à l'autre, c'est-à-dire

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

On dit qu'une famille finie ou infinie $(A_i)_{i \in I}$ de parties de E est une partition de E si elle vérifie

i) $A_i \neq \emptyset$ pour tout $i \in I$,

ii) $A_i \cap A_j = \emptyset$ pour tous i, j distincts dans I,

iii) $E = \displaystyle\bigcup_{i \in I} A_i$.

1.2 Fonctions

1.2.1 Définitions

Intuitivement, une application f d'un ensemble E dans un ensemble F est un procédé pour associer à chaque élément de E un unique élément $f(x)$ de F.

Soit E et F deux ensembles, on appelle *fonction* de E vers F tout triplet $f = (E, F, \Gamma)$ où Γ est une partie de $E \times F$, telle que pour tout élément de E il y a au plus un élément y de F tel que $(x, y) \in \Gamma$; pour tout élément x de E cet élément y, s'il existe, est appelé image de x et est notée $f(x)$. On dit que E est l'*ensemble de départ*, F l'*ensemble d'arrivée* et Γ le *graphe* de f. L'ensemble $Dom(f) = \{x \in E \,/\, \exists y \in F, (x, y) \in \Gamma\}$ est le *domaine* ou l'*ensemble de définition* de f. L'ensemble

$$Im(f) = \{y \in F \,/\, \exists x \in E, (x, y) \in \Gamma\}$$

est l'*image* de f. Soit $X \subseteq E$, on note

$$f(X) = \{y \in F \,/\, \exists x \in X, (x, y) \in \Gamma\}$$

l'ensemble des images par f des éléments de X. De même, on appelle *antécédent* par f d'un élément $y \in F$ tout élément $x \in E$ tel que $(x, y) \in \Gamma$. Pour $Y \in F$, on note

$$f^{-1}(Y) = \{x \in E \,/\, \exists y \in Y, (x, y) \in \Gamma\}$$

l'ensemble des antécédents par f des éléments de Y.

Avec ces notations, on a $Dom(f) = f^{-1}(F)$ et $Im(f) = f(E)$.

La fonction f est notée $f\colon E \longrightarrow F$. On dit qu'une fonction $f\colon E \longrightarrow F$ est une *application* si son domaine est l'ensemble E tout entier : $Dom(f) = E$. L'ensemble des applications de E dans F est noté F^E.

EXEMPLE 1.3 1. On note $id_E\colon E \longrightarrow E$ l'application identité de E définie par $f(x) = x$ pour tout x de E.

2. On appelle *fonction caractéristique* d'une partie A de E la fonction $\chi_A\colon E \longrightarrow \{0, 1\}$ définie par : $\chi_A(e) = \begin{cases} 1 & \text{si } e \in A, \\ 0 & \text{si } e \notin A. \end{cases}$

Une application $f\colon E \longrightarrow F$ est *injective* (resp. *surjective*, *bijective*) si tout élément $y \in F$ a au plus (resp. au moins, exactement) un antécédent par f. On a donc

- f est injective si et seulement si $\forall x, y \in E,\ f(x) = f(y) \Longrightarrow x = y$
- f est surjective si et seulement si $\forall y \in F,\ \exists x \in E, y = f(x)$
- f est bijective si et seulement si $\forall y \in F,\ \exists! x \in E, y = f(x)$, c'est-à-dire f est injective et surjective (le symbole $\exists!$ signifie "il existe un et un seul").

Soient $f\colon E \longrightarrow F$ et $g\colon F \longrightarrow G$ deux applications, la composition de f et g est l'application $g \circ f : E \longrightarrow G$ définie par $g \circ f(x) = g(f(x))$. Par exemple, si $f\colon E \longrightarrow F$ est une application, on a $f \circ id_E = id_F \circ f = f$. La composition des applications est associative ce qui permet d'écrire sans parenthèses $h \circ g \circ f$.

Soit $f\colon E \longrightarrow F$ une application, soient A et B deux parties de E et soient C et D deux parties de F. On a $f(A \cup B) = f(A) \cup f(B)$ et $f(A \cap B) \subseteq f(A) \cap f(B)$, et $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$ et $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$. Si de plus f est injective alors $f(A \cap B) = f(A) \cap f(B)$. Ces propriétés se montrent facilement et se généralisent à des unions ou intersections quelconques.

Proposition 1.4 *Soient $f\colon E \longrightarrow F$ et $g\colon F \longrightarrow G$ deux applications. 1. f et g injectives $\Longrightarrow g \circ f$ injective. 2. f et g surjectives $\Longrightarrow g \circ f$ surjective. 3. f et g bijectives $\Longrightarrow g \circ f$ bijective.*

1.3 Cardinaux

1.3.1 Ensembles finis

Pour tout entier n, on note $[n]$ l'ensemble $\{1, \ldots, n\}$ des entiers compris entre 1 et n. On démontre la proposition suivante (appelée principe des tiroirs)

Proposition 1.5 *Si $n < m$, il n'existe pas d'injection de $[m]$ dans $[n]$.*

On déduit aisément de cette proposition que deux entiers n et m sont égaux si et seulement si il existe une bijection de $[n]$ vers $[m]$. Un ensemble E est *fini* s'il existe un entier n et une bijection de E vers $[n]$. Cet entier n est alors unique, s'appelle *cardinal* de E et se note $|E|$.

Soient E et F des ensembles finis, et $f\colon E \longrightarrow F$ une application, avec ces notations, on a

$$\begin{array}{lcl} f \text{ injective} & \Longleftrightarrow & \forall y \in F,\ |f^{-1}(\{y\})| \leq 1 \\ f \text{ surjective} & \Longleftrightarrow & \forall y \in F,\ |f^{-1}(\{y\})| \geq 1 \\ f \text{ bijective} & \Longleftrightarrow & \forall y \in F,\ |f^{-1}(\{y\})| = 1 \end{array}$$

De plus, si E est fini et $|E| = |F|$ alors f injective $\Longleftrightarrow f$ surjective $\Longleftrightarrow f$ bijective. Si E n'est pas fini, ces équivalences sont fausses ; par exemple $f\colon \mathbb{N} \Longrightarrow \mathbb{N}$ définie par $f(n) = 2n$ est injective, mais non surjective.

Enfin, les propriétés suivantes sont très utiles

Proposition 1.6 *Soient E et F deux ensembles finis.*

i) *Si E et F sont disjoints alors $|E \cup F| = |E| + |F|$.*

ii) *Si $(A_i)_{i\in[n]}$ est une partition de E alors $|E| = |A_1| + \cdots + |A_n|$.*

iii) $|E \times F| = |E| \times |F|$.

iv) $|F^E| = |F|^{|E|}$, *où F^E désigne l'ensemble des applications de E dans F.*

v) $|\mathcal{P}(E)| = 2^{|E|}$.

1.3.2 Ensembles dénombrables

Le cardinal peut se généraliser à des ensembles non finis, de telle façon que les propriétés suivantes soient vérifiées pour E et F deux ensembles quelconques :

i) $|E| \leq |F| \iff$ il existe une injection de E vers F.

ii) $|E| \geq |F| \iff$ il existe une surjection de E vers F.

iii) $|E| = |F| \iff$ il existe une bijection de E vers F.

Des relations qui précèdent, on peut déduire que s'il existe à la fois une injection et une surjection de E vers F alors il existe une bijection de E vers F.

Un ensemble E est *dénombrable* s'il est en bijection avec l'ensemble $\mathbb{N}$ des entiers naturels. On note ω le cardinal de $\mathbb{N}$. Une union $\bigcup_{i\in I} A_i$ est dite dénombrable si l'ensemble I d'indices est dénombrable.

Les ensembles dénombrables vérifient les propriétés suivantes :

- Toute partie d'un ensemble dénombrable est finie ou dénombrable.
- Tout produit cartésien fini d'ensembles dénombrables est dénombrable.
- Toute union dénombrable d'ensembles dénombrables est dénombrable.

Enfin signalons qu'il existe des ensembles non dénombrables. Ceci provient du résultat suivant :

Proposition 1.7 *Soit E un ensemble et soit $\mathcal{P}(E)$ l'ensemble des parties de E. On a*

$$|E| < |\mathcal{P}(E)|\,.$$

On en déduit que $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable.

1.4 Opérations et relations

Une *opération* Φ sur un ensemble E est une application $\Phi\colon E^n \longrightarrow E$. On dit que n est l'*arité*, ou le *rang*, de Φ, ou encore que Φ est une opération n-aire, et on note $a(\Phi) = n$; on étudie principalement les opérations d'arité deux, ou opérations binaires.

1.4.1 Opérations binaires

Une *opération binaire* ou *loi de composition interne* $*$ sur un ensemble E est une application $*\colon E \times E \longrightarrow E$. L'image d'un couple (x, y) par cette opération est notée $x * y$ (notation infixe). On définit les propriétés suivantes

i) $*$ est *associative* si $\forall a, b, c \in E$, $a * (b * c) = (a * b) * c$,

ii) $*$ est *commutative* si $\forall a, b \in E$, $a * b = b * a$,

iii) $*$ admet l'élément $\mathbb{1}$ pour *élément neutre* si $\forall e \in E$, $e * \mathbb{1} = \mathbb{1} * e = e$.

Si une opération $*$ est associative, on notera $a * b * c$ (sans parenthèses) le produit des trois éléments a, b et c, qu'on peut indifféremment calculer en faisant $(a * b) * c$ ou $a * (b * c)$. Plus généralement, on notera $e_1 * e_2 * \cdots * e_n$ le produit de n éléments.

Définition 1.8 *Un ensemble E muni d'une opération $*$ associative est un semi-groupe. Si de plus E possède un élément neutre e pour $*$ on dit que $(E, *, e)$ est un monoïde. Si la loi $*$ est commutative, le semi-groupe (resp. le monoïde) est dit commutatif.*

Exemple 1.9 L'ensemble $\mathbb{N}$ muni de l'addition $+$ et de l'élément neutre 0 est un monoïde commutatif. L'ensemble $\mathbb{N}$ muni de la multiplication $\times$ et de l'élément neutre 1 est aussi un monoïde commutatif.

Exemple 1.10 L'ensemble $\mathcal{P}(E)$ muni de l'intersection (ou de l'union) est un monoïde commutatif. L'ensemble des applications de E dans lui-même muni de la composition des applications est un monoïde non commutatif dès que E a au moins deux éléments. L'ensemble des matrices carrées d'ordre n, à coefficients dans $\mathbb{R}$ est un monoïde, non commutatif si $n > 1$, pour l'opération de multiplication des matrices.

Un cas particulier de monoïdes, sont les *monoïdes libres*.

Définition 1.11 *Soit A un ensemble fini appelé alphabet et dont les éléments sont appelés lettres. Le monoïde libre sur A, noté A^*, est l'ensemble des mots écrits sur l'alphabet A. Un mot u est simplement une suite finie de lettres.*

Le nombre d'éléments de la suite est appelé longueur du mot et noté $|u|$. Si le mot u de longueur n est la suite $(u_1, u_2, \ldots, u_n)$, on le note simplement $u = u_1 u_2 \cdots u_n$. Par exemple, $aaba, acebdacebd, a, b, aa, aaa$ sont des mots sur l'alphabet $A = \{a, b, c, d, e\}$. Le mot vide, noté ε, est un mot particulier de A^* qui ne contient aucune lettre (la suite vide). La loi qui fait de A^* un monoïde est appelée *concaténation*. La concaténation de deux mots $u = u_1 u_2 \cdots u_n$ et $v = v_1 v_2 \cdots v_m$ est le mot $u \cdot v = u_1 u_2 \cdots u_n v_1 v_2 \cdots v_m$. Par exemple, $aaba \cdot cde = aabacde$. L'élément neutre pour la concaténation est bien sûr le mot vide ε.

Définition 1.12 *Un ensemble E muni d'une opération $*$ est un groupe si c'est un monoïde et que tout élément admet un inverse, c'est-à-dire $\forall e \in E, \exists e' \in E$ tel que $e * e' = e' * e = \mathbb{1}$ (où $\mathbb{1}$ désigne l'élément neutre pour $*$). Si de plus $*$ est commutative le groupe est dit commutatif.*

Exemple 1.13 L'ensemble $\mathbb{Z}$ des entiers relatifs muni de l'addition est un groupe commutatif. Si E muni d'une opération $*$ est un monoïde alors l'ensemble des éléments inversibles de E forme un groupe. En particulier, l'ensemble des matrices carrées inversibles d'ordre n, à coefficients dans $\mathbb{R}$ est un groupe, non commutatif si $n > 1$, pour l'opération de multiplication des matrices.

Soient $\top$ et $\perp$ deux lois sur un ensemble E. $\top$ est *distributive* par rapport à $\perp$ si $\forall a, b, c \in E$,

$$a \top (b \perp c) = (a \top b) \perp (a \top c) \quad \text{et} \quad (a \perp b) \top c = (a \top c) \perp (b \top c).$$

Si la loi $\top$ est commutative, une seule des conditions est bien sûr suffisante.

Exemple 1.14 Dans $\mathbb{R}$, la multiplication est distributive par rapport à l'addition. Dans $\mathcal{P}(E)$, l'intersection et l'union sont distributives l'une par rapport à l'autre.

1.4.2 Relations

Définition 1.15 *Une relation sur un ensemble E est la donnée d'une partie $\mathcal{R}$ de $E \times E$. Pour indiquer qu'une paire (e, e') de $E \times E$ est dans cette partie $\mathcal{R}$, on utilisera, selon les cas, l'une des notations suivantes : $(e, e') \in \mathcal{R}$, $e \,\mathcal{R}\, e'$, $\mathcal{R}(e, e')$.*

Exemple 1.16 Sur $E = \mathbb{N}$, les ensembles suivants sont des relations

- l'ensemble $\{(n, m) \,/\, n \leq m\}$,
- l'ensemble $\{(n, m) \,/\, n \leq m \leq 2n\}$,
- l'ensemble $\{(n, m) \,/\, n \leq m \text{ et } \exists k : n^2 + m^2 = k^2\}$.

Sur $E = \mathcal{P}(A)$, l'inclusion est une relation.

1.4.3 Opérations ensemblistes sur les relations

Puisqu'une relation est un ensemble on peut définir aisément

– le *complémentaire* $\overline{\mathcal{R}}$ d'une relation $\mathcal{R}$; $\overline{\mathcal{R}}$ est le complémentaire de $\mathcal{R}$ dans $E \times E$:

$$(e, e') \in \overline{\mathcal{R}} \quad \Longleftrightarrow \quad (e, e') \notin \mathcal{R},$$

– la *réunion* $\mathcal{R}_1 \cup \mathcal{R}_2$ de deux relations $\mathcal{R}_1$ et $\mathcal{R}_2$:

$$(e, e') \in \mathcal{R}_1 \cup \mathcal{R}_2 \quad \Longleftrightarrow \quad (e, e') \in \mathcal{R}_1 \text{ ou } (e, e') \in \mathcal{R}_2,$$

– l'*intersection* $\mathcal{R}_1 \cap \mathcal{R}_2$ de deux relations $\mathcal{R}_1$ et $\mathcal{R}_2$:

$$(e, e') \in \mathcal{R}_1 \cap \mathcal{R}_2 \quad \Longleftrightarrow \quad (e, e') \in \mathcal{R}_1 \text{ et } (e, e') \in \mathcal{R}_2.$$

On peut définir aussi trois relations particulières

– la *relation vide*, notée $\emptyset_E$: $\forall e, e' \in E \quad , \quad (e, e') \notin \emptyset_E$,
– la *relation pleine*, notée $\mathbf{\Pi}_E$: $\forall e, e' \in E \quad , \quad (e, e') \in \mathbf{\Pi}_E$,
– la *relation identité*, notée Id_E : $\forall e, e' \in E \quad , \quad (e, e') \in Id_E \iff e = e'$.

Puisque $\mathcal{R}_1$ et $\mathcal{R}_2$ sont des ensembles, on peut écrire $\mathcal{R}_1 \subseteq \mathcal{R}_2$ pour exprimer que

$$\forall e, e' \in E, \;\; (e, e') \in \mathcal{R}_1 \quad \Longrightarrow \quad (e, e') \in \mathcal{R}_2.$$

1.4.4 Autres opérations sur les relations

Soit $\mathcal{R}$ une relation binaire sur E. La *relation inverse*, notée $\mathcal{R}^{-1}$, est définie par

$$e \, \mathcal{R}^{-1} \, e' \quad \Longleftrightarrow \quad e' \, \mathcal{R} \, e.$$

Soient $\mathcal{R}_1$ et $\mathcal{R}_2$ deux relations binaires sur E. Leur *produit*, noté $\mathcal{R}_1 . \mathcal{R}_2$, est la relation définie par $e \left(\mathcal{R}_1 . \mathcal{R}_2\right) e' \quad \Longleftrightarrow \quad \exists e'' : e \, \mathcal{R}_1 \, e'' \text{ et } e'' \, \mathcal{R}_2 \, e'$.

Ce produit est associatif ; il a Id_E pour élément neutre.

Soit $\mathcal{R}$ une relation binaire. La relation $\mathcal{R}^*$ est égale à

$$Id_E \cup \mathcal{R} \cup (\mathcal{R}.\mathcal{R}) \cup (\mathcal{R}.\mathcal{R}.\mathcal{R}) \cup \cdots$$

ou encore $\displaystyle\bigcup_{i \geq 0} \mathcal{R}^i$ avec $\mathcal{R}^0 = Id_E$, $\mathcal{R}^{i+1} = \mathcal{R}.\mathcal{R}^i$, pour $i \geq 0$. La relation $\mathcal{R}^+$ est définie par $\mathcal{R}^+ = \displaystyle\bigcup_{i > 0} \mathcal{R}^i$ et donc $\mathcal{R}^* = Id_E \cup \mathcal{R}^+$. On admettra que $\forall i, j \leq 0, \mathcal{R}^{i+j} = \mathcal{R}^i . \mathcal{R}^j$.

1.4.5 Relations d'équivalence

Définition 1.17 *Une relation d'équivalence est une relation réflexive, symétrique et transitive.*

EXEMPLE 1.18

i) L'égalité sur un ensemble E est une relation d'équivalence, notée $=$ ou aussi Id_E (*cf.* section 1.4.3).

ii) Soit n un entier supérieur ou égal à 2, la relation sur $\mathbb{Z}$: "x et y ont même reste dans la division par n" est une relation d'équivalence. On la note $x \equiv y[n]$, ou aussi $x \equiv y \bmod n$, et on dit que "x et y sont *congrus modulo* n".

L'intersection $\mathcal{R}\cap\mathcal{R}'$ de deux relations d'équivalence est encore une relation d'équivalence, mais la réunion $\mathcal{R}\cup\mathcal{R}'$ et le produit $\mathcal{R}.\mathcal{R}'$ peuvent ne pas être des relations d'équivalence.

Proposition 1.19 *Si $\mathcal{R}$ est une relation quelconque, $(\mathcal{R} \cup \mathcal{R}^{-1})^*$ est une relation d'équivalence, et c'est la plus petite relation d'équivalence qui contient $\mathcal{R}$.*

Définition 1.20 *Soit $\mathcal{R}$ une relation d'équivalence sur E, et e un élément de E, l'ensemble $\{e' \in E \,/\, e\,\mathcal{R}\,e'\}$, noté $[e]_\mathcal{R}$, est appelé la classe d'équivalence de e.*

Proposition 1.21 *1) $\forall e \in E$, $e \in [e]_\mathcal{R}$, 2) $\forall e, e' \in E$, $e\,\mathcal{R}\,e' \Longrightarrow [e]_\mathcal{R} = [e']_\mathcal{R}$, 3) si $[e]_\mathcal{R} \cap [e']_\mathcal{R} \neq \emptyset$, alors $[e]_\mathcal{R} = [e']_\mathcal{R}$.*

Démonstration. Le premier point est évident puisque $e\,\mathcal{R}\,e$. Pour montrer le second point, considérons $e'' \in [e']_\mathcal{R}$; alors $e'\,\mathcal{R}\,e''$, et comme $e\,\mathcal{R}\,e'$, on a aussi $e\,\mathcal{R}\,e''$ et $e'' \in [e]_\mathcal{R}$. D'où $[e']_\mathcal{R} \subseteq [e]_\mathcal{R}$. Réciproquement, $[e]_\mathcal{R} \subseteq [e']_\mathcal{R}$ pour les mêmes raisons. Enfin, si $e'' \in [e]_\mathcal{R} \cap [e']_\mathcal{R}$, alors $e\,\mathcal{R}\,e''$ et $e''\,\mathcal{R}\,e'$, donc $e\,\mathcal{R}\,e'$ et $[e]_\mathcal{R} = [e']_\mathcal{R}$. □

L'ensemble $\{[e]_\mathcal{R} \,/\, e \in E\}$ de parties de E, appelé l'*ensemble quotient* de E par $\mathcal{R}$ et noté $E/\mathcal{R}$, est donc une *partition* de E. Réciproquement, si $A \subseteq \mathcal{P}(E)$ est une partition de E (c'est-à-dire, $\forall E_1, E_2 \in A, E_1 \neq E_2 \Longrightarrow E_1 \cap E_2 = \emptyset$ et $\forall e \in E, \exists E_e \in A : e \in E_e$), on peut définir une relation d'équivalence $\mathcal{R}_A$ par $e\,\mathcal{R}_A\,e'$ si et seulement si e et e' sont dans le même élément de la partition ; il est facile de vérifier que c'est bien une équivalence.

1.4.6 Congruences

Définition 1.22 *Une relation d'équivalence $\mathcal{R}$ définie sur un ensemble muni d'une loi de composition interne $*$ est une congruence si elle est compatible avec la loi $*$ c'est-à-dire si $\forall e, e', d, d' \in E,\ (e\,\mathcal{R}\,e'$ et $d\,\mathcal{R}\,d') \quad \Longrightarrow \quad (e * d)\,\mathcal{R}\,(e' * d')$.*

EXEMPLE 1.23 Soit n un entier supérieur ou égal à 2, la relation sur $\mathbb{Z}$: "$x \equiv y[n]$" est une congruence pour l'addition et pour la multiplication.

Si $\mathcal{R}$ est une congruence sur l'ensemble E muni de la loi $*$, la loi $*$ "passe au quotient", c'est-à-dire que l'ensemble quotient $E/\mathcal{R}$ est muni d'une loi $[*]$ en posant $[e][*][e'] = [e * e']$, et l'opération $[*]$ est bien définie (elle ne dépend pas des représentants des classes d'équivalence que l'on a choisis). Pour simplifier, la loi $[*]$ sera notée simplement $*$.

Proposition 1.24 *Soit $\mathcal{R}$ une congruence sur un monoïde (resp. groupe) $(E, *)$ l'ensemble quotient $E/\mathcal{R}$ muni de $*$ est un monoïde (resp. groupe).*

Exemple 1.25 Soit n un entier supérieur ou égal à 2, le quotient de $\mathbb{Z}$ par la relation $x \equiv y[n]$ est noté $\mathbb{Z}/n\mathbb{Z}$, c'est un groupe pour l'addition et un monoïde pour la multiplication.