I . −un bref survol de téhorie des ensembles

I.1 . −Le système de ZERMELO fini

Faute de pouvoir « définir » les ensembles (à partir de quoi d'ailleurs) on est amené à proposer une axiomatique des ensembles. La pertinence de ce point de vue, qui pourrait paraître dogmatique, ne se révèlera que dans le fait que l'on puisse écrire les mathématiques de manière convenable dans ce cadre .

Les axiomes de la théorie **ZFC** sécrivent avec les symboles de la logique dont nous rappelons la signification, mais pour lesquels nous ne rappelons pas ici les règles qui font qu'un enchaînement de tels symboles constitue ou non une proposition correcte :

Notation I.1.1 i) $\forall$: pour tout (quantificateur universel ;)

ii) $\exists$: il existe ;

iii) $\text{et ou} \wedge$: et (conjonction ;)

iv) $\text{ou ou} \vee$: disjonction ;

v) $\text{non ou} \not$ négation ;

vi) $\Rightarrow$: implication ; en notant d'ailleurs que ce dernier symbol est introduit par pure comodité ; puisqu'il peut s'exprimer grâce à ceux déjà introduit ci-dessus : En effet $P \Rightarrow Q$ signifie $\not P \vee Q$.

Le système de ZERMELO *fini* $\mathbf{Z}_{\text{fini}}$ explicité ci-après fournit un premier point de départ à la théorie **ZFC** donnée à la définition I.4.2 . Il consiste en un certain nombre d'axiomes qui sont des propositions écrites avec les symboles de la logiques rappelés ci-dessus et dont les seules variables sont des ensembles. Il comportent en outre et principalement le symbole $\in$ dont en quelque sorte, il fixe la « grammaire ». On pourait à juste titre s'étonner une fois encore ici que les axiomes de $\mathbf{Z}_{\text{fini}}$ (et ceux de **ZFC** ne feront pas mieux d'ailleurs) ne « construisent un monde où il n'y a que des ensembles » alors que l'intuition semble suggérer qu'il « existe » des objets mathématiques de « natures » multiples et diverses. Les constructions faites au paragraphe I.2 assurent que ce « monde » des ensembles est assez vaste pour représenter une partie substantiellle des mathématiques. En outre l'homogénéité de ce système est d'une grande lisibilité pour les questions relatives à la cohérence de l'édifice mathématique.

Notation I.1.2 ($\Leftrightarrow$) Nous utiliseront librement dans la suite, pour deux proposition P et Q $P \Leftrightarrow Q$ qui ne signifie rien de plus (mais rien de moins d'ailleurs), que

$$P \Rightarrow Q \wedge Q \Rightarrow P .$$

Définition I.1.3 (Le système $\mathbf{Z}_{\text{fini}}$) $\mathbf{Z}_{\text{fini}\,1}$) (**Ext**)

$$\forall a, b \, (\forall x \, (x \in a \Leftrightarrow x \in b) \Rightarrow a = b) ,$$

$\mathbf{Z}_{\text{fini}\,2}$) (**Paire**)

$$\forall a, b \, \exists c \, (a \in c \text{ et } b \in c) ,$$

$\mathbf{Z}_{\text{fini}\,3}$) (**Un**)

$$\forall a\ \exists b\ \forall x\ (\exists y\ (x \in y \text{ et } y \in a)\ \Rightarrow\ x \in b)\ ,$$

$\mathbf{Z}_{\text{fini}\,4}$) (**Par**)

$$\forall a\ \exists b\ \forall x\ (\forall y\ (y \in x\ \Rightarrow\ y \in a)\ \Rightarrow\ x \in b)\ ,$$

et pour chaque formule ensembliste $F(x, c)$ où a et b n'apparaissent pas comme variables libres,

$\mathbf{Z}_{\text{fini}\,5}$) (**Sep**$_F$)

$$\forall a\ \forall c\ \exists b\ \forall x\ (x \in b\ \Leftrightarrow (x \in a \text{ et } F(x, c)))\ .$$

Les axiomes ci-dessus permettent d'introduire de nouveaux symboles :

Définition I.1.4 (Symboles du langage ensembliste) i) ($\subset$:)

$$\forall a,\ \forall b,\ (a\ \subset\ b\ \Leftrightarrow\ (\forall x(x \in a \Rightarrow x \in b))\ .$$

ii) ($\mathcal{P}(\cdot)$:)
L'ensemble b introduit dans l'axiome $\mathbf{Z}_{\text{fini}\,4}$ de la définition I.1.3 sera noté $\mathcal{P}(a)$.

iii) ($\bigcup$:)
L'ensemble b introduit dans l'axiome de l'union définition I.1.3, axiome $\mathbf{Z}_{\text{fini}\,3}$ peut être noté

$$\bigcup_{x \in a} x\ .$$

iv) ($\cup$:)
Pour deux ensembles a et b l'axiome de la paire définition I.1.3, axiome $\mathbf{Z}_{\text{fini}\,2}$ assure que $c := \{a, b\}$ est bien un ensemble et l'on peut dès lors grâce au point précédent, noter

$$a\ \cup\ b\ :=\ \bigcup_{x \in c} x\ =\ \bigcup_{x \in \{a,b\}} x\ .$$

v) ($\cap$:)

$$\forall a,\ \forall b,\ \forall x, (x \in\ a\ \cap\ b\ \Leftrightarrow\ x \in a\ \wedge\ x \in b)\ .$$

vi) ($\emptyset$:)

$$\forall x(x\ =\ \emptyset\ \Leftrightarrow\ \forall y(y \notin x))\ .$$

Définition I.1.5 i) (**Formules ensemblistes**)
On appelle *formule ensembliste* une formule comportant des variables, les symboles de la logique (cf. I.1.1) et le symbole $\in$.

ii) (**Formules ensemblistes étendues**)
On appelle *formule ensembliste étendue* une formule comportant des variables, les symboles de la logique et les symboles supplémentaires définis à la définition I.1.4 .

Remarque I.1.6 Il faut noter que toute formule ensembliste étendue peut se reformuler à l'aide de formule ensemblistes et que par conséquent, on pourra les utiliser dans la suite sans sortir du cadre des axiomes de la définition I.1.3 y compris pour formuler de nouveaux axiomes. Un bon exercice consiste à réécrire avec les symboles de la définition I.1.4 ceux des axiomes de la définition I.1.3 qui peuvent l'être leur donnant alors une forme plus lisible et plus usuelle.

I.2 . –Représentation des objets mathématique

On peut désormais constater qu'un certain nombre de constructions très usuelles peuvent être faite dans le cadre de la théorie des ensembles :

Définition I.2.1 i) (**Couples**)
Au regard des axiomes de la définition I.1.3 , seules les paires existent. Or dans une paire il est impossible de parler de l'ordre des éléments : $\{x, y\} = \{y, x\}$. On peut représenter le *couple* (x, y) par $\big\{\{x, y\}, \{x\}\big\}$. C'est alors un bon exercice sur les manipulations des axiomes de la définition I.1.3 de montrer que $(x, y) \neq (y, x)$.

ii) (**Produit cartésien**)
Dès l'instant où l'on dispose de couples on peut définir le *produit cartésien* de deux ensembles a et b noté $a \times b$ par :

$$a \times b := \{(x, y) \,;\, x \in a,\ y \in b\} .$$

iii) (**Relation**)
une *relation* (ou *relation binaire*) sur un ensemble a est alors une partie R du produit cartésien $a \times a$. À la notation naturellement issue du formalisme développé jusqu'ici $(x, y) \in R$, on préférera bien sûr, celle tout à fait usuelle et connue de $x\ R\ y$.

iv) (**Fonction**)
Une *fonction* f d'un ensemble a dans un ensemble b est une partie du produit cartésien $a \times b$ [1] telle que

$$\forall (x, y) \in f,\ \forall (z, y) \in f,\ x = z .$$

Autrement dit un élément de a possède au plus une image par f. Ici encore on continuera à écrire (comme on l'a toujours fait) $y = f(x)$ pour $(x, y) \in f$.

On rappelle maintenant quelques définitions espérons-le bien connues concernant les relations et les fonctions :

Définition I.2.2 (Relations) Soit a un ensemble et R une relation sur a :

i) (**Réflexivité**)
On dit que R est *réflexive* si

$$\forall x \in a,\ x\ R\ x .$$

ii) (**Symétrie**)
On dit que R est *symétrique* si

$$\forall x \in a,\ \forall y \in a,\ (x\ R\ y \ \Rightarrow\ y\ R\ x) .$$

1. Autrement dit on représente une fonction par son *graphe*.

iii) (**Antisymétrie**)
On dit que R est *antisymétrique* si

$$\forall x \in a,\ \forall y \in a,\ (x\ R\ y\ \wedge\ y\ R\ x\ \Rightarrow x\ =\ y)\ .$$

iv) (**Transitivité**)
On dit que R est *transitive* si

$$\forall x \in a,\ \forall y \in a,\ \forall z \in a,\ (x\ R\ y\ \wedge\ yRZ\ \Rightarrow x\ R\ z)\ .$$

v) (**Relation d'équivalence**)
On dit que R est une *relation d'équivalence* si elle est réflexive symétrique et transitive.

vi) (**Relation d'ordre**)
On dit que R est une *relation d'ordre* si elle est réflexive antisymétrique et transitive. On dit alors que le couple (a, R) est un *ensemble ordonné*. On dit que R est une *relation d'ordre totale* si

$$\forall x \in a,\ \forall y \in a,\ (x\ R\ y\ \vee\ y\ R\ x)\ ;$$

dans ce cas on dit que le couple (a, R) est un *ensemble totalement ordonné*.

vii) (**Majorant/minorant** . . .)
Si $(a, \leq)$ est un ensemble ordonnée et b
$subseta$ une partie de a : Un *majorant* (resp. *minorant*) pour b (dans a,) est un élément $x\ \in\ a$ vérifiant

$$\forall y \in b,\ (y \leq x) \text{ resp. } (\forall y \in b,\ (x \leq y))\ .$$

Si b possède un majorant (resp. un minorant) on dit que b est *majoré* (resp. *minoré*.)
Un *plus grand élément* (resp. *plus petit élément*) pour b est un majorant (resp. minorant) de b appartenant à b.

Lemme I.2.3 *Si une partie $b\ \subset\ a$ d'un ensemble ordonné $(a, \leq)$ possède un plut petit (resp. plus grand) élément, celui-ci est unique.*

Démonstration : *C'est une conséquence immédiate de l'antisymétrie des relations d'ordre.*

Définition I.2.4 (Fonctions) Soit f une fonction de a dans b

$$\text{ce que nous noterons } f\ :\ a\ \rightarrow\ b\ :$$

i) (**Domaine**)
On appelle *domaine* de f et on note

$$\mathrm{Dom}\, f\ :=\ \{x\ \in\ a\ ;\ \exists y \in b\ ;\ (x, y) \in f\}\ =\ \{x\ \in\ a\ ;\ \exists y \in b\ ;\ f(x)\ =\ y\}$$

le sous-ensemble de a formé des éléments qui ont une image par f.

ii) (**Image**)
On appelle *image* de f et on note

$$\mathrm{Im}\, f \;:=\; \{y \;\in\; b\,;\, \exists x \in a\,;\, (x,y) \in f\} \;=\; \{y \;\in\; b\,;\, \exists x \in a\,;\, f(x) \;=\; y\}$$

le sous-ensemble de b formé des éléments qui ont un antécédent dans a.

iii) (**Application**)
On dit que f est une *application* si $\mathrm{Dom}\, f \;=\; a$.

Notation I.2.5 Pour deux ensembles a et b on peut montrer que les applications de a dans b qui sont des parties de $a \times b$ *i.e.* des éléments de $\mathcal{P}(a \times b)$ forment un ensemble qu'on notera b^a.

Exemple I.2.6 a) (**Identité**)
Pour tout ensemble A (y compris $A \;=\; \emptyset$) l'ensemble A^A contient toujours au moins un élément noté Id_A appelé *identité de* A et caractérisé par

$$\forall x \in A,\; \mathrm{Id}_A(x) \;=\; x\;.$$

b) ($A^\emptyset$)
Il existe une unique application $\emptyset \;\to\; A$ si bien que $A^\emptyset$ est un singleton.

c) ($\emptyset^A$)
Si A n'est pas vide il n'existe aucune application de A dans $\emptyset$ $\emptyset^A$ est donc vide. En revanche $\emptyset^\emptyset$ est un singleton.

Définition I.2.7 (Applications) Soit $f \;:\; a \;\to\; b$ une application.

i) (**Injectivité**)
On dit que f est *injective* si

$$\forall x \in a,\; \forall y \in a,\; (f(x) \;=\; f(y) \;\Rightarrow\; x \;=\; y)\;.$$

ii) (**Surjectivité**)
On dit que f est *surjective* si

$$\forall y \in b,\; \exists x \in a (f(x) \;=\; y)\;.$$

iii) (**Bijectivité**)
On dit que f est *bijective* si elle est simultanément injective et surjective.

Définition I.2.8 (Restriction) Soient a et b des ensembles. Pour tout $c \;\subset\; a$, il est immédiat de vérifier que

$$(c \times b) \;\subset\; (a \times b)\;.$$

Pour toute fonction (resp. application) $f \;:\; a \;\to\; b$ [2] il n'est pas difficile de constater non plus que $f \cap (c \times b)$ est une fonction (resp une application) de c dans b, qu'on appellera *restriction* de f à c et qu'on notera $f_{|c}$.

Lemme I.2.9 (Propriétés de la restriction) *i) Si* $f \;:\; a \;\to\; b$ *est une fonction* $f_{|\mathrm{Dom}\, f}$ *est une application.*

2. définie rappelons-le par son graphe (cf. I.2.1. iv ,)

ii) Si $f : a \to b$ est une application injective, pour tout $c \subset a$, $f_{|c}$ est encore une application injective.

Démonstration : *Laissée en exercice.*

Définition I.2.10 (Applications et ordre) Si

$$f : (a, \leq) \to (b, \leq)$$

est une application d'un ensemble ordonné $(a, \leq)$ dans un ensemble ordonné $(b, \leq)$ on dit que f est *croissante* (resp. *décroissante*) si

$$\forall x \in a,\ \forall y \in a,\ \big(x \leq y \ \Rightarrow\ f(x) \leq f(y) (\text{resp. } f(y) \leq f(x))\big) .$$

On dit que f est *strictement croissante* (resp. *strictement décroissante* si

$$\forall x \in a,\ \forall y \in a,\ \big(x < y \ \Rightarrow\ f(x) < f(y) (\text{resp. } f(y) < f(x))\big) .$$

Lemme I.2.11 *Une application strictement croissante (resp. strictement décroissante) entre ensembles ordonnés est injective.*

Définition I.2.12 (Image directe/réciproque d'une partie)

Étant donnée une fonction $f : a \to b$,

i) (**Image directe**)
Pour toute partie $c \in a$ de a, on appelle *image directe* (ou simplement *image*) de c par f et on note $f(c)$ l'ensemble

$$f(c) := \{y \in b\,;\, \exists x \in a,\ y = f(x)\} .$$

C'est aussi l'image $\mathrm{Im}\, f_{|c}$ de la restriction de f à c.

ii) (**Image réciproque**)
Pour toute partie $d \in b$ de b, on appelle *image réciproque* de d par f l'ensemble noté

$$f^{-1}(d) := \{x \in a\,;\, f(x) \in d\} .$$

Remarque I.2.13 (ATTENTION) La notation $f^{-1}(d)$ ci-dessus ne signifie pas qu'il existe une fonction f^{-1} et que $f^{-1}(d)$ soit l'image directe de d par cette fonction.

Dans le cas où f est bijective, il existe effectivement une bijection réciproque $g : b \to a$ vérifiant

$$f \circ g = \mathrm{Id}_b \text{ et } g \circ f = \mathrm{Id}_a .$$

Alors pour toute partie $d \in b$ de b, c'est un exercice (qu'il convient de faire si on ne l'a jamais fait auparavant) de montrer que

$$f^{-1}(d) = g(d) .$$

Proposition I.2.14 (Produit) *Étant donnés deux ensembles a et b non vides, on définit les applications*

$$p : a \times b \to a\,,\ (x, y) \mapsto x \text{ et } q : a \times b \to b\,,\ (x, y) \mapsto y .$$

Alors :

i) Les applications p et q sont surjectives.

ii) Pour tout ensemble c et tout couple d'applications

$$\big(f\,:\,c\,\to\,a, g\,:\,c\,\to\,b\big),$$

il existe une unique application

$$h\,:\,c\,\to\,a\times b \text{ telle que } p\,\circ\,h\,=\,f \text{ et } q\,\circ\,h\,=\,g\,.$$

Définition I.2.15 Avec les notations de la proposition ci-dessus, l'application p (resp. q,) est appelée *première projection* (resp. *deuxième projection*) ou encore *projection sur le premier facteur* (resp. *projection sur le deuxième facteur*.)

I.3 . −Représentation des entiers

On vient de voir qu'un certain nombre de construction usuelles peuvent se faire dans le cadre des axiomes de ZERMELO finis définition I.1.3 . On va expliquer sommairement maintenant comment ils permettent presque de représenter les entiers .

On s'apercevra cependant que les axiomes de la définition I.1.3 ne sont pas tout à fait suffisants et la possibilité de faire de larithmétique motivera suffisaemment, espérons-le, du moins, l'introduction de l'axiome de l"infini définition I.3.4 .

Remarque I.3.1 L'axiome $\mathbf{Z}_{\text{fini}\,4}$ et l'axiome $\mathbf{Z}_{\text{fini}\,5}$ de la définition I.1.3 permettent de définir pour tout ensemble a le singleton

$$\{a\}\,:=\,\{b\in\mathcal{P}(a)\,;\,a\,b\,=\,a\}\,.$$

L'union de deux ensembles construite au point iv de la définition I.1.4 permet ensuite de définir $\mathfrak{s}(a)\,:=\,a\,\cup\,\{a\}$.

Exemple I.3.2 Rien dans l'axiomatique de la définition I.1.3 n'assure jusqu'ici que l'ensemble vide $\emptyset$ défini au point vi de la définition I.1.4 existe ni même qu'il existe aucun ensemble. Cependant on pourrait s'interroger sur le bien fondé d'une théorie sans objets. De toute façon l'axiome de l'infini définition I.3.4 remediera à cette lacune. Même si nous en donnerons une formulation impliquant le symbole $\emptyset$ il faut se persuader qu'on pourrait en donner une formulation purement ensembliste au sens du point i de la définition I.1.5 et qu'alors l'existence de l'ensemble vide s'en déduit grâce à l'axiome $\mathbf{Z}_{\text{fini}\,5}$ de la définition I.1.3 (de séparation).

À ce point, si on suppose cependant que $\emptyset$ existe on a :

$$\begin{array}{rcl}\mathfrak{s}(\emptyset) &=& \emptyset\cup\{\emptyset\}\\ &=& \{\emptyset\},\\ \mathfrak{s}(\mathfrak{s}(\emptyset)) &=& \{\emptyset\}\cup\{\{\emptyset\}\}\\ &=& \big\{\emptyset,\{\emptyset\}\big\}\\ \mathfrak{s}(\mathfrak{s}(\mathfrak{s}(\emptyset))) &=& \big\{\emptyset,\{\emptyset\}\big\}\cup\big\{\big\{\emptyset,\{\emptyset\}\big\}\big\}\\ \big\{\emptyset,\{\emptyset\},\big\{\emptyset,\{\emptyset\}\big\}\big\}\ \ldots & & \end{array}\qquad \text{I.3.2.1}$$

On s'aperçoit qu'à chaque opération $\mathfrak{s}$, le « nombre d'éléments » augmente d'un et que les ensembles ainsi construits pourraient être de bons candidats pour représenter les entiers, pour peu qu'on puisse les « équiper » de suffisamment de « structure algébrique » *i.e.* $+,\cdot,\ldots$

On va donc préciser un peu ce qui précède sans toutefois entrer trop dans les détails.

Définition I.3.3 (Ensembles récurrent) On dit qu'un ensemble a est *récurrent* si

$$\emptyset \in a \text{ et } \forall x \in a,\ (\mathfrak{s}(x) \in a)\ .$$

On a dès lors le sentiement qu'un ensemble représentant les entiers naturels devrait être un ensemble récurrent .

Cependant à ce point il ne semble pas possible d'établir l'existence même de tels ensembles uniquement à partir des axiomes du système de ZERMELO fini définition I.1.3 . Dans ce cas on a recours à l'introduction d'un nouvel axiome, lequel d'ailleurs ne choque pas la raison :

Définition I.3.4 (Axiome de l'infini) On appelle *axiome de l'infini* la formule :

$$\exists a(\emptyset \in a \text{ et } \forall x \in a,\ (\mathfrak{s}(x) \in a))\ .$$

Définition I.3.5 (Système de ZERMELO Z) On appelle *système de* ZERMELO le système d'axiomes constitué des axiomes de ZERMELO fini définition I.1.3 auquel on adjoint l'axiome de l'infini.

Autrement dit il existe au moins un ensemble récurrent. Cependant parmi les ensembles récurrents reste à déterminer le bon candidat pour représenter les entiers naturels, c'est-à-dire, moralement, celui qui contiendrait les entiers naturels ; rien de plus rien de moins. Moyennant de vérifier le lemme :

Lemme I.3.6 *L'intersection de deux ensembles récurrents est un ensemble récurrent.*

On peut introduire l'ensemble ω défini comme suit :

Définition I.3.7 On notera ω le plus petit ensemble récurrent.

I.4 . −Le système de ZERMELO–FRAENKEL

On présente les derniers axiomes qu'il faut adjoindre au système de ZERMELO définition I.3.5 pour arriver au système de ZERMELO–FRAENKEL **ZF** (cf. I.4.1 ,) puis finalement au système **ZFC** (cf. I.4.2 .) On ne mentionnera ces axiomes que pour mémoire et parce que le système **ZF** voire **ZFC** est couramment utilisé par une large partie de la communauté mathématique :

Définition I.4.1 (Le système de ZERMELO–FRAENKEL ZF) Le *système de* ZERMELO–FRAENKEL est obtenu en adjoignant au système de ZERMELO les axiomes : Pour $F(x, y, c)$ formule ensembliste où a et b n'apparaissent pas comme variables libres, on appelle axiome de remplacement pour F :

ZF$_7$) (Remp$_F$)

$$\begin{array}{ll} \forall a \forall c & \big((\forall x, y, z((F(x, y, c) \quad \text{et\&} F(x, z, c)) \Rightarrow y = z\big) \\ \Rightarrow & \exists b \forall y \big(\exists x \in a(F(x, y, c)) \qquad\qquad \Rightarrow \qquad\qquad y \in b)\big)\big)\ . \end{array}$$

ZF$_8$) (Fondation)

$$\forall a(a \neq \emptyset \Rightarrow \exists b \in a(b \cap a = \emptyset))\ .$$

On réserve ordinairement une place à part à l'axiome du choix sans doute parce qu'un certain nombre de matthématiciens ne l'utilisent qu'avec une extrême circonspection tandis que certains autres le refusent tout bonnement. Le point de vue le plus pragmatique consiste à clairement désigner les résultats dont une preuve utilise l'axiome du choix.

Les deux résultats marquants de GÖDEL (1938) *s'il est cohérent, le système* ***ZF****ne réfute pas l'axiome du choix, c'est-à-dire qu'il n'existe pas de preuve de la négation de l'axiome du choix à partir des axiomes du système* ***ZF*** et COHEN (1963) *s'il est cohérent, le système* ***ZF****ne démontre pas l'axiome du choix, c'est-à-dire qu'il n'existe pas de preuve de l'axiome du choix à partir des axiomes du système* ***ZF*** ne permettent de choisir ni en sa faveur ni en sa défaveur.

Définition I.4.2 (ZFC) i) (**fonction de choix**)
Soit a un ensemble. On appelle *fonction de choix* sur a une application $f \,:\, a \setminus \{\emptyset\} \,\to\, a$ vérifiant $f(x) \in x$ pour tout x non vide dans a.

ii) (**Axiome du choix**)
On appelle *axiome du choix* l'énoncé : Tout ensemble possède une fonction de choix.

iii) (**Le système ZFC**)
On appelle *système* ***ZFC*** la famille d'axiomes constituée des axiomes de **ZF**
et de l'axiome du choix ci-dessus, c'est-à-dire constituée des axiomes de ZERMELO fini introduits à la définition I.1.3 de l'axiome définition I.3.4 de l'infini, de l'axiome $\mathbf{ZF}_7$ de la définition I.4.1 (de remplacement,) de l'axiome $\mathbf{ZF}_8$ de la définition I.4.1 (de fondation) et de l'axiome du choix.

I.5 . −Loi de composition, (magma,) morphisme

Définition I.5.1 (Loi de composition) Pour un ensemble M on appelle *loi de composition* (ou *loi de composition interne* ou *loi interne*) $*$ sur M une application (cf. I.2.4. iii ,)

$$* \,:\, M \times M \,\to\, M\,.$$

Évidemment à la notation $((x,y),z) \in *$ qui découle de l'axiomatique présentée précédemment on préférera toujours celle $x * y \,=\, z$.

Le couple $(M,*)$ est appelé *magma*.

Définition I.5.2 (Morphisme homomorphisme) Étant donnés deux magmas

$$(M,*) \text{ et } (N,\cdot)$$

on dit qu'une application $f \,:\, M \,\to\, N$ est un *morphisme* ou *homomorphisme* de $(M,*)$ dans $(N,\cdot)$ si

$$\forall x \in M,\ \forall y \in M,\ (f(x*y) \,=\, f(x) \,\cdot\, f(y))\,.$$

Lemme I.5.3 *i) Pour tout magma $(M,*)$ l'identité Id_M est un morphisme du magma M dans lui-même.*

ii) Pour $(M,*_M)$, $(N,*_N)$ et $(P,*_P)$ des magmas, $f \,:\, M \,\to\, N$ et $g \,:\, N \,\to\, P$ des morphismes, le composé $g \circ f$ est un morphisme.

Définition I.5.4 Étant donnés deux magmas $(M, *)$ et $(N, \cdot)$, un morphisme $f : M \to N$ est un *isomorphisme* s'il existe un morphisme $g : N \to M$ tel que

$$g \circ f = \mathrm{Id}_M \text{ et } f \circ g = \mathrm{Id}_N .$$

On notera $\mathrm{Isom}(M, N)$ l'ensemble des isomorphismes de $(M, *)$ dans $(N, \cdot)$.

Lemme I.5.5 *Étant donné un morphisme $f : M \to N$, si f possède une application réciproque i.e. une application $g : N \to M$ telle que*

$$f \circ g = \mathrm{Id}_N \text{ et } g \circ f = \mathrm{Id}_M,$$

alors g et également un morphisme.

Démonstration *:*

$$\begin{array}{lll} \forall (u, v) \in N \times N, \quad g(u \cdot v) & = & g\big[f[g(u)] \cdot f[g(v)]\big] \\ & = & g\big[f[g(u) * g(v)]\big] \\ & = & g(u) * g(v) . \end{array}$$

Proposition I.5.6 *Étant donnés deux magmas $(M, *)$ et $(N, \cdot)$, une application $f : M \to N$ est un isomorphisme si et seulement si c'est un morphisme bijectif.*

Démonstration *: Si f est un isomorphisme, c'est par définition un morphisme qui est bijectif puisque possédant une application réciproque.*

Réciproquement si $f : M \to N$ est une application bijective, il existe (cf. l'exercice I.7.8 ,) une application

$$g : N \to M \text{ telle que } g \circ f = \mathrm{Id}_M \text{ et } f \circ g = \mathrm{Id}_N .$$

Alors : Le résultat découle immédiatement du lemme I.5.5 .

Définition I.5.7 Soit $(M, *)$ un magma.

i) (**Enndomorphismes**)
Un morphisme $f : M \to M$ de M dans lui-même est appelé *endomorphisme*. On note $\mathrm{End}(M)$ l'ensemble des endomorphismes de M.

ii) (**Automorphisme**)
Un morphisme $f : M \to M$ est un *automorphisme* si c'est à la fois un isomorphisme et un endomorphisme. Il revient au même, grâce à la proposition I.5.6 , de dire que f est un endomorphisme bijectif. On note $\mathrm{Aut}(M)$ l'ensemble des automorphismes de M.

Exemple I.5.8 Pour un magma M, l'identité Id_M est un automorphisme de M.

Définition I.5.9 (Associativité) On dit qu'une loi de composition $*$ sur un ensemble M est *associative* si

$$\forall x \in M, \ \forall y \in M, \ \forall z \in M, \ ((x * y) * z = x * (y * z)) .$$

On peut alors parler pour $(M, *)$ de *magma associatif*.

Définition I.5.10 (Commutativité) On dit qu'une loi de composition $*$ sur un ensemble M est *commutative* si

$$\forall x \in M,\ \forall y \in M,\ (x * y \ = \ y * x)\ .$$

Définition I.5.11 (Éléments particuliers) Soit $(M, *)$ un ensemble muni d'une loi de composition associative (magma associatif)

i) (**Élément neutre**)
Un *élément neutre* pour $(M, *)$ est un élément $\epsilon \ \in \ M$ tel que

$$\forall x \in M,\ (x * \epsilon \ = \ \epsilon * x \ = \ x)\ .$$

ii) (**Symétrique**)
Si M possède un élément neutre ϵ on dit qu'un élément $x \ \in \ M$ possède un symétrique pour la loi $*$ s'il existe $y \ \in \ M$ tel que

$$x * y \ = \ y * x \ = \ \epsilon\ .$$

Remarque I.5.12 Dans la suite on ne considérera que des magmas associatifs dans la mesure où ce seront les seuls que nous rencontrerons. Il se peut que certains énoncés puissent être formulés sans cette hypothèse mais nous ne cherchons pas le plus grand degré de généralité possible mais une présentation que nous espérons la plus claire et la plus lisible ainsi que la moins répétitive.

Exemple I.5.13 Si X est un ensemble l'ensemble M des applications de X dans lui-même est un magma associatif pour la loi $\circ$ de composition des applications. Il possède un élément neutre Id_X. En revanche un élément $f \ : \ X \ \to \ X$ de M n'a pas de symétrique en général puisque f n'est pas bijective en général. La loi $\circ$ n'est en général pas commutative non plus.

Proposition I.5.14 (Propriétés) *Soient $(M, *)$ un magma associatif.*

i) Si ϵ et ϵ' sont des éléments neutres de $(M, *)$ alors $\epsilon \ = \ \epsilon'$.

ii) Si $(M, *)$ possède un élément neutre et si y et z éléments de M sont des symétriques pour $x \ \in \ M$, $y \ = \ z$.

Remarque I.5.15 On pourra donc parler de L'élément neutre d'un magma lorsqu'il en possède un et du symétrique d'un élément lorsqu'il en possède un.

Pour un magma $(M, *)$ et une partie N de M, $N \times N$ est une partie de $M \times M$. La restriction $*_{|N\times N}$ de $*$ à $N \times N$ est une application $*_{|N\times N} \ : \ N \times N \ \to \ N$. Il se peut cependant que :

Définition I.5.16 (Sous-magma) Que $*_{|N\times N}$ soit à valeurs dans N. On dit dans se cas que la loi $*$ se restreint en une loi interne (usuellement encore notée $*$) sur N.
On pourra alors dire que $(N, *)$ est un sous-magma de $(M, *)$

La définition ci-dessus ne présente pas un grand intérêt en soi, hormis celui de pouvoir énoncer confortablement la proposition I.5.17 . Cette dernière n'étant d'ailleurs elle-même qu'un moyen commode de ne pas réécrire de nombreuses fois le même argument.

Proposition I.5.17 (Propriétés des sous-magmas) *Soit $(M, *)$ un magma.*

i) Le magma $(M, *)$ est toujours un sous-magma de lui-même. Si M possède un élément neutre ϵ, $(\{\epsilon\}, *)$ est un sous-magma de $(M, *)$.

ii) Soit $(N,*)$ un sous-magma de $(M,*)$. Si $(M,*)$ est associatif (resp. commutatif) $(N,*)$ l'est aussi.
Soit $f : (M,*) \to (N,\cdot)$ un morphisme de magmas.

iii) Pour tout sous-magma M' de M, $f(M')$ est un sous-magma de N.

iv) Pour tout sous-magma N' de N, $f^{-1}(N')$ est un sous-magma de M.

Proposition I.5.18 *Soient $(M,*)$ un magma, E un ensemble et M^E l'ensemble des applications de E dans M. Pour tout $(f,g) \in M^E \times M^E$, on définit $f *_{M^E} g \in M^E$ de la manière suivante : Pour tout $x \in E$,*

$$f *_{M^E} g(x) := f(x) * g(x) .$$

i) $(M^E, *_{M^E})$ est un magma c'est-à-dire que $*_{M^E}$ est une loi de composition interne sur M^E.

ii) La loi $*_{M^E}$ est la seule loi sur l'ensemble M^E telle que, pour tout $x \in E$, l'application

$$M^E \to M , f \mapsto f(x)$$

soit un morphisme.

iii) Le magma $(M^E, *_{M^E})$ est associatif dès que $(M,*)$ l'est.

iv) Le magma $(M^E, *_{M^E})$ est commutatif dès que $(M,*)$ l'est.

v) Si $(M,*)$ possède un élément neutre ϵ, l'application

$$\epsilon_{M^E} : E \to M , x \mapsto \epsilon$$

est l'élément neutre de M^E.

Définition I.5.19 Étant donnés un magma $(M,*)$ et un ensemble E, on appellera *loi induite* par celle de M sur M^E, la loi $*_{M^E}$ construite à la proposition I.5.18 . On la notera bien sûr simplement $*$ en général.

Exemple I.5.20 On est habitué depuis longtemps à écrire $f+g$ pour f et g des applications de $\mathbb{R}$ dans lui-même par exemple, ainsi que $f * g$ en utilisant les lois de compositions $+$ et $*$ dont on dispose sur l'ensemble $\mathbb{R}$ des nombres réels.

Proposition I.5.21 *Étant donnés deux magmas $(M,*)$ et $(N,\cdot)$,*

i) la loi $\dagger$ définie sur le produit cartésien $M \times N$ par

$$(x,y) \dagger (z,t) := (x * z, y \cdot t)$$

est l'unique loi telle que les projections

$$p : M \times N \to M , (x,y) \mapsto x \text{ et } q : M \times N \to N , (x,y) \mapsto y$$

(cf. I.2.15 ,) soient des morphismes ;

ii) Pour tout magma $(P, \sharp)$, et tout couple de morphismes

$$\big(f \,:\, (P,\sharp) \,\to\, (M,*)\,,\; g \,:\, (P,\sharp) \,\to\, (N,\cdot)\big)$$

il existe un unique morphisme

$$h \,:\, (P,\sharp) \,\to\, (M\times N,\dagger) \text{ tel que } p \,\circ\, h \,=\, f \text{ et } q \,\circ\, h \,=\, g\,.$$

Démonstration *: (cf. I.7.18 .)*

I.6 . −Ce qu'il faut retenir

La plupart des développements de ce chapitre (I ,) constituent des considérations historiques ou de motivation.

Cependant il est indispensable de pouvoir utiliser correctement les symboles $\in$, $\subset$, $\cap$ et $\cup$ du langage ensembliste.

Il est également nécessaire d'être familier avec les définitions concernants les relations binaires et les fonctions définition I.2.1, point iii à remarque I.2.13 .

Enfin le paragraphe I.5 servira de base aux chapitres II .

I.7 . −Exercices

Exercice I.7.1 (L'ensemble des parties) Est-il vrai que

$$\mathcal{P}(A\cap B) \,=\, \mathcal{P}(A)\cap\mathcal{P}(B) \text{ et } \mathcal{P}(A\cup B) \,=\, \mathcal{P}(A)\cup\mathcal{P}(B)\,?$$

Exercice I.7.2 Soient $A, B \subset E$. Résoudre les équations à l'inconnue $X \subset E$

1) $A \cup X = B$.

2) $A \cap X = B$.

Exercice I.7.3 (Fonctions caractéristiques) Soit A une partie de E, on appelle fonction caractéristique de A l'application f de E dans l'ensemble à deux éléments $\{0,1\}$, telle que :

$$f(x) = \begin{cases} 0 & \text{si } x \notin A \\ 1 & \text{si } x \in A \end{cases}$$

Soit A et B deux parties de E, f et g leurs fonctions caractéristiques. Montrer que les fonctions suivantes sont les fonctions caractéristiques d'ensembles que l'on déterminera :

$$1-f\,,\; fg\,,\;\;,\; f+g-fg\,.$$

Exercice I.7.4 (Différence symétrique) Soit un ensemble E et deux parties A et B de E. On désigne par $A\triangle B$ l'ensemble $(A\cup B)\setminus(A\cap B)$. *Dans les questions ci-après il pourra être commode d'utiliser la notion de fonction caractéristique.*

1) Démontrer que

$$A\triangle B \,=\, (A\setminus B)\,\cup\,(B\setminus A)\,.$$

2) Démontrer que pour toutes les parties A, B, C de E on a

$$(A\triangle B)\triangle C \;=\; A\triangle(B\triangle C)\,.$$

3) Démontrer qu'il existe une unique partie X de E telle que pour toute partie A de E,

$$A\triangle X \;=\; X\triangle A \;=\; A\,.$$

4) Démontrer que pour toute partie A de E, il existe une partie A' de E et une seule telle que

$$A\triangle A' \;=\; A'\triangle A \;=\; X\,.$$

Exercice I.7.5 (Propriétés de la différence symétrique) A **et** B **sont des parties d'un ensemble** E.
Montrer que :

1) $(A\triangle B \;=\; A\cap B) \;\Leftrightarrow\; (A \;=\; B \;=\; \emptyset)\,.$

2)

$$(A\cup B)\cap(B\cup C)\cap(C\cup A) \;=\; (A\cap B)\cup(B\cap C)\cup(C\cap A)\,.$$

3) $A\triangle B \;=\; B\triangle A\,.$

4) $(A\triangle B)\triangle C \;=\; A\triangle(B\triangle C)\,.$

5) $A\triangle B \;=\; \emptyset \;\Leftrightarrow A \;=\; B\,.$

6) $A\triangle C \;=\; B\triangle C \;\Leftrightarrow A \;=\; B\,.$

Exercice I.7.6 (Injection) Étant donée une application $f \;:\; A \;\to\; B$,

1) démontrer que les propositions suivantes sont équivalentes

i) f est injective ;

ii) il existe une application g de B dans A telle que $g \circ f \;=\; \mathrm{Id}A$.

On dit alors que g **est une *rétraction* de** f.

2) Une telle rétraction est elle unique ? Étudier le cas de $A = B = \mathbb{N},\; f(n) = 2n$.

Exercice I.7.7 (Surjection) Étant donnée une application $f \;:\; A \;\to\; B$,

1) démontrer que les propositions suivantes sont équivalentes

i) f est surjective ;

ii) il existe une application g de B dans A telle que $f \circ g \;=\; \mathrm{Id}B$.

On dit alors que g est une *section* de f.

2) Une telle section est elle unique ?

3) Démontrer que si deux sections ont même image elles coïncident.

Exercice I.7.8 (Bijection) 1) Pour des ensembles E et F, montrer que $f : E \to F$ est une bijection de E sur F si et seulement si il existe une application $g : F \to E$ telle que

$$g \circ f = \mathrm{Id}_E \text{ et } f \circ g = \mathrm{Id}_F . \qquad 1$$

2) Il existe au plus une application $g : F \to E$ vérifiant 1. 1 .

3) Si g vérifie 1. 1 , g est elle-même une bijection qu'on appelle du fait de l'unicité établie à la question 2 , la *bijection réciproque* de f.

Exercice I.7.9 (Propriétés des applications) Soit $f : E \to F$ une application.

1) a) Montrer que

$$\forall A \in \mathcal{P}(F),\ f(f^{-1}(A)) \subset A .$$

b) Montrer que f est surjective si et seulement si

$$\forall A \in \mathcal{P}(F),\ A = f(f^{-1}(A)) .$$

2) (**Injectivité (facultatif)**)

a) Montrer que

$$\forall A \in \mathcal{P}(E),\ A \subset f^{-1}(f(A)) .$$

b) Montrer que f est injective si et seulement si

$$\forall A \in \mathcal{P}(E),\ A = f^{-1}(f(A)) .$$

Exercice I.7.10 (Image directe/réciproque) 1) Soient X et Y deux ensembles et f une application de X dans Y.

Si A et B sont deux sous-ensembles de X (respectivement de Y), quel est le lien entre $f(A \cup B)$ et $f(A) \cup f(B)$, $f(A \cap B)$ et $f(A) \cap f(B)$, $f^{-1}(f(A))$ et A (respectivement $f^{-1}(A \cup B)$ et $f^{-1}(A) \cup f^{-1}(B)$, $f^{-1}(A \cap B)$ et $f^{-1}(A) \cap f^{-1}(B)$, $f(f^{-1}(A))$ et A).

Pour toute inclusion fausse, donner un exemple et éventuellement une propriété supplémentaire de f qui la rend juste.

2) Pour $f : E \to F$ une application entre deux ensembles, les applications :

$$\begin{array}{rcl} \mathcal{P}(E) & \to & \mathcal{P}(F) \\ A & \mapsto & f(A) \\ & \text{et} & \\ \mathcal{P}(F) & \to & \mathcal{P}(E) \\ B & \mapsto & f^{-1}(B) \end{array}$$

sont-elles (strictement) croissantes ? décroissantes ? par rapport à $\subset$?

Exercice I.7.11 Faire la preuve de la proposition I.2.14 .

Exercice I.7.12 (Produit cartésien et applications) Soient A, B, C trois ensembles.

$$\text{Étant donnée une application } f : A \times B \to C,$$

pour tout $x \in A$, on définit $g(x) \in C^B$ une application de B dans C par

$$g(x)(y) := f\big((x,y)\big) .$$

Montrer que l'application

$$\phi : C^{A\times B} \to (C^B)^A , \ f \mapsto g$$

est une bijection,
Indication : *on pourra donner sa bijection réciproque.*

Exercice I.7.13 Faire les détails de la preuve de la proposition I.5.14 .

Exercice I.7.14 Étant doné un morphisme $f : M \to N$, (de magmas associatifs,) montrer que :

1) si ϵ est l'élément neutre de M son image $f(\epsilon)$ n'est pas nécessairement l'élément neutre de N ;

2) si y est le symétrique de x dans M, $f(y)$ n'est pas nécessairement le symétrique de $f(x)$ dans N.

Exercice I.7.15 Donner la preuve de la proposition I.5.18 .

Exercice I.7.16 **1)** Compléter la preuve de la proposition I.5.17 .

2) **a)** Si ϵ est un élément neutre de M est-il encore un élément neutre d'un sous-magma N ?

b) Si N possède un élément neutre η celui-ci est-il nécessairement celui de M ?

c) Si $x \in N$ possède un symétrique dans M celui-ci est-il aussi son symétrique dans N ?

d) Si $x \in N$ possède un symétrique dans N est-il aussi son symétrique dans M ?

Exercice I.7.17 Soit $(M, *)$ un magma associatif, d'élément neutre ϵ et N un sous-magma tel que $\epsilon \in N$. Montrer que :

1) ϵ est l'élément neutre de N.

2) si $x \in N$ a un inverse y dans N, c'est aussi son inverse dans M.

Exercice I.7.18 Faire la preuve de la proposition I.5.21 .

II . −Groupes, morphismes . . .

II.1 . −Groupe

Définition II.1.1 (Groupe) Un *groupe* est un couple $(G, *)$ (le plus souvent simplement noté $G,$) où G est un ensemble et $* \ : \ G \times G \ \to \ G$ est une application appelée *loi de composition* vérifiant :

Gr_1) Pour tout triplet (x, y, z) d'éléments de G,

$$(x * y) * z \ = \ x * (y * z) \ ,$$

on dit que la loi interne $*$ est *associative*.

Gr_2) Il existe un élément $e \ \in \ G$ appelé *élément neutre* de G tel que, pour tout $x \ \in \ G, x * e \ = \ e * x \ = \ x$.

Gr_3) Pour tout élément $x \ \in \ G$, il existe un élément $x' \ \in \ G$ appelé *symétrique* de x et tel que $x * x' \ = \ x' * x \ = \ e$.

Il revient au même de dire que $(G, *)$ est un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique.

Les formulations « $(G, *)$ est un groupe » ou « $*$ munit G d'une *structure de groupe* » sont synonymes.

Exemple II.1.2 i) Il n'existe pas de loi de composition $*$ sur $\emptyset$ fasse de $(\emptyset, *)$ un groupe. L'axiome Gr_2 de la définition II.1.1 entraîne, en effet, qu'un groupe possède toujours au moins un élément c'est-à-dire n'est jamais vide.

b) On peut définir une unique loi de composition qui donne à l'ensemble $\{\emptyset\}$ à un élément une structure de groupe :

$$\emptyset * \emptyset \ := \ \emptyset \ .$$

c) (**Le groupe** $\mathcal{S}(X)$)

Un des premiers groupes qu'on peut introduire, au sens où sa définition ne nécessite guère plus que les premiers axiomes de la théorie des ensembles(cf. I ,) est le groupe $\mathcal{S}(E)$ des bijections d'un ensemble E muni de la loi $\circ$(cf. la question 1 de l'exercice II.5.4 .) C'est une partie du magma considéré dans l'exemple I.5.13 , et précisément celle constituée des éléments qui ont un symétrique. Pour ne nécessiter que très peu de matériel pour être défini, ce groupe n'est cependant pas le plus aisé à étudier

Définition II.1.3 (Groupe abélien) Étant donné un groupe $(G, *)$, si pour tout couple (x, y) d'éléments de G, $x * y \ = \ y * x,$ on dira que G est *abélien* ou *commutatif*.

Dans ce cas on notera usuellement $+$ la loi interne et 0 l'élément neutre en référence au groupe abélien $(\mathbb{Z}, +)$

Un groupe n'étant rien de plus (ni de moins d'ailleurs) qu'un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique, la proposition I.5.14 vaut encore ici mutatis mutandis.

Proposition II.1.4 (Propriétés) *Soient $(G, *)$ un grouepe.*

i) Si ϵ et ϵ' sont des éléments neutres de $(G, *)$ alors $\epsilon \ = \ \epsilon'$.

ii) Si y et z éléments de E sont des symétriques pour $x \ \in \ E, y \ = \ z$.