

## Fondements des mathématiques

### 2. Constructions élémentaires

#### 2.1. Quelques propriétés des quantificateurs

Soient deux ensembles  $E$  et  $F$ , un prédicat binaire  $\mathcal{R}$ , et une variable booléenne  $C$ .

$$\begin{aligned}(\exists x \in E, C) &\Rightarrow C \\(\exists x \in E, C) &\Leftrightarrow (C \text{ et } E \neq \emptyset) \\C &\Rightarrow \forall x \in E, C\end{aligned}$$

Exemple: s'il existe une chaise telle que la Terre est ronde, alors la Terre est ronde. Puis, si la Terre est ronde, alors, quelle que soit la chaise que l'on considèrerait, la Terre serait toujours ronde.

$$\begin{aligned}(\exists x \in E, \forall y \in F, \mathcal{R}(x, y)) &\Rightarrow (\forall y \in F, \exists x \in E, \mathcal{R}(x, y)) \\(\exists x \in E, \exists y \in F, \mathcal{R}(x, y)) &\Leftrightarrow (\exists y \in F, \exists x \in E, \mathcal{R}(x, y)) \\(\forall x \in E, \forall y \in F, \mathcal{R}(x, y)) &\Leftrightarrow (\forall y \in F, \forall x \in E, \mathcal{R}(x, y)). \\(\exists x \in E, x \in F) &\Leftrightarrow (\exists x \in F, x \in E) \Leftrightarrow E \cap F \neq \emptyset \\(\forall x \in E, x \notin F) &\Leftrightarrow (\forall x \in F, x \notin E) \Leftrightarrow E \cap F = \emptyset\end{aligned}$$

**Définition.** On dit que deux ensembles  $E$  et  $F$  sont disjoints ssi  $E \cap F = \emptyset$ .

Sous-entendant partout un même domaine où des prédicats unaires  $\mathcal{A}$ ,  $\mathcal{B}$  sont valides,

$$\begin{aligned}((\exists x, \mathcal{A}(x)) \text{ ou } (\exists x, \mathcal{B}(x))) &\Leftrightarrow (\exists x, \mathcal{A}(x) \text{ ou } \mathcal{B}(x)) \\((\forall x, \mathcal{A}(x)) \text{ et } (\forall x, \mathcal{B}(x))) &\Leftrightarrow (\forall x, \mathcal{A}(x) \text{ et } \mathcal{B}(x)) \\(\exists x, C \text{ ou } \mathcal{A}(x)) &\Rightarrow (C \text{ ou } \exists x, \mathcal{A}(x)) \\(C \text{ et } \forall x, \mathcal{A}(x)) &\Rightarrow (\forall x, C \text{ et } \mathcal{A}(x)) \\(\forall x, C \Rightarrow \mathcal{A}(x)) &\Leftrightarrow (C \Rightarrow \forall x, \mathcal{A}(x)) \\(\forall x, \mathcal{A}(x) \Rightarrow C) &\Leftrightarrow ((\exists x, \mathcal{A}(x)) \Rightarrow C) \\((\forall x, \mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \text{ et } (\forall x, \mathcal{A}(x))) &\Rightarrow (\forall x, \mathcal{B}(x)) \\(\exists x, C \text{ et } \mathcal{A}(x)) &\Leftrightarrow (C \text{ et } \exists x, \mathcal{A}(x)) \\(\forall x, C \text{ ou } \mathcal{A}(x)) &\Leftrightarrow (C \text{ ou } \forall x, \mathcal{A}(x))\end{aligned}$$

Appliquant les deux dernières formules à la sorte booléenne, on a pour trois variables booléennes  $A$ ,  $B$ ,  $C$ , les distributivités

$$\begin{aligned}((A \text{ et } B) \text{ ou } C) &\Leftrightarrow ((A \text{ ou } C) \text{ et } (B \text{ ou } C)) \\((A \text{ ou } B) \text{ et } C) &\Leftrightarrow ((A \text{ et } C) \text{ ou } (B \text{ et } C)).\end{aligned}$$

On abrègera  $\forall x \in E, \forall y \in E, \mathcal{R}(x)$  en  $\forall x, y \in E, \mathcal{R}(x)$ , et de même pour  $\exists$ . Si  $F \subset E$  on a

$$(\forall x, y \in F, \mathcal{R}(x, y)) \Leftrightarrow (\forall x, y \in E, (x \in F \text{ et } y \in F) \Rightarrow \mathcal{R}(x, y))$$

et de même avec des domaines différents pour  $x$  et  $y$ ; et de même avec des  $\exists$ .

*Quantificateur d'unicité*

Pour tous ensembles  $F \subset E$ , tout prédicat unaire  $\mathcal{A}$  valide sur  $E$ , et tout  $x \in E$ ,

$$\begin{aligned}x \in F &\Leftrightarrow \{x\} \subset F \Leftrightarrow (\exists y \in E, x = y \text{ et } y \in F) \Leftrightarrow (\forall y \in E, x = y \Rightarrow y \in F) \\x \in F &\Rightarrow ((\forall y \in F, \mathcal{A}(y)) \Rightarrow \mathcal{A}(x) \Rightarrow \exists y \in F, \mathcal{A}(y)) \\F \subset \{x\} &\Leftrightarrow (\forall y \in F, x = y) \Rightarrow ((\exists y \in F, \mathcal{A}(y)) \Rightarrow \mathcal{A}(x) \Rightarrow (\forall y \in F, \mathcal{A}(y))) \\F = \{x\} &\Leftrightarrow (x \in F \text{ et } \forall y \in F, x = y) \Leftrightarrow (\forall y \in E, y \in F \Leftrightarrow x = y)\end{aligned}$$

Introduisons 3 nouveaux quantificateurs  $\exists!, !, \exists!$ , qui tout comme  $\exists$  sont des conditions internes à la classe correspondante, et se traduisent donc en prédicats unaires d'argument  $F = \{x \in E, \mathcal{R}(x)\}$ :

$$\begin{aligned} (\exists x \in E, \mathcal{R}(x)) &\Leftrightarrow (\exists : F) \Leftrightarrow (\exists x \in F, \text{vrai}) \Leftrightarrow (\exists x \in E, \{x\} \subset F) \Leftrightarrow F \neq \emptyset \\ (\exists! x \in E, \mathcal{R}(x)) &\Leftrightarrow (\exists! : F) \Leftrightarrow (\exists x, y \in F, x \neq y) \Leftrightarrow (\exists x, y \in E, \mathcal{R}(x) \text{ et } \mathcal{R}(y) \text{ et } x \neq y) \\ (!x \in E, \mathcal{R}(x)) &\Leftrightarrow (! : F) \Leftrightarrow \text{non}(\exists! : F) \Leftrightarrow (\forall x, y \in F, x = y) \Leftrightarrow \forall x \in F, F \subset \{x\} \\ (\exists! x \in E, \mathcal{R}(x)) &\Leftrightarrow (\exists! : F) \Leftrightarrow (\exists x \in F, F \subset \{x\}) \Leftrightarrow (\exists x \in E, F = \{x\}) \end{aligned}$$

L'énoncé " $\exists!x \in E, \mathcal{R}(x)$ " se lit "il existe un unique  $x \in E$  tel que  $\mathcal{R}(x)$ ", ou " $F$  est un singleton".

On a de plus les propriétés suivantes dont la première peut être vue comme propriété de  $=$ , ou comme utilisation du  $\mathcal{A}(x) \Rightarrow (\forall y \in F, \mathcal{A}(y))$  ci-dessus:

$$\begin{aligned} F \subset \{x\} &\Rightarrow (! : F) \\ (\exists! : F) &\Leftrightarrow (F \neq \emptyset \text{ et } (! : F)) \\ F \neq \emptyset &\Rightarrow ((\forall y \in F, \mathcal{A}(y)) \Rightarrow (\exists y \in F, \mathcal{A}(y))) \\ (! : F) &\Rightarrow ((\exists y \in F, \mathcal{A}(y)) \Rightarrow (\forall y \in F, \mathcal{A}(y))) \end{aligned}$$

si  $\exists!x \in E, \mathcal{A}(x)$  alors les énoncés  $B$  qu'on peut formuler sur l'unique objet  $x$  tel que  $\mathcal{A}(x)$  peuvent également s'exprimer sans le symbole de la variable libre " $x$ ", au moyen d'une variable liée par un quantificateur, et de la relation unaire  $A$ .

Une fonction  $f$  est dite *constante* ssi  $(! : \text{Im } f)$ .

#### Traduction des opérateurs en prédicats

Il est possible de reformuler une théorie générique en remplaçant tous ses (ou n'importe quels) symboles d'opérateurs par des symboles de prédicats. Cette même méthode permettrait de formuler une théorie des ensembles en simulant les fonctions par des relations, si l'on n'avait pas choisi de concevoir les relations comme construites au moyen des fonctions.

Dans une théorie générique, soit  $T$  un symbole d'opérateur unaire (par exemple). Le prédicat binaire  $T_0$  défini par  $x, y \mapsto (y = T(x))$  peut servir à remplacer  $T$  de la manière suivante.

D'abord, sans le support de la définition ci-dessus de  $T_0$  au moyen de  $T$ , on doit poser l'axiome  $\forall x, \exists!y, T_0(x, y)$ . Puis, faute de pouvoir remplacer  $T$  par  $T_0$  dans les termes, on se satisfera de le faire les énoncés (où les termes ont finalement vocation à être employés), de la manière suivante.

Dans chaque énoncé ayant pour symbole principal un symbole de prédicat (appliqué à des termes), éliminons une seule occurrence de  $T$  à la fois. L'énoncé peut se relire sous forme abrégée  $R(T(K))$  où  $R$  est un prédicat unaire et  $K$  une constante (tous deux paramétrés). Il est alors remplaçable par  $(\exists z, T_0(K, z) \text{ et } R(x))$ , ou par  $(\forall z, T_0(K, z) \Rightarrow R(x))$ , ce qui revient au même.

#### Définitions d'opérateurs par des prédicats

Inversement, dans toute théorie générique, tout axiome ou théorème de la forme

$$\forall a, b, \exists!x, \mathcal{R}(a, b, x)$$

(où  $\mathcal{R}$  est un quelconque énoncé avec un nombre quelconque de paramètres au lieu de  $a, b$ ) permet d'introduire un symbole d'opérateur  $T$  tel que  $\forall a, b, x, T(a, b) = x \Leftrightarrow \mathcal{R}(a, b, x)$  considéré comme implicitement présent, dans la mesure où son usage est traduisible vers le formalisme initial suivant le procédé ci-dessus avec l'énoncé  $\mathcal{R}$  à la place de  $T_0$ .

#### Remarque sur les axiomes d'existence en théories des ensembles

La forme traditionnelle de la théorie des ensembles (ZF) ne présente que le langage minimum, constitué du seul prédicat  $\in$ . La panoplie des objets utiles que nous présentons par des opérateurs, ne s'y trouve formalisée que par des  $\exists$  dans des axiomes, de la forme suivante (même remarque sur  $a, b$ ):

$$\forall a, b, \exists x, \forall y, y \in x \Leftrightarrow (\mathcal{A}(a, b, x)).$$

Par l'axiome d'extensionnalité, il revient au même d'écrire  $\forall a, b, \exists!x, \forall y, y \in x \Leftrightarrow \mathcal{A}(a, b, x)$ , ce qui permet de reformuler les choses au moyen d'un opérateur  $T$  et de l'axiome

$$\forall a, b, \forall y, y \in T(a, b) \Leftrightarrow \mathcal{A}(a, b, T(a, b))$$

qui exprime que  $x = T(a, b)$  convient; l'unicité étant là encore garantie par l'axiome d'extensionnalité.

Hors des besoins de la preuve du théorème de complétude, un  $\exists$  non réductible à un  $\exists!$  n'est pas ainsi remplaçable par un opérateur. En effet la règle d'usage d'existence ne représente son objet que comme variable libre, qui diffère d'une constante par la qualification de ce qu'on construit avec, à savoir l'invariance des structures (tandis que la variable donnée par un axiome  $\exists!$  s'élimine par un symbole liant). De plus, une telle variable libre n'est disponible que tant que les autres variables libres restent libres (sauf avec l'axiome du choix, cf plus loin), contrairement aux constantes qui demeurent comme opérateurs ou opérations quand les autres variables sont liées.

Or non seulement une existence d'objet non unique introduit une indétermination locale (comme variable libre), mais un axiome d'existence ajoutant un choix indéterminé d'objets à l'univers, pourrait rendre globalement la théorie indéterminée (avec des énoncés clos indécidables, c'est-à-dire dont ni lui ni sa négation n'est démontrable). De fait, les axiomes ensemblistes présentent bien des  $\exists$  non réductibles à des  $\exists!$ , à commencer par l'axiome d'extensionnalité (un  $\forall$  à gauche d'un  $\Rightarrow$  est un  $\exists$  déguisé:  $\forall E, F, E \neq F \Rightarrow (\exists x, x \in E \not\leftrightarrow x \in F)$ ). Mais une étude plus approfondie de la théorie des ensembles, hors de portée ici, permettrait de voir l'essentiel de ces sources d'indécidabilité comme éliminables par d'autres axiomes.

## 2.2. $n$ -uplets, familles

Introduisons de nouveaux objets, ajoutables de même à toute théorie, indépendamment de la notion d'ensemble. En théorie des ensembles, ce seront les derniers qu'on puisse utilement regarder comme de sorte distincte, même s'ils sont aussi utilement reconstructibles au moyen des sortes précédentes. En fait, ce n'est pas une seule sorte, mais pour chaque entier  $n \geq 2$  (uniquement admis ici comme méta-objet) on aura une sorte différente d'objets appelés  $n$ -uplets. Un 2-uplet s'appelle un *couple*, un 3-uplet est un *triplet*, un 4-uplet est un *quadruplet*. . . (on a rarement besoin de plus).

Un  $n$ -uplet se conçoit comme une méta-fonction de domaine une liste  $\mathcal{A}_n$  de  $n$  méta-objets (fixés une fois pour toutes), à valeurs parmi les objets. Regardant ces méta-objets comme symboles de variables, un  $n$ -uplet est une interprétation de ce système de variables vues comme libres. Autrement dit, c'est l'expression condensée de  $n$  variables en une seule.

Comme évaluateur de  $n$ -uplet on n'a pas un opérateur binaire mais une liste de  $n$  opérateurs unaires, appelés *projections*. En effet,  $\mathcal{A}_n$  ne pouvant être parcouru par une variable de la théorie, chacun de ses  $n$  méta-éléments doit être pris séparément. Pour chaque  $k$  de 1 à  $n$ , l'évaluation de tout  $n$ -uplet sur le  $k$ -ième méta-élément de  $\mathcal{A}_n$ , constitue l'opérateur unaire  $\pi_k$  de  $k$ -ième projection, de domaine la sorte (ou classe) des  $n$ -uplets.

Comme définisseur, on a l'*opérateur de  $n$ -uplet*, d'arité  $n$ , non liant, noté simplement avec ses  $n$  arguments dans une parenthèse, séparés par des virgules.

Ces opérateurs sont reliés par l'axiome suivant: pour tous objets  $x_1, \dots, x_n$  et tout  $n$ -uplet  $y$ ,

$$y = (x_1, \dots, x_n) \Leftrightarrow (\pi_1(y) = x_1 \text{ et } \dots \text{ et } \pi_n(y) = x_n)$$

exprimant que  $(x_1, \dots, x_n)$  est l'unique  $n$ -uplet  $y$  tel que  $\pi_1(y) = x_1$  et  $\dots$  et  $\pi_n(y) = x_n$ . Cela se traduit en  $n + 1$  axiomes:

$$\begin{aligned} \pi_k((x_1, \dots, x_n)) &= x_k \quad \text{pour chaque } k \text{ de } 1 \text{ à } n \\ y &= (\pi_1(y), \dots, \pi_n(y)) \end{aligned}$$

Il en résulte par exemple dans le cas des couples que pour tous  $x, y, z, t$ ,

$$(x, y) = (z, t) \Leftrightarrow (x = z \text{ et } y = t).$$

Les couples suffisent à fabriquer des  $n$ -uplets pour tout  $n > 2$ . Par exemple on peut construire les triplets sous la forme  $(x, y, z) = (x, (y, z))$ .

Les structures  $n$ -aires  $T$  se traduisent en structures unaires  $T_1$  sur des classes de  $n$ -uplets, par

$$x = (x_1, \dots, x_n) \Rightarrow T_1(x) = T(x_1, \dots, x_n) = T(\pi_1(x), \dots, \pi_n(x)).$$

On construit un symbole liant  $n$  variables en appliquant un symbole liant une variable au cas d'un ensemble de  $n$ -uplets, et en donnant un  $n$ -uplet de variables à lier au lieu d'une seule. Par exemple, étant donné un ensemble  $C$  de couples,

$$(\forall (x, y) \in C, \mathcal{R}(x, y)) \Leftrightarrow (\forall z \in C, \mathcal{R}(\pi_1(z), \pi_2(z))) \Leftrightarrow (\forall x, \forall y, (x, y) \in C \Rightarrow \mathcal{R}(x, y)).$$

Dans notre théorie des ensembles, nous considérerons les  $n$ -uplets comme fonctions particulières, en figurant  $\mathcal{A}_n$  par un ensemble à  $n$  éléments chacun désigné par une constante. Ceci permet d'enrichir l'étude des  $n$ -uplets, et donc celle des structures  $n$ -aires, par les outils d'étude des fonctions.

Ainsi  $(x = y = z)$ , qui d'abord est l'abréviation de  $((x = y) \text{ et } (y = z))$ , signifie finalement que le triplet  $(x, y, z)$  est une fonction constante, de sorte qu'il en résulte aussi  $x = z$ .

#### Autres connecteurs logiques

Les outils précédents peuvent éclairer certains connecteurs  $n$ -aires: les chaînes de "et" et de "ou"

$$(B_1 \text{ et } \dots \text{ et } B_n) \Leftrightarrow ((B_1 \text{ et } B_2) \dots) \text{ et } B_n \Leftrightarrow (\forall x \in \mathcal{A}_n, (B_1, \dots, B_n)(x))$$

$$(B_1 \text{ ou } \dots \text{ ou } B_n) \Leftrightarrow ((B_1 \text{ ou } B_2) \dots) \text{ ou } B_n \Leftrightarrow (\exists x \in \mathcal{A}_n, (B_1, \dots, B_n)(x))$$

La double implication se généralise à des chaînes d'implications de longueur quelconque:

$$(B_0 \Rightarrow B_1 \Rightarrow \dots \Rightarrow B_n) \Leftrightarrow ((B_0 \Rightarrow B_1) \text{ et } \dots \text{ et } (B_{n-1} \Rightarrow B_n)) \Rightarrow (B_0 \Rightarrow B_n).$$

Remarquons que pour trois variables booléennes  $A, B, C$ ,

$$(A \Rightarrow B \Rightarrow C) \Leftrightarrow ((A \text{ ou } B) \Rightarrow (B \text{ et } C)) \Leftrightarrow ((\text{non } A \text{ et non } B) \text{ ou } (B \text{ et } C))$$

de sorte que  $(A \Rightarrow B \Rightarrow C)$  équivaut à  $C$  si  $B$  est vrai, et à  $(\text{non } A)$  sinon.

Soit le connecteur ternaire appelé *connecteur conditionnel*, noté  $(\rightarrow |)$ , défini par

$$(A \rightarrow B|C) \Leftrightarrow (\text{non } C \Rightarrow A \Rightarrow B) \Leftrightarrow ((A \text{ et } B) \text{ ou } (\text{non } A \text{ et } C)).$$

ce qu'on lit *Si A alors B sinon C*. De plus,  $(A \rightarrow B|C) \Leftrightarrow (\text{non } A \rightarrow C|B) \not\Leftrightarrow (A \rightarrow \text{non } B|\text{non } C)$ .

Tout connecteur  $K$  d'arité  $n + 1$  est traduisible au moyen de deux connecteurs d'arité  $n$  reliés par le connecteur conditionnel: sous-entendant  $n$  arguments booléens,

$$K(A) \Leftrightarrow (A \rightarrow K(\text{vrai})|K(\text{faux}))$$

Ainsi le connecteur conditionnel permet avec vrai et faux de redéfinir les autres, par exemple

$$(A \Rightarrow B) \Leftrightarrow (A \rightarrow B|\text{vrai})$$

$$(A \text{ ou } B) \Leftrightarrow (A \rightarrow \text{vrai}|B)$$

$$(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B \Rightarrow A) \Leftrightarrow (B \rightarrow A|\text{non } A).$$

#### Opérateur conditionnel

La notation ci-dessus du connecteur conditionnel sera réemployée pour l'*opérateur conditionnel*, à deux arguments ordinaires  $a, b$  et un argument booléen  $A$ , qui vaut  $a$  si  $A$  est vrai et  $b$  sinon:

$$\text{Pour tout } x, \quad x = (A \rightarrow a|b) \Leftrightarrow (A \rightarrow x = a|x = b)$$

$$\text{pour tout prédicat } \mathcal{R}, \quad \mathcal{R}(A \rightarrow a|b) \Leftrightarrow (A \rightarrow \mathcal{R}(a)|\mathcal{R}(b))$$

Il s'interprète comme valeur de  $(a, b)$  en  $A$  où  $\mathcal{A}_2$  est identifié à la sorte booléenne par le couple (vrai, faux). Chaque argument booléen d'un opérateur est éliminable en remplaçant l'opérateur par un couple d'opérateurs sans cet argument. Ainsi toute théorie est réductible au cas où aucune autre structure que l'opérateur conditionnel (lui-même non structurant) n'a d'argument booléen.

Il peut aussi servir à traduire des valeurs booléennes en objets, étant données deux constantes distinctes  $a$  et  $b$  choisies pour figurer le vrai et le faux; la traduction inverse s'écrit  $= a$ .

#### Ensembles finis, écriture extensive

On a aussi  $\{a, b\} = \text{Im}(a, b)$ , ce qui se généralise de la manière suivante.

Pour toute liste finie donnée d'objets, par exemple  $a, b, c$ , on note  $\{a, b, c\} = \text{Im}(a, b, c)$  l'ensemble dont  $a, b$  et  $c$  sont les seuls éléments. Ainsi pour tout  $x$  on a  $x \in \{a, b, c\} \Leftrightarrow (x = a \text{ ou } x = b \text{ ou } x = c)$ .

La notation d'un ensemble  $E$  par l'énumération  $\{a, b, \dots\}$  de ses éléments, s'appelle une *écriture extensive* de  $E$ . Tout ensemble  $E$  ainsi obtenu comme image d'un  $n$ -uplet pour quelque entier  $n$ , est un ensemble fini au sens naïf (ou méta). Son nombre d'éléments (le plus petit  $n$  tel que  $E$  soit l'image d'un  $n$ -uplet) est appelé le *cardinal* de  $E$  et noté  $\#E$ .

Ceci n'est qu'une introduction intuitive au moyen de méta-notions supposées acquises, où de petites valeurs de  $n$  suffisent. On introduira ultérieurement une autre définition, formelle, de la finitude en théorie des ensembles sans plus s'appuyer sur les méta-notions.

En fait, cette écriture extensive peut se reconstruire au moyen des seuls opérateurs de paire et d’union: par exemple

$$\{a, b, c, d, e\} = \{a, b\} \cup (\{c, d\} \cup \{e, e\}).$$

### Familles

On parlera de *famille* comme synonyme de fonction, mais vue comme généralisation des  $n$ -uplets, dans le sens où ces derniers ont été reconstruits comme fonctions. C’est une réinterprétation des fonctions où le domaine est regardé comme s’il était fait de méta-objets (symboles de variables), alors même qu’en toute rigueur ça n’est pas le cas. Notamment, par rapport aux  $n$ -uplets, cela permet d’une part de rendre  $n$  formellement variable; d’autre part, d’avoir un domaine infini. Comme exemple typique, une famille de domaine  $\mathbb{N}$  (ensemble des entiers) est appelée une *suite*.

Mais alors le formalisme spécifique des  $n$ -uplets est inapplicable, faute de pouvoir manipuler une infinité de symboles comme un seul; seul demeure valide celui des fonctions, de domaine un ensemble d’objets (on doit être en théorie des ensembles). Or, ces notions ensemblistes viseront à construire des notions d’autres théories, où différents objets ensemblistes joueront des rôles de sortes différentes. Alors, une fonction qui envoie une sorte d’objets sur une autre pourra être pensée comme une famille. Son domaine ressemblera à un ensemble de méta-objets (symboles) en n’y cherchant pas de structures élaborées, et en le traitant comme fixe et “en dehors” du système étudié.

Les outils formels des familles sont ceux des fonctions mais d’allure modifiée à l’image de ceux des  $n$ -uplets. Ainsi le définisseur par le terme  $t$  se note  $(t)_{i \in I}$  au lieu de  $(I \ni i \mapsto t)$ , et l’évaluateur d’une famille  $u$  en  $i$  se note  $u_i$  au lieu de  $u(i)$ . Le nom d’argument pour  $i$  est renommé *indice*; la famille  $u$  est dite *indexée par  $I$* . Ainsi  $u_i$  ressemble à un symbole méta-variable de variable. En effet, si  $u = (u_1, u_2)$ , on peut aussi bien interpréter la notation  $u_1$  comme premier symbole de variable, ou comme notation condensée de  $\pi_1(u)$  ou comme valeur  $u(1)$  de la fonction  $u$  en 1.

L’usage d’une famille sera souvent interchangeable avec celui de son ensemble image, en exerçant les quantificateurs sur celui-ci au lieu du domaine (en vertu de  $(\forall x \in \text{Im } u, \mathcal{R}(x)) \Leftrightarrow (\forall i \in I, \mathcal{R}(u_i))$ ).

En langage courant, la classe d’arrivée d’une famille peut se désigner en disant “famille de...”: une famille de trucs est une famille dont les éléments images sont des trucs ( $\forall i \in I, \text{truc}(x_i)$ ), tout comme on parle d’un “ensemble de...” pour spécifier la nature de ses éléments.

Tout opérateur  $n$ -aire désigne un opérateur unaire sur les  $n$ -uplets, combiné avec le définisseur de  $n$ -uplet. Le concept plus général de structure unaire sur les familles, combiné avec leur définisseur, n’est autre que celui de symbole liant sur un terme.

Ainsi l’écriture extensive se généralise en un nouveau symbole liant (à distinguer de celui de compréhension):  $\{f(x)|x \in E\} = \text{Im}(E \ni x \mapsto f(x))$ , ce qu’on peut encore compliquer en

$$\begin{aligned} \{f(x)|x \in E \text{ et } \mathcal{R}(x)\} &= \text{Im}(\{x \in E | \mathcal{R}(x)\} \ni x \mapsto f(x)) \\ (\forall y \in \{f(x)|x \in E \text{ et } \mathcal{R}(x)\}, \mathcal{A}(x)) &\Leftrightarrow (\forall x \in E, \mathcal{R}(x) \Rightarrow \mathcal{A}(f(y))) \end{aligned}$$

## 2.3. Autres opérateurs sur les ensembles

### L’algèbre des parties d’un ensemble

Voici d’abord les opérateurs binaires entre ensembles qui traduisent des connecteurs. Soient deux ensembles  $A$  et  $B$ , se traduisant en prédicats unaires, de valeurs  $\mathcal{A}$  et  $\mathcal{B}$  une fois appliqués à une même variable  $x$ :  $\mathcal{A} \Leftrightarrow x \in A$ ,  $\mathcal{B} \Leftrightarrow x \in B$ . Opérant entre eux un connecteur  $T$  et liant la variable sur le résultat, le prédicat obtenu se traduit en ensemble lorsque  $T$  donne faux sur le couple  $(\mathcal{A}, \mathcal{B}) = (\text{faux}, \text{faux})$ . En effet alors, sa classe est incluse dans  $A \cup B$ , et peut donc s’exprimer comme ensemble par compréhension dedans. Si  $A$  et  $B$  sont des parties d’un même ensemble  $E$ , le résultat le sera également.

$\mathcal{A}$ ou $\mathcal{B}$	$A \cup B$	union
$\mathcal{A}$ et $\mathcal{B}$	$A \cap B$	intersection
$\mathcal{A}$ et (non $\mathcal{B}$ )	$A \setminus B$	différence
$\mathcal{A} \nleftrightarrow \mathcal{B}$	$A \Delta B$	différence symétrique

En arité zéro on a seulement  $\emptyset$  pour faux.

En arité 1, le seul connecteur utile est le non, qui n’a pas la propriété requise. Alors on doit s’appuyer sur un choix d’ensemble  $E$  englobant  $A$ , comme domaine de  $x$ , et considérer au lieu de prédicats, des relations unaires sur  $E$  (ce en quoi les opérateurs ci-dessus étaient déjà interprétables). Alors (non  $\mathcal{A}$ ) se traduit en  $E \setminus A$ , aussi noté  $\mathbb{C}_E A$  et appelé *complémentaire de  $A$  dans  $E$* .

Entre deux parties  $A$  et  $B$  d’un ensemble  $E$  on a  $A \subset B \Leftrightarrow (\forall x \in E, x \in A \Rightarrow x \in B)$ .

De même, entre deux prédicats unaires  $\mathcal{A}$  et  $\mathcal{B}$  valides dans  $E$  on a

$$\{x \in E | \mathcal{A}(x)\} \subset \{x \in E | \mathcal{B}(x)\} \Leftrightarrow (\forall x \in E, \mathcal{A}(x) \Rightarrow \mathcal{B}(x))$$

*Union et intersection d'une famille d'ensembles*

L'opérateur binaire d'union entre 2 ensembles se généralise à toute arité, puis en opérateur unaire d'union de toute famille d'ensembles: la classe des  $x$  tels que  $(\exists i \in I, x \in E_i)$  est l'ensemble  $\bigcup_{i \in I} E_i$  défini par

$$\bigcup_{i \in I} E_i = \bigcup \text{Im}(I \ni i \mapsto E_i)$$

Inversement l'union d'un ensemble d'ensembles se redéfinit comme union de famille:  $\bigcup E = \bigcup_{F \in E} F$ . Cette généralisation traduit celle du connecteur (ou) en arité quelconque puis en  $\exists$ . Et tout comme (et) se généralise en  $(\forall)$ , on généralise l'intersection aux familles non vides ( $I \neq \emptyset$ ):

$$\text{Pour tout } x, \quad x \in \bigcap_{i \in I} E_i \Leftrightarrow \forall i \in I, x \in E_i$$

$$\forall j \in I, \quad \bigcap_{i \in I} E_i = \{x \in E_j | \forall i \in I, x \in E_i\}$$

De même on définit l'intersection d'un ensemble non vide d'ensembles par  $\bigcap E = \bigcap_{F \in E} F$ . Lors de l'étude des intersections d'ensembles (ou de familles) de parties d'un ensemble  $E$ , l'intersection de  $\emptyset$  est abusivement convenue égale à  $E$  (comme définie par compréhension dans  $E$ ).

On a les propriétés d'associativité et de distributivité:

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

$$A \cap B \cap C = (A \cap B) \cap C = A \cap (B \cap C) = \bigcap(A, B, C)$$

$$\begin{aligned} \left(\bigcup_{i \in I} A_i\right) \cap C &= \bigcup_{i \in I} (A_i \cap C) & \left(\bigcap_{i \in I} A_i\right) \cup C &= \bigcap_{i \in I} (A_i \cup C) \\ (A \cup B) \cap C &= (A \cap C) \cup (B \cap C) & (A \cap B) \cup C &= (A \cup C) \cap (B \cup C) \end{aligned}$$

*Somme ou union disjointe*

**Notation.** On appelle graphe tout ensemble de couples. Pour tout graphe  $R$ , on notera

$$\text{Dom } R = \{x | (x, y) \in R\}$$

$$\text{Im } R = \{y | (x, y) \in R\}$$

Le prédicat binaire  $x, y \mapsto ((x, y) \in R)$ , se traduit par curryfication en opérateur unaire  $\vec{R}$  vers les prédicats unaires et plus précisément les ensembles: pour tous  $x, y$ ,

$$\begin{aligned} \vec{R}(x) &= \{y | (x', y) \in R \text{ et } x' = x\} \\ y \in \vec{R}(x) &\Leftrightarrow (x, y) \in R \\ \vec{R}(x) \neq \emptyset &\Leftrightarrow x \in \text{Dom } R \end{aligned}$$

**Lemme et définition.** Pour toute famille d'ensembles  $(E_i)_{i \in I}$ , on appelle somme ou union disjointe des  $E_i$ , et on note  $\coprod_{i \in I} E_i$ , l'unique graphe  $S$  satisfaisant les conditions équivalentes:

- 1)  $S = \bigcup_{i \in I} \{(i, x) | x \in E_i\}$
- 2) Pour tous  $i, x, (i, x) \in S \Leftrightarrow (i \in I \text{ et } x \in E_i)$
- 3)  $\text{Dom } S \subset I$  et  $\forall i \in I, E_i = \vec{S}(i)$
- 4) Pour tout prédicat binaire  $\mathcal{R}$ ,  $(\forall (i, x) \in S, \mathcal{R}(i, x)) \Leftrightarrow (\forall i \in I, \forall x \in E_i, \mathcal{R}(i, x))$ .

Il en résulte  $\text{Im } S = \bigcup_{i \in I} E_i$ .

Posant  $\mathcal{A}_n = \{1, \dots, n\}$ , on définit la somme de 2 ensembles  $E \sqcup F = \coprod(E, F)$ , et celle de  $n$  ensembles

$$E_1 \sqcup \dots \sqcup E_n = \coprod(E_1, \dots, E_n) = \coprod_{i \in \mathcal{A}_n} E_i$$

Lorsque tous les  $E_i$  sont finis, leur somme l'est aussi et  $\#(E_1 \sqcup \dots \sqcup E_n) = \#E_1 + \dots + \#E_n$ .

*Produit fini*

On appelle produit (ou produit cartésien) de deux ensembles  $E$  et  $F$ , l'ensemble des  $(x, y)$  où  $x \in E$  et  $y \in F$ :

$$E \times F = \prod_{x \in E} F$$

On a les propriétés:

$$\begin{aligned} E \times \emptyset &= \emptyset = \emptyset \times E \\ (E \subset E' \text{ et } F \subset F') &\Rightarrow E \times F \subset E' \times F' \\ (\forall i \in I, E_i \subset E'_i) &\Rightarrow \prod_{i \in I} E_i \subset \prod_{i \in I} E'_i. \end{aligned}$$

Plus généralement, étant donnés  $n$  ensembles  $E_1, \dots, E_n$ , on définit leur produit  $E_1 \times \dots \times E_n$  comme étant l'ensemble des  $n$ -uplets  $(x_1, \dots, x_n)$  où  $x_1 \in E_1$  et  $\dots$  et  $x_n \in E_n$ . Il se justifie par le principe de génération des ensembles:

$$(\forall (x_1, \dots, x_n) \in E_1 \times \dots \times E_n, \mathcal{R}(x_1, \dots, x_n)) \Leftrightarrow (\forall x_1 \in E_1, \dots, \forall x_n \in E_n, \mathcal{R}(x_1, \dots, x_n)).$$

*Retour sur les opérations et relations*

Une opération  $f$  d'arguments de domaines  $E$  et  $F$  est formalisable comme fonction de domaine  $E \times F$ , avec pour définisseur  $(E \times F) \ni (x, y) \mapsto \dots$ , et pour évaluateur  $f(x, y) = f(z)$  où  $z = (x, y)$ .

Une relation  $n$ -aire se réduit de même à une relation unaire sur un produit et donc à un ensemble de  $n$ -uplets: pour une relation  $\mathcal{R}$  entre  $E$  et  $F$ , c'est un ensemble  $R \subset E \times F$ , évalué par  $((x, y) \in R)$ , défini par  $\{(x, y) \in E \times F \mid \mathcal{R}(x, y)\}$ . Appelé graphe de la relation, il sera souvent confondu avec elle en pratique dans de nombreux contextes, les domaines des arguments étant déjà fixés par ailleurs.

Pour tout graphe  $R$ , pour tous ensembles  $E$  et  $F$ ,

$$R \subset E \times F \Leftrightarrow (\text{Dom } R \subset E \text{ et } \text{Im } R \subset F)$$

$$\text{Dom } R \subset E \Leftrightarrow R = \prod_{x \in E} \vec{R}(x)$$

$$\text{Im } R \subset F \Rightarrow \forall x \in E, \vec{R}(x) = \{y \in F \mid (x, y) \in R\}$$

Si  $\text{Dom } R \subset E$  alors  $R \subset S \Leftrightarrow \forall x \in E, \vec{R}(x) \subset \vec{S}(x)$ .

Mais on peut au besoin compléter la donnée ainsi. Une relation unaire sur  $E$  peut s'écrire  $(E, G)$  où  $G \subset E$ . Une relation entre deux ensembles  $E$  et  $F$ , de graphe  $G \subset E \times F$ , peut se définir soit comme triplet  $(E, F, G)$ , soit comme couple  $(E \times F, G)$ . La différence est que dans le deuxième cas la donnée de  $F$  est perdue si  $E = \emptyset$ , et de même celle de  $E$  si  $F = \emptyset$ .

*Graphe d'une fonction*

**Définitions.** Un graphe  $G$  sera dit fonctionnel si  $\forall (x, y) \in G, \forall (x', y') \in G, x = x' \Rightarrow y = y'$ , autrement dit  $\forall x \in \text{Dom } G, ! : \vec{G}(x)$ . Pour toute fonction  $f$  de domaine  $E$ , on appelle graphe de  $f$  le graphe fonctionnel

$$\text{Gr } f = \{(x, f(x)) \mid x \in E\} = \prod_{x \in E} \{f(x)\}.$$

On a  $\text{Dom } f = \text{Dom } \text{Gr } f$ ,  $\text{Im } f = \text{Im } \text{Gr } f$ , et pour tout ensemble  $F$ ,

$$\text{Im } f \subset F \Leftrightarrow \text{Gr } f \subset E \times F \Leftrightarrow \text{Gr } f = \{(x, y) \in E \times F \mid y = f(x)\}$$

Pour toute fonction  $f$  de  $E$  dans  $F$  et tout  $R \subset E \times F$  on a

$$\text{Gr}(f) \subset R \Leftrightarrow \forall x \in E, (x, f(x)) \in R$$

$$\text{Gr}(f) = R \Leftrightarrow \forall x \in E, \{f(x)\} = \vec{R}(x).$$

Le procédé évoqué en 2.1. permettrait de construire une théorie des ensembles où les fonctions seraient remplacées par les graphes fonctionnels, avec des règles de qualification des énoncés ensemblistes, et de reconnaissance des fonctions définies par des termes.

Au lieu de cela, introduisons un nouvel opérateur  $\epsilon$ , valide sur les singletons ( $\text{Ens}(E)$  et  $\exists ! : E$ ), pour en extraire l'élément. Inexprimable comme terme par les outils précédents, il se définit par les axiomes équivalents:  $(\forall x, \epsilon\{x\} = x)$ , et  $(\forall E, (\text{Ens}(E) \text{ et } \exists ! : E) \Rightarrow \epsilon E \in E)$ .

Alors tout graphe fonctionnel  $G$  est celui de la fonction  $\Psi(G) = ((\text{Dom } G) \ni x \mapsto \epsilon \vec{G}(x))$ .

## 2.4. Ensembles des parties, produit et puissance

Introduisons trois nouveaux opérateurs désignant comme ensembles certaines classes. Chaque tel opérateur  $T$  est donc muni d'un axiome spécifiant la classe  $\mathcal{R}$  équivalente à l'ensemble désigné: sous-entendant les arguments,  $\forall x, x \in T \Leftrightarrow \mathcal{R}(x)$ .

Cela ressemble aux usages du principe de génération des ensembles, mais ce n'en sera pas, les quantificateurs sur ces classes n'étant pas traduisibles en énoncés ensemblistes.

L'approche traditionnelle des théories axiomatiques se contente de les formaliser comme axiomes  $\exists K, \forall x, x \in K \Leftrightarrow \mathcal{R}(x)$ , laissant la désignation de ces ensembles n'être qu'un emploi implicite de leur caractérisation ( $\forall x, x \in K \Leftrightarrow \mathcal{R}(x)$ ) dans les énoncés, suivant la procédure évoquée au 2.1.

Mais ce n'est là qu'un omni-énoncé, a priori intraduisible en énoncé ensembliste: l'implication s'écrit ( $\forall x \in K, \mathcal{R}(x)$ ), mais la réciproque laisse un  $\forall$  ouvert irréductible,  $\forall x, \mathcal{R}(x) \Rightarrow x \in K$ . Faute d'énoncé ensembliste équivalent, ces axiomes d'existence sont inutilisables dans notre théorie des ensembles. La présentation comme opérateurs supplémentaires munis d'axiomes est nécessaire.

**Ensemble des parties.** Pour tout ensemble  $E$ , on note  $\mathcal{P}(E)$  l'ensemble de toutes les parties de  $E$ : pour tout  $F$ ,

$$F \in \mathcal{P}(E) \Leftrightarrow (\text{Ens}(F) \text{ et } F \subset E)$$

**Ensemble puissance.** Pour tous ensembles  $E$  et  $F$ , on note  $F^E$  l'ensemble des fonctions de  $E$  dans  $F$ : pour tout  $f$ ,

$$f \in F^E \Leftrightarrow (\text{App}(f) \text{ et } \text{Dom } f = E \text{ et } \text{Im } f \subset F)$$

**Produit d'une famille d'ensembles.** L'opérateur unaire de produit d'une famille d'ensembles, généralisation du produit précédent, se présente comme symbole liant:

$$\forall x, x \in \prod_{i \in I} E_i \Leftrightarrow (\text{App}(x) \text{ et } \text{Dom } x = I \text{ et } \forall i \in I, x_i \in E_i).$$

Pour chaque symbole liant, l'usage d'un  $\mathcal{P}(\dots)$  comme domaine sera abrégé en remplaçant  $\in$  par  $\subset$ . Ainsi ( $\forall A \subset E, \dots$ ) signifie ( $\forall A \in \mathcal{P}(E), \dots$ ).

Ces trois opérateurs sont "équivalents", en ce sens qu'ils sont définissables les uns par les autres:

$$\begin{aligned} \mathcal{P}(E) &= \{\{x \in E \mid f(x) = 1\} \mid f \in \{1, 2\}^E\} \\ F^E &= \prod_{x \in E} F = \{\Psi(R) \mid R \subset E \times F \text{ et } \forall x \in E, \exists ! : \vec{R}(x)\} \\ \prod_{i \in I} E_i &= \{x \in (\bigcup_{i \in I} E_i)^I \mid \forall i \in I, x_i \in E_i\} = \{\Psi(R) \mid R \subset \prod_{i \in I} E_i \text{ et } \forall x \in E, \exists ! : \vec{R}(x)\} \end{aligned}$$

Même certains cas sont exprimables au moyen des outils précédents:

$$\begin{aligned} (\exists i \in I, E_i = \emptyset) &\Rightarrow \prod_{i \in I} E_i = \emptyset \\ (\forall i \in I, \exists ! : E_i) &\Rightarrow \prod_{i \in I} E_i = \{(\epsilon E_i)_{i \in I}\} \\ F^\emptyset &= \{\emptyset\} \\ F^{\{a\}} &= \{\{a\} \ni x \mapsto y \mid y \in F\}, \quad \mathcal{P}(\{a\}) = \{\emptyset, \{a\}\} \\ F^{E \cup E'} &= \{(E \cup E') \ni x \mapsto (x \in E \rightarrow f(x) \mid g(x)) \mid (f, g) \in F^E \times F^{E'}\} \end{aligned}$$

et de même on peut formuler  $\prod_{i \in I \cup J} E_i$ .

Pour tout  $i \in I$  on appelle *i-ième projection*, la fonction  $\pi_i$  de  $\prod_{i \in I} E_i$  dans  $E_i$  qui évalue toute famille  $x$  en  $i$ :  $\pi_i(x) = x_i$ . C'est l'évaluateur de fonction vu comme curryfié dans l'ordre inhabituel.

Si  $F \subset F'$  alors  $F^E \subset F'^E$ ,  $\mathcal{P}(F) \subset \mathcal{P}(F')$ , et

$$(\forall i \in I, E_i \subset E'_i) \Rightarrow \prod_{i \in I} E_i \subset \prod_{i \in I} E'_i$$

Pour une théorie des ensembles capable de fonder les mathématiques (définir les concepts tant des mathématiques courantes que du cycle fondateur principal), ces opérateurs sont indispensables,

déjà pour pouvoir définir la finitude (sinon, seuls seraient connus comme finis les ensembles de cardinal limité par un nombre plus ou moins explicite). Puis il restera à poser l'axiome "Il existe un ensemble infini" (d'ailleurs formulable par un autre critère d'ensemble clairement infini). C'est en effet sur les ensembles infinis que  $\mathcal{P}$  prendra toute sa force (les produits finis étant déjà donnés avant): construction de  $\mathbb{N}$  et  $\mathcal{P}(\mathbb{N})$  (un quantificateur sur  $\mathcal{P}(\mathbb{N})$  est déjà nécessaire pour définir  $\mathbb{N}$ ) et par là de  $\mathbb{R}$ ; principe de définition des suites par récurrence.

Certes, l'utilité de ces montages finit par s'essouffler: après quelques  $\forall X \subset \mathbb{R}$  ou  $\forall X \subset \mathcal{P}(\mathbb{N})$  (pour des buts souvent réalisables autrement avec un peu plus de peine), ce qui vient ensuite ( $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$ ) et au-delà n'a plus d'utilité pratique. On pourrait alors se limiter à ces premiers cas, sauf qu'une telle distinction compliquerait inutilement un exposé déjà assez difficile des fondements des mathématiques. Pour partir des fondements les plus simples possibles, comme d'ailleurs suivant la tradition ZF, nous accepterons ces opérateurs dans leur intégralité.

Ils apportent une forte contrainte sur l'univers (on pense qu'ils n'entraînent pas de contradiction, bien qu'il soit impossible de le démontrer). Mais pour chaque  $E$ , cette exigence que  $\mathcal{P}(E)$  contienne toutes les parties de  $E$ , reste relative à l'étendue de la classe des parties de  $E$  présentes dans notre univers, indéterminée par ailleurs. Cela n'exprime finalement qu'une relation entre  $\mathcal{P}(E)$  et l'univers.

On peut toujours oublier cette dépendance de  $\mathcal{P}(E)$  vis-à-vis de l'univers, en imaginant celui-ci suffisamment grand pour contenir "vraiment" toutes les parties de  $E$ , et par là, le "vrai"  $\mathcal{P}(E)$ . Mais rien ne peut exprimer d'interdiction qu'il existe ailleurs, dans un autre univers plus grand, d'autres parties de  $E$  hors de notre  $\mathcal{P}(E)$ . Cet autre univers peut aussi avoir un opérateur  $\mathcal{P}$ , mais son interprétation de  $\mathcal{P}(E)$  pourra différer de la nôtre pour le même  $E$ . Ces jeux de Grandes Illusions s'avèrent le paradoxe central des fondements des mathématiques, source principale des indécidabilités.

## 2.5. Injections, surjections, bijections canoniques

### Propriétés des graphes

**Proposition.** Soit  $R$  une relation entre deux ensembles  $E$  et  $F$ . Il y a équivalence entre

1.  $\forall x \in E, \exists ! y \in F, R(x, y)$
2.  $\exists f \in F^E, \text{Gr}(f) = \text{Gr}(R)$
3.  $\exists ! f \in F^E, \text{Gr}(f) = \text{Gr}(R)$
4.  $\exists ! f \in F^E, \text{Gr}(f) \subset \text{Gr}(R)$ .

De là, pour toutes fonctions  $f, g$  on a  $(\text{Dom } f = \text{Dom } g \text{ et } \text{Gr}(f) \subset \text{Gr}(g)) \Leftrightarrow f = g$ .

*Preuves:* De manière évidente d'après les résultats précédents, 1.  $\Leftrightarrow$  2.  $\Leftrightarrow$  3.  $\Rightarrow$  4.

Enfin pour 4.  $\Rightarrow$  2. :  $\text{Gr}(f) \subset \text{Gr}(R) \Rightarrow \forall (x, y) \in \text{Gr}(R), \text{Gr}(x' \mapsto (x = x' \rightarrow y | f(x'))) \subset \text{Gr}(R)$ , donc  $f = (x' \mapsto (x = x' \rightarrow y, f(x')))$ , donc  $y = f(x)$ . Finalement  $\text{Gr}(f) = \text{Gr}(R)$ .  $\square$

### Injections, surjections, bijections

Pour tout  $f \in F^E$  et tout  $y$  on notera  $f^\bullet(y) = \{x \in E | f(x) = y\}$ , et  $f_F^\bullet = (F \ni z \mapsto f^\bullet(z))$ .

**Lemme et définition.** Une fonction  $f$  est dite *injective* (ou : une *injection*) si elle satisfait les conditions équivalentes où  $E = \text{Dom } f$  et  $\text{Im } f \subset F$ :

$$\begin{aligned} \forall x, x' \in E, x \neq x' &\Rightarrow f(x) \neq f(x') \\ \forall x, x' \in E, f(x) = f(x') &\Rightarrow x = x' \\ \forall y \in F, ! : f^\bullet(y) & \end{aligned}$$

La première équivalence est évidente; la deuxième se vérifie ainsi (par  $f(x) \in F$ ):

$$\begin{aligned} \forall y \in F, ! x \in E, f(x) = y &\Leftrightarrow \forall y \in F, \forall x, x' \in E, (f(x) = y \text{ et } f(x') = y) \Rightarrow x = x' \\ &\Leftrightarrow \forall x, x' \in E, \forall y \in F, f(x) = y \Rightarrow (f(x') = y \Rightarrow x = x') \\ &\Leftrightarrow \forall x, x' \in E, f(x) = f(x') \Rightarrow x = x' \end{aligned}$$

**Définition.** On dit qu'une fonction de  $E$  dans  $F$  est *surjective* (ou une *surjection*) lorsque  $\text{Im } f = F$ .

Ce n'est donc pas une propriété de  $f$  seul mais qui dépend d'un ensemble d'arrivée  $F$  donné. On dit aussi une surjection de  $E$  sur  $F$ .

**Définition.** Une fonction bijective (ou bijection) de  $E$  sur  $F$  est une fonction  $f$  injective et surjective de  $E$  sur  $F$ , autrement dit  $\forall y \in F, \exists ! : f^\bullet(y)$ .

Une bijection d'un ensemble sur lui-même s'appelle une *permutation* (on dit aussi une *transformation* pour un espace géométrique).

**Définition.** L'inverse de toute injection  $f$  est  $f^{-1} = (\text{Im } f \ni y \mapsto \epsilon f^\bullet(y))$  (bijective sur  $\text{Dom } f$ ).

*Identité, composition et restriction*

Pour tout ensemble  $E$  on appelle *identité sur  $E$*  la fonction  $\text{Id}_E = (E \ni x \mapsto x) \in E^E$  aussi appelée *l'injection canonique* de  $E$  dans tout ensemble englobant  $E$ .

On définit les compositions de fonctions  $f, g, h$  par

$$\text{Im } f \subset \text{Dom } g \Rightarrow g \circ f = (\text{Dom } f \ni x \mapsto g(f(x)))$$

$$\text{Im } f \subset \text{Dom } g \text{ et } \text{Im } g \subset \text{Dom } h \Rightarrow h \circ g \circ f = (h \circ g) \circ f = h \circ (g \circ f) = (\text{Dom } f \ni x \mapsto h(g(f(x)))).$$

Pour toute fonction  $f \in F^E$  et  $A \subset E$ , on appelle *restriction de  $f$  à  $A$*  la fonction

$$f|_A = (A \ni x \mapsto f(x)) = f \circ \text{Id}_A \in F^A.$$

*Bijections canoniques: généralités*

On appelle *bijection canonique* entre deux ensembles  $E$  et  $F$ , une bijection obtenue par restriction à  $E$  d'un opérateur unaire invariant (de définition souvent simple). L'existence d'une telle bijection sera notée  $E \simeq F$ . Ce méta-énoncé  $E \simeq F$  ne fait donc que sous-entendre une formule de définition d'une bijection qu'il faut réexpliquer pour obtenir un travail effectif de théorie des ensembles.

Si  $E \simeq F$  et  $F \simeq G$  alors  $E \simeq G$  par composition des expressions des opérateurs unaires.

Les bijections canoniques ressembleront souvent à des identités remarquables sur les opérations entre entiers, car sur les ensembles finis elles donnent l'égalité des cardinaux.

Des bijections canoniques engendrent d'autres entre des ensembles construits à partir des précédents, par exemple  $(E \simeq E' \text{ et } F \simeq F') \Rightarrow E \times F \simeq E' \times F'$  d'où, par les graphes,  $F^E \simeq F'^{E'}$ .

Une bijection canonique sera dite *bicanonique* si son inverse est aussi canonique. Cela n'est pas possible lorsque l'opérateur unaire invariant utilisé n'est pas injectif. Par exemple  $E \times \{x\} \simeq E^{\{x\}}$  n'est bicanonique que si  $E \neq \emptyset$ , tandis que  $\{x\}^E \simeq \{x\}$  et  $E \times \{x\} \simeq E$  ne le sont généralement pas. Seulement, notant comme des chiffres des constantes invariantes comme  $0 = \emptyset$  et  $1 = \{\emptyset\}$ , on a  $E \simeq E \times \{0\}$ ,  $E \simeq E^{\{0\}}$  et  $\{0, 1\}^E \simeq \mathcal{P}(E)$  bicanoniques.

*Somme de fonctions ou décurryfication*

La somme des familles d'ensembles définit des bijections canoniques, d'inverse  $R \mapsto \vec{R}$  non canonique par indétermination de  $\text{Dom } \vec{R}$  (sauf à admettre  $E$  comme paramètre):

$$\begin{aligned} (\mathcal{P}(F))^E &\simeq \mathcal{P}(E \times F) \quad (\simeq \{0, 1\}^{E \times F}) \\ \prod_{x \in E} \mathcal{P}(F_x) &\simeq \mathcal{P}\left(\prod_{x \in E} F_x\right) \\ \text{Dom } R \subset E &\Rightarrow \prod_{x \in E} \mathcal{P}(\vec{R}(x)) \simeq \mathcal{P}(R) \end{aligned}$$

On définit la somme de toute famille  $(f_i)_{i \in I}$  de fonctions, notant  $E_i = \text{Dom } f_i$  et  $S = \coprod_{i \in I} E_i$  :

$$\begin{aligned} (f_i)_{i \in I} &\mapsto \prod_{i \in I} f_i = (S \ni (i, x) \mapsto f_i(x)) = f \\ \forall i \in I, f_i &= f \circ j_i \quad \text{où } j_i = (E_i \ni x \mapsto (i, x)) \in S^{E_i} \end{aligned}$$

Cela définit des bijections canoniques (bicanoniques si  $\forall i \in I, E_i \neq \emptyset$ , sinon en fixant  $I$ ):

$$\begin{aligned} (F^E)^I &\simeq F^{I \times E} \\ \prod_{i \in I} F^{E_i} &\simeq F^S \quad \text{où } S = \prod_{i \in I} E_i \\ \prod_{i \in I} \prod_{x \in E_i} F_{(i,x)} &\simeq \prod_{c \in S} F_c \\ (E \times F) \times G &\simeq E \times F \times G \end{aligned}$$

### Transposition

Une transposition sur un ensemble est une permutation de cet ensemble qui échange deux éléments et laisse fixe les autres. Sur toute paire il existe une unique transposition.

L'emploi de la transposition sur le domaine des couples définit l'opérateur unaire  $\sigma$  sur la classe des couples:  $\sigma(x, y) = (y, x)$ . Pour tout couple  $z$  on a  $\sigma(\sigma(z)) = z$ .

Il en résulte les bijections canoniques:  $E \times F \simeq F \times E$ , et  $G^{E \times F} \simeq G^{F \times E}$ . Ainsi, pour toute opération  $f \in G^{E \times F}$  on appelle *transposée de  $f$*  l'opération  ${}^t f = ((x, y) \ni F \times E \mapsto f(y, x)) \in G^{F \times E}$ .

De même,  $\mathcal{P}(E \times F) \simeq \mathcal{P}(F \times E)$  par  ${}^t R = \{(y, x) | (x, y) \in R\}$ .

### Produit de fonctions ou currying

Les graphes peuvent se currier en sens contraire:  $\overleftarrow{R} = \overrightarrow{{}^t R}$ . Ainsi,

$$\begin{aligned} (\mathcal{P}(F))^E &\simeq \mathcal{P}(E \times F) \simeq (\mathcal{P}(E))^F \\ \overrightarrow{R} \mapsto \overleftarrow{R} &= (F \ni y \mapsto \{x \in E | y \in \overrightarrow{R}(x)\}) \\ x \in \overleftarrow{R}(y) &\Leftrightarrow y \in \overrightarrow{R}(x). \end{aligned}$$

Pour toute famille  $(f_i)_{i \in I}$  de fonctions de même domaine  $E$ , on définit son produit par

$$\begin{aligned} \prod_{i \in I} f_i &= (E \ni x \mapsto (f_i(x))_{i \in I}) \\ h &= \prod_{i \in I} f_i \Leftrightarrow \text{Dom } h = E \text{ et } \forall i \in I, f_i = \pi_i \circ h \\ (F^E)^I &\simeq (F^I)^E \\ \prod_{i \in I} (F_i^E) &\simeq \left( \prod_{i \in I} F_i \right)^E \\ \text{Dom } f = \text{Dom } g = E &\Rightarrow f \times g = (E \ni x \mapsto (f(x), g(x))) \\ I^E \times F^E &\simeq (I \times F)^E \\ \prod_{\phi \in I^E} \prod_{x \in E} F_{\phi(x)} &\simeq \left( \prod_{i \in I} F_i \right)^E. \end{aligned}$$

## 2.6. Autres propriétés des fonctions

### Image directe, image réciproque

On appelle *image réciproque* d'un ensemble  $B$  par une fonction  $f$  l'ensemble

$$f^*(B) = \{x \in \text{Dom } f | f(x) \in B\}.$$

Fixant un ensemble d'arrivée  $F$  de  $f$ , on verra  $f^*$  comme fonction de domaine  $\mathcal{P}(F)$ .

On a  $f^\bullet(y) = f^*(\{y\})$ .

Si  $A \subset B \subset F$  alors  $f^*(A) \subset f^*(B)$  et  $f^*(\mathbb{C}_F A) = \mathbb{C}_E f^*(A)$ . Pour toute famille d'ensembles  $(A_i)_{i \in I}$ ,

$$\begin{aligned} f^*\left(\bigcup_{i \in I} A_i\right) &= \bigcup_{i \in I} f^*(A_i) \\ f^*\left(\bigcap_{i \in I} A_i\right) &= \bigcap_{i \in I} f^*(A_i). \end{aligned}$$

Soit maintenant un ensemble  $A \subset E$ . On appelle *image directe de  $A$  par  $f$*  et on note  $f[A]$  l'ensemble

$$f[A] = \text{Im}(f|_A) = \{f(x) | x \in A\} = \{y \in F | \exists x \in A, y = f(x)\} \subset \text{Im } f \subset F.$$

(Cette notation  $f[A]$ , évitant l'ambiguïté de la notation classique  $f(A)$ , est tirée du Wikipedia anglophone.) C'est une surjection  $f|_{\mathcal{P}(E)}$  de  $\mathcal{P}(E)$  sur  $\mathcal{P}(\text{Im } f)$  car  $\forall B \subset \text{Im } f, f[f^*(B)] = B$ .

Pour tous  $A \subset B \subset E$  on a  $f[A] \subset f[B]$ . Pour toute famille  $(A_i)_{i \in I}$  de parties de  $E$ ,

$$\begin{aligned} f\left[\bigcup_{i \in I} A_i\right] &= \bigcup_{i \in I} f[A_i] \\ f\left[\bigcap_{i \in I} A_i\right] &\subset \bigcap_{i \in I} f[A_i] \quad \text{avec égalité si } f \text{ injective et } I \neq \emptyset. \end{aligned}$$

**Proposition.** Soient deux fonctions  $f \in F^E$  et  $g \in G^F$ . On a:

1. Si  $f$  et  $g$  sont injectives alors  $g \circ f$  est injective.
2. Si  $g \circ f$  est injective alors  $f$  est injective.
3.  $\text{Im}(g \circ f) = g[\text{Im } f] \subset \text{Im } g$
4. Si  $f$  est surjective (i.e.  $\text{Im } f = F$ ) alors  $\text{Im}(g \circ f) = \text{Im } g$ .
5. Si  $f$  et  $g$  sont surjectives alors  $g \circ f$  est surjective (i.e.  $\text{Im}(g \circ f) = G$ ).
6. Si  $g \circ f$  est surjective alors  $g$  est surjective.
7. Si  $f$  et  $g$  sont bijectives alors  $g \circ f$  est bijective.

Preuves:

1. Si  $f$  et  $g$  sont injectives,  $\forall x, y \in E, g(f(x)) = g(f(y)) \Rightarrow f(x) = f(y) \Rightarrow x = y$ .
  2.  $\forall x, y \in E, f(x) = f(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow x = y$ .
  3.  $\forall z \in G, z \in \text{Im}(g \circ f) \Leftrightarrow (\exists x \in E, g(f(x)) = z) \Leftrightarrow (\exists y \in \text{Im } f, g(y) = z) \Leftrightarrow z \in g[\text{Im } f]$ .
- Puis, 3.  $\Rightarrow$  4.  $\Rightarrow$  5. puis 3.  $\Rightarrow$  6. puis (1. et 5.)  $\Rightarrow$  7.

*Propriétés de la fonction inverse*

Soient  $E$  et  $F$  deux ensembles,  $f \in F^E$  et  $g \in E^F$ . Alors on a équivalence entre

- 1)  $g \circ f = \text{Id}_E$
- 2)  $\forall x \in E, \forall y \in F, f(x) = y \Rightarrow g(y) = x$
- 3)  $\text{Gr } f \subset {}^t\text{Gr } g$ .
- 4)  $\forall y \in F, f^\bullet(y) \subset \{g(y)\}$
- 5)  $\forall x \in E, f(x) \in g^\bullet(x)$
- 6)  $f$  est injective et  $g|_{\text{Im } f} = f^{-1}$

De même en combinant ces énoncés avec ceux où on échange  $f$  et  $g$ : on a équivalence entre

- 1)  $g \circ f = \text{Id}_E$  et  $f \circ g = \text{Id}_F$ .
- 2)  $\forall x \in E, \forall y \in F, f(x) = y \Leftrightarrow g(y) = x$
- 3)  $\text{Gr } g = {}^t\text{Gr } f$ .
- 4)  $\forall y \in F, f^\bullet(y) = \{g(y)\}$
- 5)  $\forall x \in E, \{f(x)\} = g^\bullet(x)$
- 6)  $f$  est bijective et  $g = f^{-1}$

On a  $(f^{-1})^{-1} = f$ . D'après les propriétés des graphes de fonctions,

$$\forall f \in F^E, \quad f \text{ bijective} \Leftrightarrow (\exists g \in E^F, \text{Gr } g = {}^t\text{Gr } f) \Leftrightarrow (\exists! g \in E^F, \text{Gr } g \subset {}^t\text{Gr } f).$$

**Proposition.** Soient deux ensembles  $E$  et  $F$  et trois fonctions  $f, h \in F^E, g \in E^F$  telles que  $g \circ f = \text{Id}_E$  et  $h \circ g = \text{Id}_F$ . Alors  $f = h$ , de sorte que  $g = f^{-1}$ .

Preuve:  $\forall x \in E, f(x) = h(g(f(x))) = h(x)$ . Autre méthode:  $\text{Gr } f \subset {}^t\text{Gr } g \subset \text{Gr } h$ .

**Proposition.** Soient deux fonctions  $f \in F^E$  et  $g \in G^F$  bijectives. Alors  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

On peut écrire la preuve

$$\forall x \in E, \forall y \in G, g \circ f(x) = y \Leftrightarrow f(x) = g^{-1}(y) \Leftrightarrow x = f^{-1} \circ g^{-1}(y)$$

ou encore  $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ \text{Id}_F \circ g^{-1} = \text{Id}_G$ , et de même  $(f^{-1} \circ g^{-1}) \circ (g \circ f) = \text{Id}_E$ .

*Propriétés de la composition*

**Théorème.** Soient trois ensembles  $E, F, G$ , soit  $f \in F^E$ , et soit  $\phi = (G^F \ni g \mapsto g \circ f)$  la fonction de composition à droite par  $f$ , arrivant dans  $G^E$ . On a alors:

- 1) Si  $f$  est surjective alors  $\phi$  est injective
- 2) Si  $f$  est injective et  $G \neq \emptyset$  alors  $\phi$  est surjective
- 3) Si  $\phi$  est surjective et  $\exists 2 : G$  alors  $f$  est injective.
- 4) Si  $\phi$  est injective et  $\exists 2 : G$  alors  $f$  est surjective.

Preuves:

- 1)  $\forall g, h \in G^F, \phi(g) = \phi(h) \Leftrightarrow (\forall x \in E, g(f(x)) = h(f(x))) \Leftrightarrow \forall y \in F, g(y) = h(y) \Leftrightarrow g = h$ .
- 2) Soient  $h \in G^E$  et  $z \in G$ . Alors,  $f$  étant injective,  $\phi(F \ni y \mapsto (y \in \text{Im } f \rightarrow h \circ f^{-1}(y)|z)) = h$ .
- 3) Soient  $z \neq z' \in G$ . Alors  $\forall x \in E, \exists g \in G^F, \forall y \in E, g(f(y)) = (y = x \rightarrow z|z')$ , donc  $f(y) = f(x) \Rightarrow g(f(y)) = g(f(x)) = z \Rightarrow y = x$ .
- 4)  $\phi(y \mapsto z) = \phi(y \mapsto (y \in \text{Im } f \rightarrow z|z')) \Rightarrow (\forall y \in F, (y \in \text{Im } f \text{ ou } z = z')) \Rightarrow \text{Im } f = F$ .

**Corrolaire 1.** Si  $G \neq \emptyset$  et  $E \subset F$ , l'application  $G^F \ni g \mapsto g|_E$  est surjective sur  $G^E$ .

**Corrolaire 2.** Soit une injection  $f \in F^E$  où  $E \neq \emptyset$ , alors  $\exists g \in E^F, g \circ f = \text{Id}_E$ .

**Corrolaire 3.** Soient deux ensembles  $E, F$ , soit  $f \in F^E$ , et considérons  $f^*$  comme fonction de  $\mathcal{P}(F)$  dans  $\mathcal{P}(E)$ . Alors on a ( $f$  injective  $\Leftrightarrow f^*$  surjective), et ( $f$  surjective  $\Leftrightarrow f^*$  injective).

**Théorème.** Soient trois ensembles  $E, F, G$ , soit  $g \in G^F$ , et soit  $\psi = (F^E \ni f \mapsto g \circ f)$  la fonction de composition à gauche par  $g$ , arrivant dans  $G^E$ . On a alors:

- 1) Si  $g$  est injective alors  $\psi$  est injective
- 2) (Si  $g$  est surjective alors  $\psi$  est surjective) est une expression de l'axiome du choix.
- 3) Si  $\psi$  est injective et  $E \neq \emptyset$  alors  $g$  est injective.
- 4) Si  $\psi$  est surjective et  $E \neq \emptyset$  alors  $g$  est surjective.

Preuves:

- 1)  $\forall f, f' \in F^E, \psi(f) = \psi(f') \Leftrightarrow \forall x \in E, g(f(x)) = g(f'(x)) \Rightarrow \forall x \in E, f(x) = f'(x) \Rightarrow f = f'$ .
- 2) sera étudié avec l'axiome du choix.
- 3)  $\forall y, y' \in F, g(y) = g(y') \Rightarrow \psi(x \mapsto y) = \psi(x \mapsto y') \Rightarrow (\forall x \in E, y = y') \Rightarrow y = y'$  car  $E \neq \emptyset$ .
- 4)  $\forall z \in G, \exists f \in F^E, g \circ f = (x \mapsto z)$  donc  $E \neq \emptyset \Rightarrow z \in \text{Im } g$ .

**Proposition.** Soient  $f \in F^E, g \in E^F$  tels que  $g \circ f = \text{Id}_E$ . Alors  $f$  est injective,  $g$  est surjective, et on a les équivalences : ( $f$  surjective)  $\Leftrightarrow$  ( $g$  injective)  $\Leftrightarrow f \circ g = \text{Id}_F$ .

Preuve:

Les premiers résultats découlent de l'injectivité et la surjectivité de  $\text{Id}_E = g \circ f$ .

De  $f \circ g = \text{Id}_F$  on tire les résultats analogues en échangeant  $f$  et  $g$ .

Si  $f$  est surjective alors  $f \circ g \circ f = f \Rightarrow f \circ g = \text{Id}_F$

Si  $g$  est injective alors  $g \circ f \circ g = g \Rightarrow f \circ g = \text{Id}_F$ . □

En particulier, si  $f$  ou  $g$  est bijective et  $g \circ f = \text{Id}_E$  alors  $f$  et  $g$  sont l'inverse l'un de l'autre.

*Points fixes; fonctions idempotentes*

**Définition.** Etant donnée une fonction  $f$  d'un ensemble  $E$  dans lui-même, on dit qu'un élément  $x \in E$  est un point fixe de  $f$  ssi  $f(x) = x$ . L'ensemble des points fixes de  $f$  sera noté  $\text{Fix } f$ .

**Définition.** Une fonction  $f$  d'un ensemble dans lui-même est dite idempotente ssi  $f \circ f = f$ .

Pour tous ensembles  $E$  et  $F$ , tous  $f \in F^E$  et  $g \in F^F$ ,

$$\begin{aligned} \text{Fix } g &\subset \text{Im } g \\ g \circ f = f &\Leftrightarrow \text{Im } f \subset \text{Fix } g \\ g \circ g = g &\Leftrightarrow \text{Im } g = \text{Fix } g \end{aligned}$$

## 2.7. Quelques propriétés des relations binaires sur un ensemble.

On appelle *relation binaire sur un ensemble  $E$* , une relation dont les 2 arguments sont de domaine  $E$ , autrement dit  $R \subset E \times E$ . Nous noterons ici  $x R y$  au lieu de  $(x, y) \in R$ .

Une relation binaire  $R$  sur un ensemble  $E$  est dite:

- *réflexive* ssi  $\forall x \in E, x R x$
- *antiréflexive* ssi  $\forall x \in E, \text{non}(x R x)$
- *symétrique* ssi  $\forall x, y \in E, x R y \Rightarrow y R x$
- *antisymétrique* ssi  $\forall x, y \in E, (x R y \text{ et } y R x) \Rightarrow x = y$ .
- *transitive* ssi  $\forall x, y, z \in E, (x R y \text{ et } y R z) \Rightarrow x R z$

Toute relation binaire transitive et antiréflexive est antisymétrique.

**Relation de préordre.** On appelle *préordre* toute relation binaire réflexive et transitive. Un ensemble muni d'une relation de préordre est dit un ensemble préordonné.

**Relation d'ordre.** On appelle *ordre* tout préordre antisymétrique. Un ensemble muni d'un ordre est appelé un ensemble ordonné.

**Relation d'équivalence.** On nomme ainsi tout préordre symétrique.

Sous-entendons les quantificateurs comme portant sur  $E$  dans la proposition suivante.

**Proposition.** 1) Si  $R$  est un préordre alors  $x R y \Leftrightarrow \overleftarrow{R}(x) \subset \overleftarrow{R}(y)$ , i.e.

$$\forall x, y, x R y \Leftrightarrow \forall z, (z R x \Rightarrow z R y)$$

2) Si de plus  $R$  est symétrique (donc, une relation d'équivalence) alors  $x R y \Leftrightarrow \overleftarrow{R}(x) = \overleftarrow{R}(y)$ , i.e.

$$\forall x, y, x R y \Leftrightarrow \forall z, (z R x \Leftrightarrow z R y)$$

3) Si  $R$  est réflexive et  $\forall x, y, z, (x R y \text{ et } z R y) \Rightarrow z R x$  alors  $R$  est une relation d'équivalence.

Preuves:

1) La transitivité se réécrit  $\forall x, y, x R y \Rightarrow \forall z, (z R x \Rightarrow z R y)$ .

Puis,  $R$  étant réflexive,  $\forall x, y, (\forall z, z R x \Rightarrow z R y) \Rightarrow (x R x \Rightarrow x R y) \Rightarrow x R y$ .

2)  $\forall x, y, x R y \Leftrightarrow (x R y \text{ et } y R x) \Leftrightarrow (\overleftarrow{R}(x) \subset \overleftarrow{R}(y) \text{ et } \overleftarrow{R}(y) \subset \overleftarrow{R}(x)) \Leftrightarrow (\overleftarrow{R}(x) = \overleftarrow{R}(y))$ .

3) on vérifie la symétrie:  $\forall x, y, (x R y \text{ et } y R y) \Rightarrow y R x$ . La transitivité en découle.  $\square$

En fait, les propriétés 1) et 2) sont respectivement équivalentes aux notions de préordre et de relation d'équivalence, et peuvent donc leur servir de définitions.

## 2.8. Etude des relations d'équivalence

*Partitions et familles-partitions*

Soit  $E$  un ensemble.

On appellera *famille-partition de  $E$*  une famille  $(A_i)_{i \in I}$  de parties de  $E$  non vides, deux à deux disjointes et dont l'union est  $E$ , autrement dit

$$\begin{aligned} \forall i \in I, A_i \neq \emptyset \\ \forall i, j \in I, i \neq j \Rightarrow A_i \cap A_j = \emptyset \\ \bigcup_{i \in I} A_i = E \end{aligned}$$

Reformulons la deuxième condition:

$$\begin{aligned} (\forall i, j \in I, i \neq j \Rightarrow A_i \cap A_j = \emptyset) &\Leftrightarrow \forall i, j \in I, i \neq j \Rightarrow \forall x \in E, \text{non}(x \in A_i \text{ et } x \in A_j) \\ &\Leftrightarrow \forall i, j \in I, \forall x \in E, i \neq j \Rightarrow \text{non}(x \in A_i \text{ et } x \in A_j) \\ &\Leftrightarrow \forall x \in E, \forall i, j \in I, (x \in A_i \text{ et } x \in A_j) \Rightarrow i = j \\ &\Leftrightarrow \forall x \in E, \forall i \in I, x \in A_i \end{aligned}$$

Par conséquent, le système des 3 conditions pour qu'une famille  $(A_i)_{i \in I}$  de parties de  $E$  soit une famille-partition de  $E$  se résume en un système de deux conditions

$$\begin{aligned} \forall i \in I, \exists x \in E, x \in A_i \\ \forall x \in E, \exists i \in I, x \in A_i. \end{aligned}$$

On appelle *partition de  $E$*  un ensemble  $P$  d'ensembles non vides, deux à deux disjoints et dont l'union est  $E$ . Ceci équivaut à dire que  $\text{Id}_P$  est une famille-partition de  $E$ .

Examinons les correspondances entre les notions suivantes:

- Surjection de domaine  $E$ ;
- Famille-partition de  $E$ ;
- Partition de  $E$ ;
- Relation d'équivalence sur  $E$ .

*Surjection et famille-partition*

Dans ce qui suit, interprétons la notation  $f^\bullet$  comme signifiant  $f_{\text{Im } f}^\bullet$ .

On a une bijection canonique entre l'ensemble des surjections  $f$  de  $E$  sur  $I$  et celui des familles-partitions de  $E$  indexées par  $I$ , définie par  $f \mapsto f^\bullet$ . En effet,  $\mathcal{P}(E \times I) \simeq \mathcal{P}(E)^I$  envoie l'ensemble des graphes de surjections  $\text{Gr } f$ , sur l'ensemble des familles-partitions  $f^\bullet = \overline{\text{Gr } f}$ .

De surjection à relation d'équivalence

**Relation d'équivalence associée à une fonction  $f$ .** On nomme ainsi la relation  $\sim_f$  définie sur  $E = \text{Dom } f$  par :  $\forall x, y \in E, x \sim_f y \Leftrightarrow f(x) = f(y)$ .

Ses propriétés de réflexivité, symétrie et transitivité se vérifient immédiatement.

Relation d'équivalence et partition, surjection canonique

Soit  $R$  une relation binaire sur  $E$  et  $P = \text{Im } \overleftarrow{R}$ , où par convention  $\text{Dom } \overleftarrow{R} = E$ .

Le fait que  $R$  soit une relation d'équivalence, se réexprime par les formules équivalentes

$$\begin{aligned} \forall x, y \in E, x R y &\Leftrightarrow \overleftarrow{R}(x) = \overleftarrow{R}(y) \\ \forall x, y \in E, x \in \overleftarrow{R}(y) &\Leftrightarrow \overleftarrow{R}(x) = \overleftarrow{R}(y) \\ \forall x \in E, \forall A \in P, x \in A = \text{Id}_P(A) &\Leftrightarrow \overleftarrow{R}(x) = A \\ \text{Id}_P &= \overleftarrow{R}^\bullet. \end{aligned}$$

L'ensemble des partitions de  $E$ , autrement dit des  $P \subset \mathcal{P}(E)$  tels que  $\text{Id}_P$  est une famille-partition de  $E$ , donc de la forme  $\overleftarrow{R}^\bullet$  pour une certaine relation binaire  $R$  sur  $E$  finalement unique, est ainsi en bijection canonique avec l'ensemble des relations d'équivalence.

Dans les constructions ci-dessus, lorsque  $R$  est une relation d'équivalence, et que donc  $P$  est une partition, l'ensemble  $P$  est appelé le *quotient de  $E$  par  $R$*  et noté  $E/R$ ; et la fonction  $\overleftarrow{R} \in P^E$  est appelée *surjection canonique* de  $E$  sur  $E/R$ . Pour tout  $x \in E$ , l'élément  $\overleftarrow{R}(x)$ , unique élément  $A$  de  $P$  tel que  $x \in A$ , est appelé la *classe de  $x$  par  $R$* .

De surjection à partition

A toute surjection  $f$  de  $E$  sur  $I$  nous avons associé une relation d'équivalence  $R$  sur  $E$  par  $\forall x, y \in E, x R y \Leftrightarrow f(x) = f(y)$ , et montré que toute relation d'équivalence  $R$  est égale à celle associée à  $\overleftarrow{R}$ . Puis nous avons associé à une telle relation  $R$  une partition  $P = \text{Im } \overleftarrow{R}$  de  $E$ .

En fait  $P = \text{Im}(f^\bullet)$ , tout comme il était égal à  $\text{Im}(\overleftarrow{R}^\bullet)$  où  $\overleftarrow{R}^\bullet = \text{Id}_P$ : la définition de  $R$  se traduit par

$$\forall x, y \in E, x \in \overleftarrow{R}(y) \Leftrightarrow f(x) = f(y) \Leftrightarrow x \in f^\bullet(f(y))$$

autrement dit  $\overleftarrow{R} = f^\bullet \circ f$ , d'où  $P = \text{Im } \overleftarrow{R} = \text{Im } f^\bullet$  puisque  $f$  est surjective.

L'ensemble  $I$  muni de  $f$ , étant naturellement par  $f^\bullet$  en bijection avec  $E/R$ , pourra être utilisé comme jouant le rôle de  $E/R$ , autrement dit être vu comme un autre quotient (une copie du quotient) de  $E$  par  $R$ ; le rôle de la surjection canonique est alors joué par  $f$ .

**Remarque.**  $f_{\text{Im } f}^\bullet$  est injective (ce qui devient faux sur  $f^\bullet$  étendu à plus d'un élément hors de  $\text{Im } f$ ).

On peut le voir directement, ou en notant que  $\sim_f = \sim_{f^\bullet \circ f}$ .

Autre résultat

**Lemme.** Soient  $E, F, G$  ensembles,  $f \in F^E, g \in G^E, H = \text{Im}(f \times g) \subset F \times G$ , et soit  $R \subset F \times G$ . Alors

$$(\forall x \in E, (f(x), g(x)) \in R) \Leftrightarrow (\forall (y, z) \in H, (y, z) \in R)$$

**Théorème.** Avec les mêmes notations, si  $\text{Im } f = F$  et  $\forall x, x' \in E, f(x) = f(x') \Rightarrow g(x) = g(x')$  (ce qu'on abrégera en  $\sim_f < \sim_g$ ) alors il existe un unique  $h \in G^F$  tel que  $g = h \circ f$ . Finalement,

$$\begin{aligned} \{h \circ f | h \in G^F\} &= \{g \in G^E | \sim_f < \sim_g\} \\ \{h \circ f | h \in G^F \text{ et } h \text{ inject.}\} &= \{g \in G^E | \sim_f = \sim_g\} \end{aligned}$$

Preuve:  $g = h \circ f \Leftrightarrow (\forall (y, z) \in H, z = h(y)) \Leftrightarrow H \subset \text{Gr } h$ . On vérifie que  $H$  est un graphe fonctionnel de domaine  $F$ : d'une part,  $\text{Im } f = F \Rightarrow \forall y \in F, \exists z \in G, (y, z) \in H$ . Enfin,

$$\sim_f < \sim_g \Leftrightarrow \forall (y, z) \in H, \forall (y', z') \in H, y = y' \Rightarrow z = z' \quad \square$$

**Notation.** Soit  $g \in F^E$  et  $R$  une relation d'équivalence sur  $E$  telle que  $R < \sim_g$ . On note alors  $g/R$  la fonction de domaine  $E/R$  définie par  $g = (g/R) \circ \overleftarrow{R}$ . Elle est injective lorsque  $R = \sim_g$ .

## 2.9. Axiome du choix

**Axiome du choix (AC).** Il s'écrit (pour tout ensemble  $X$ ,  $AC_X$ ), où  $AC_X$  (axiome du choix sur  $X$ ) est l'omni-énoncé pouvant s'écrire sous les formes équivalentes:

- 1) Tout produit indexé par  $X$  d'ensembles non vides est non vide
- 2) Pour tout ensemble  $E$  et toute relation  $R$  entre  $X$  et  $E$ ,

$$(\forall x \in X, \exists y \in E, R(x, y)) \Rightarrow (\exists f \in E^X, \forall x \in X, R(x, f(x)))$$

- 3) Toute fonction  $g$  d'image  $X$  a un inverse à droite:  $\exists f \in (\text{Dom } g)^X, g \circ f = \text{Id}_X$ .

1)  $\Rightarrow$  2) est immédiat;

2)  $\Rightarrow$  1) en définissant  $E$  par l'union.

2)  $\Rightarrow$  3) en définissant  $R(x, y) \Leftrightarrow (x = g(y))$ .

1)  $\Rightarrow$  3) en prenant la famille  $g^\bullet$  d'ensembles non vides.

3)  $\Rightarrow$  1) par la somme de la famille

3)  $\Rightarrow$  2) à l'aide du graphe de  $R$ . □

Déjà,  $AC_X$  est vrai si  $X$  est fini (on l'a vu dans le cas méta-fini et on le vérifiera ultérieurement).

**Théorème.** Les énoncés suivants sont équivalents à l'axiome du choix:

- 4) Pour tous ensembles  $E, F, G$  et toute  $g \in G^F$  surjective,  $\{g \circ f \mid f \in F^E\} = G^E$ .
- 5) Pour tout ensemble  $E$  et toute relation d'équivalence  $R$  sur  $E$ ,  $\exists A \subset E, \forall x \in E, \exists! y \in A, xRy$ .
- 6) Pour tout ensemble  $E$  d'ensembles,  $\emptyset \notin E \Rightarrow (\prod_{A \in E} A) \neq \emptyset$ .

Preuves:

$AC_E \Rightarrow$  4) par  $\forall h \in G^E, (\forall x \in E, \exists y \in F, g(y) = h(x)) \Rightarrow (\exists f \in F^E, \forall x \in E, g(f(x)) = h(x))$

$AC_G \Rightarrow$  4) par  $\exists i \in F^G, g \circ i = \text{Id}_G$  et  $\forall h \in G^E, i \circ h \in F^E$  et  $g \circ i \circ h = h$ .

4)  $\Rightarrow$  3) : avec  $E = G$ , par  $\text{Id}_E \in \{g \circ f \mid f \in F^E\}$ .

3)  $\Rightarrow$  5) :  $\exists g \in E^{E/R}, \overline{R} \circ g = \text{Id}_{E/R}$  de sorte que  $A = \text{Im } g$  convient.

5)  $\Rightarrow$  3) : soit  $E = \text{Dom } g$ , et  $A \subset E$  tel que  $\forall x \in E, \exists! y \in A, g(x) = g(y)$ . Alors  $g|_A$  est bijective de  $A$  sur  $X$ , et son inverse  $f \in A^X \subset E^X$  vérifie  $g \circ f = g|_A \circ f = \text{Id}_X$ .

1)  $\Rightarrow$  6) : il suffit de prendre la famille  $\text{Id}_E$ .

6)  $\Rightarrow$  1) : soit  $(A_i)_{i \in I}$  une famille d'ensembles non vides, et soit  $E$  son image  $\{A_i \mid i \in I\}$ . On a alors  $\emptyset \notin E$ , donc il existe  $f \in \prod_{A \in E} A$ . Alors  $(f(A_i))_{i \in I} \in \prod_{i \in I} A_i$ . □

Les logiciens professionnels ont établi que AC est indécidable dans le système axiomatique ZF: s'il est vrai dans un univers de ZF, alors il est faux dans un autre ( $AC_X$  devient faux pour certains ensembles infinis  $X$ ), et inversement. C'est le premier exemple d'indécidabilité d'un énoncé utilisant l'opérateur de puissance, due à sa dépendance par rapport à l'univers dans lequel on l'interprète.

Ainsi AC peut être faux dans un univers  $\mathcal{U}$  mais vrai dans un univers plus vaste  $\mathcal{U}'$ , si une fonction  $g$  dans  $\mathcal{U}$  n'a des inverses à droite que dans  $\mathcal{U}'$  et non dans  $\mathcal{U}$ . Au contraire il peut être vrai dans  $\mathcal{U}$  mais faux dans  $\mathcal{U}'$ , à cause de fonctions  $g$  dans  $\mathcal{U}'$  sans inverse à droite, qui n'existent pas dans  $\mathcal{U}$ . Mais ces constructions sont bien trop complexes pour être abordés ici.

En pratique, comme l'axiome du choix est conforme à l'intuition et plus facile à affirmer qu'à nier (comme il y a plusieurs manières de le nier), la majorité des travaux de mathématiques sur les questions qui en dépendent le supposent vrai. Cependant, bien des questions n'en dépendent pas, ou se satisfont d'une version plus faible (notamment  $AC_{\mathbb{N}}$ ).

Dans la suite nous utiliserons les opérateurs de puissance de manière encore plus poussée; mais non pas l'axiome du choix (sauf cas particuliers), pour la seule raison qu'on n'en aura pas besoin.