

## Rappels de théorie des ensembles

L'objectif de ces notes est de rappeler quelques notions de base de la théorie des ensembles. Ce n'est pas un cours sur le sujet au sens formel du terme. Par exemple, on ne donne pas la définition précise d'un ensemble, étant entendu qu'un ensemble est généralement défini par une propriété caractéristique de ses éléments. En particulier, on supposera acquis le fait que deux ensembles sont égaux si et seulement si ils ont les même éléments. On utilisera aussi librement les notions d'appartenance et d'inclusion. Néanmoins, on évoquera l'axiome du choix sans lequel de nombreux résultats considérés comme «évidents» ne pourraient être démontrés. À la fin du chapitre se trouve une démonstration du théorème de Cantor-Bernstein établi vers 1900, qui est parfois très pratique pour démontrer que deux ensembles sont en bijection.

### Table des matières

1. Parties d'un ensemble - L'ensemble vide	1
2. Applications	2
3. L'axiome du choix	5
4. Relations d'ordre - Lemme de Zorn	8
5. L'ensemble des entiers naturels	13
6. Relations d'équivalence	24
7. Théorème de Cantor-Bernstein	26

### 1. Parties d'un ensemble - L'ensemble vide

Pour tout ensemble  $E$  il en existe un autre, noté  $\mathcal{P}(E)$ , dont les éléments sont les parties de  $E$ . Par exemple,  $E$  est un élément de  $\mathcal{P}(E)$ . Pour toute partie  $A$  de  $E$ , l'ensemble des éléments de  $E$  qui ne sont pas dans  $A$ , que l'on notera  $E - A$  ou  $E \setminus A$ , s'appelle le complémentaire de  $A$  dans  $E$ . En particulier, on peut considérer l'ensemble

$$\emptyset_E = E - E.$$

Pour tout  $x \in E$ , la relation  $x \in \emptyset_E$  est équivalente à la conjonction des deux relations  $x \in E$  et  $x \notin E$ . Il n'existe donc aucun élément dans  $\emptyset_E$ . C'est la partie vide de  $E$ . En fait l'ensemble  $\emptyset_E$  ne dépend pas de  $E$ . Autrement dit, quels que soient les ensembles  $E$  et  $F$ ,

on a  $\emptyset_E = \emptyset_F$ . En effet, tout élément de  $\emptyset_E$  est dans  $\emptyset_F$ , vu que  $\emptyset_E$  n'en contient aucun. On note ainsi

$$\emptyset_E = \emptyset$$

et on l'appelle l'ensemble vide, sans faire référence à l'ensemble considéré. C'est un élément de  $\mathcal{P}(E)$ . Il a la propriété remarquable que tout ce que l'on peut dire sur ses éléments est vrai, pour la raison qu'il n'en possède pas. Par exemple, il est vrai que tout élément de l'ensemble vide vaut à la fois 1 et 2. Ce n'est pas pour autant que l'on a  $1 = 2$ . Contrairement à ce que l'on pourrait penser, tout cela n'est pas sans intérêt, notamment dans certains raisonnements par récurrence. On retiendra par ailleurs que  $E$  et  $\emptyset$  sont complémentaires l'un de l'autre.

Pour tout ensemble  $E$  et tous  $A$  et  $B$  dans  $\mathcal{P}(E)$ , on note comme il se doit  $A \cup B$  et  $A \cap B$  respectivement la réunion et l'intersection de  $A$  et  $B$ . La différence symétrique de  $A$  et  $B$  est par définition

$$A \triangle B = A \cup B - A \cap B.$$

On a l'égalité

$$(A \cap A) \triangle A = A \triangle A = \emptyset.$$

Si  $E$  est infini, elle fournit un exemple d'un polynôme de degré 2, à coefficients dans un anneau commutatif non intègre, ayant une infinité de racines. L'anneau en question est le triplet  $(\mathcal{P}(E), \triangle, \cap)$ , avec  $\triangle$  comme addition et  $\cap$  comme multiplication. L'élément neutre additif est l'ensemble vide et l'élément neutre multiplicatif est  $E$ . Le polynôme de degré 2 est alors  $X^2 + X$  à coefficients dans  $\mathcal{P}(E)$ . Cela sera confirmé dans le cours sur la théorie des anneaux.

## 2. Applications

Rappelons ce que l'on entend par application (ou fonction, ces mots sont synonymes) entre deux ensembles.

**Définition 1.** Soient  $E$  et  $F$  des ensembles. On appelle application  $E$  dans  $F$  tout triplet

$$f = (G, E, F)$$

satisfaisant les deux conditions suivantes :

- 1)  $G$  est une partie de  $E \times F$ .
- 2) Pour tout élément  $x$  de  $E$ , il existe un unique élément  $y$  de  $F$  tel que  $(x, y)$  soit dans  $G$ .

On dit que  $G$  est le graphe de  $f$ . L'ensemble  $E$  (resp.  $F$ ) s'appelle l'ensemble de départ (resp. d'arrivée) de  $f$ . On note généralement  $f : E \rightarrow F$  une application de  $E$  dans  $F$ . À chaque élément  $x$  de  $E$ , elle associe par définition un unique élément  $f(x)$  de  $F$ .

**Exemples 1.**

1) Pour tout ensemble  $E$ , il existe une unique application  $\emptyset \rightarrow E$ . Il s'agit du triplet  $(\emptyset, \emptyset, E)$ . Si  $E = \emptyset$ , on l'appelle l'application vide.

2) Il n'existe pas d'applications  $E \rightarrow \emptyset$  sauf si  $E = \emptyset$ .

3) Si  $F = E$ , l'application  $\text{Id}_E : E \rightarrow E$  qui à chaque  $x \in E$  associe  $x$ , s'appelle l'application identique, ou l'identité, de  $E$ .

4) Soient  $E$  un ensemble et  $A$  une partie de  $E$ . L'application  $\mathbf{1}_A : E \rightarrow \{0, 1\}$  définie pour tout  $x \in E$  par

$$\mathbf{1}_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon,} \end{cases}$$

s'appelle la fonction caractéristique de  $A$  relativement à  $E$ . Pour tous  $A$  et  $B$  dans  $\mathcal{P}(E)$ , on a les égalités

$$\mathbf{1}_{A \cap B} = \mathbf{1}_A \mathbf{1}_B, \quad \mathbf{1}_{E-A} = 1 - \mathbf{1}_A, \quad \mathbf{1}_{A \cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \mathbf{1}_B,$$

$$\mathbf{1}_{A \Delta B} = \mathbf{1}_A + \mathbf{1}_B - 2\mathbf{1}_A \mathbf{1}_B.$$

5) Une fonction est parfois définie à l'aide d'opérations algébriques sur la variable  $x$ . Soit  $\mathbb{R}$  l'ensemble des nombres réels. À titre indicatif, la fonction  $f : \mathbb{R} \rightarrow \mathbb{R}$  définie par l'égalité  $f(x) = x^2$  n'est autre que le triplet  $(G, \mathbb{R}, \mathbb{R})$ , où  $G$  est l'ensemble des couples  $(x, y) \in \mathbb{R} \times \mathbb{R}$  tels que  $y = x^2$ .

6) Si  $f : E \rightarrow F$  et  $g : F \rightarrow G$  sont des applications, on dispose de l'application composée  $g \circ f : E \rightarrow G$  qui à chaque  $x \in E$  associe  $g(f(x))$ .

**Définition 2.** Soient  $f : E \rightarrow F$  une application,  $A$  une partie de  $E$  et  $B$  une partie de  $F$ .

1) L'image de  $A$  par  $f$ , notée  $f(A)$ , est l'ensemble des éléments  $y \in F$  pour lesquels il existe  $x \in A$  tels que  $y = f(x)$ .

2) L'image réciproque de  $B$  par  $f$ , notée  $f^{-1}(B)$ , est l'ensemble des éléments  $x \in E$  tels que  $f(x)$  appartienne à  $B$ .

Si  $y$  est dans  $F$ , on note souvent  $f^{-1}(y)$  l'image réciproque du singleton  $\{y\}$  par  $f$ .

**Définition 3.** Soit  $f : E \rightarrow F$  une application.

1) Elle est injective si pour tous  $x$  et  $y$  dans  $E$ , on a l'implication

$$f(x) = f(y) \implies x = y.$$

2) Elle est surjective si pour tout  $y \in F$ , il existe  $x \in E$  tel que  $y = f(x)$ .

3) Elle est bijective si elle est à la fois injective et surjective.

L'application  $f$  est bijective si et seulement si il existe une application  $g : F \rightarrow E$  telle que l'on ait

$$g \circ f = \text{Id}_E \quad \text{et} \quad f \circ g = \text{Id}_F.$$

Si tel est le cas,  $g$  est unique. C'est l'application réciproque de  $f$ .

**Remarques 1.** Soient  $E$  et  $F$  des ensembles et  $f : E \rightarrow F$  une application.

1) Pour tous  $A$  et  $B$  dans  $\mathcal{P}(E)$ , on a

$$f(A \cup B) = f(A) \cup f(B).$$

2) On a toujours  $f(A \cap B) \subseteq f(A) \cap f(B)$ , mais on n'a pas en général l'égalité. En effet, soit  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  l'application qui à un entier associe sa valeur absolue. Prenons  $A = \mathbb{N}$  et  $B = -\mathbb{N}$  les opposés des entiers naturels. On a  $A \cap B = \{0\}$ , d'où  $f(A \cap B) = \{0\}$ , pour autant on a  $f(A) = f(B) = f(A) \cap f(B) = \mathbb{N}$ .

3) Pour tous  $A$  et  $B$  dans  $\mathcal{P}(F)$ , on a

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B) \quad \text{et} \quad f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B).$$

4) Pour tous  $A \in \mathcal{P}(E)$  et  $B \in \mathcal{P}(F)$ , on a les inclusions

$$A \subseteq f^{-1}(f(A)) \quad \text{et} \quad f(f^{-1}(B)) \subseteq B.$$

Ce ne sont pas en général des égalités. En effet, considérons comme ci-dessus l'application  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  telle que  $f(n) = |n|$ . En prenant  $A = \mathbb{N}$ , on a  $f(A) = \mathbb{N} = f(\mathbb{Z})$ , d'où  $f^{-1}(f(A)) = \mathbb{Z} \neq A$ . De même, avec  $B = \{0\}$ , on a  $f^{-1}(B) = \{0\}$ , d'où  $f(f^{-1}(B)) = \{0\}$ .

5) Pour tout  $B \in \mathcal{P}(F)$ , on a

$$E - f^{-1}(B) = f^{-1}(F - B).$$

Étant donné  $A \in \mathcal{P}(E)$ , les ensembles  $f(E - A)$  et  $F - f(A)$  ne sont généralement pas comparables. Avec  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  définie par  $f(n) = |n|$ , et  $A = \mathbb{N}$ , on a  $f(\mathbb{Z} - A) = \mathbb{N}^*$  et  $\mathbb{Z} - f(A)$  est l'ensemble des entiers strictement négatifs. Dans ce cas,  $f(E - A)$  et  $F - f(A)$  sont disjoints, donc en particulier non comparables.

6) Les conditions suivantes sont équivalentes :

(1)  $f$  est injective.

(2) Pour tout  $A \in \mathcal{P}(E)$ , on a  $f^{-1}(f(A)) = A$ .

(3) Pour tous  $A$  et  $B$  dans  $\mathcal{P}(E)$ , on a  $f(A \cap B) = f(A) \cap f(B)$ .

7)  $f$  est surjective si et seulement si pour tout  $B \in \mathcal{P}(F)$ , on a  $f(f^{-1}(B)) = B$ .

**Exemple 2.** L'application  $E \rightarrow \mathcal{P}(E)$  qui à  $x$  associe le singleton  $\{x\}$  est une injection. Cela étant,  $E$  et  $\mathcal{P}(E)$  ne sont jamais en bijection :

**Théorème 1 (Cantor, 1891).** *Il n'existe pas de surjection de  $E$  sur  $\mathcal{P}(E)$ .*

Démonstration : Soit  $f : E \rightarrow \mathcal{P}(E)$  une application. Soit  $A$  la partie de  $E$  formée des  $x \in E$  tels que  $x$  n'appartienne pas à  $f(x)$ . Supposons qu'il existe  $a \in E$  tel que  $f(a) = A$ . On a alors l'équivalence  $a \in A \iff a \notin A$ , d'où une contradiction. Ainsi,  $A$  n'est pas dans l'image de  $f$ , donc  $f$  n'est pas surjective.

### 3. L'axiome du choix

Étant donnés des ensembles  $I$  et  $E$ , une famille d'éléments de  $E$  indexée par  $I$ , que l'on note  $(x_i)_{i \in I}$ , est une application de  $I$  dans  $E$  qui à  $i$  associe  $x_i$ . Mis à part la notation, il n'y a donc pas de différence entre les notions d'application et de famille d'éléments d'un ensemble. La notation que l'on adopte dépend en fait du contexte. Si  $I = \mathbb{N}$  on dit que c'est une suite d'éléments de  $E$ . On peut ainsi parler de familles d'ensembles  $(E_i)_{i \in I}$ , où les  $E_i$  sont des parties de  $E$  i.e. des éléments de  $\mathcal{P}(E)$ , notion liée à l'axiome du choix :

**Axiome du choix.** Soient  $E$  un ensemble et  $(E_i)_{i \in I}$  une famille de parties non vides de  $E$  indexée par un ensemble  $I$ . Il existe une application  $f : I \rightarrow E$  telle que pour tout  $i \in I$ , on ait  $f(i) \in E_i$ .

**Remarque 2.** On définit le produit cartésien des  $E_i$  comme étant l'ensemble des applications  $f$  de  $I$  dans  $E$  telles que pour tout  $i \in I$  on ait  $f(i) \in E_i$ , autrement dit, l'ensemble des familles d'éléments  $(x_i)_{i \in I}$  de  $E$  telles que pour tout  $i \in I$ , on ait  $x_i \in E_i$ . L'axiome du choix signifie donc qu'un produit d'ensembles non vides est non vide.

Si  $I$  est infini, ce qui est la situation qui justifie cet axiome, il signifie que  $f$  s'obtient en choisissant un élément  $x_i$  dans chaque  $E_i$ , d'où une infinité de choix pour construire  $f$ , sans autre précision et donc sans définition explicite de  $f$ . Kurt Gödel a démontré en 1939 que l'axiome du choix est logiquement compatible avec les autres axiomes de la théorie des ensembles et Paul Cohen en 1963 a établi qu'il en est logiquement indépendant.

Voici deux autres formulations de l'axiome du choix.

**Lemme 1.** *Les deux assertions suivantes sont chacune équivalentes à l'axiome du choix.*

1) Soit  $R(x, y)$  une relation entre les éléments d'un ensemble  $E$  et ceux d'un ensemble  $F$ , autrement dit, une partie de  $E \times F$ . Si pour tout  $x \in E$ , il existe  $y \in F$  tel que l'on ait  $R(x, y)$ , alors il existe une application  $f : E \rightarrow F$  telle que pour tout  $x \in E$ , on ait  $R(x, f(x))$ .

2) Pour tout ensemble  $E$ , il existe une fonction  $h : \mathcal{P}(E) \setminus \{\emptyset\} \rightarrow E$  telle que pour tout  $A \in \mathcal{P}(E) \setminus \{\emptyset\}$ , on ait  $h(A) \in A$ .

**Terminologie.** Une application satisfaisant la condition 2 du lemme s'appelle une fonction de choix sur  $E$ . Une fonction de choix sur  $E$  associe donc à chaque partie non vide  $A$  de  $E$  un élément de  $A$ .

Démonstration : 1) Supposons l'assertion 1 satisfaite. Soit  $(E_i)_{i \in I}$  une famille de parties non vides d'un ensemble  $E$ . Désignons pour tous  $i \in I$  et  $y \in E$  par  $R(i, y)$  la relation  $y \in E_i$ . Les  $E_i$  étant non vides, pour tout  $i \in I$ , il existe  $y \in E_i$  i.e. on a  $R(i, y)$ . D'après l'hypothèse faite, il existe donc une application  $f : I \rightarrow E$  telle que pour tout  $i \in I$ , on ait  $R(i, f(i))$  i.e.  $f(i) \in E_i$ , d'où la condition de l'axiome du choix. Inversement, pour tout  $x \in E$ , considérons l'ensemble

$$F_x = \{y \in E \mid R(x, y)\}.$$

Par hypothèse, pour tout  $x \in E$ , on a  $F_x \neq \emptyset$ . D'après l'axiome du choix, on a donc

$$\prod_{x \in E} F_x \neq \emptyset.$$

Il existe ainsi une application  $f : E \rightarrow E$  telle que pour tout  $x \in E$ , on ait  $R(x, f(x))$ , d'où l'assertion 1.

2) Soient  $E$  un ensemble et  $(E_i)_{i \in I}$  une famille de parties non vides de  $E$ . Supposons qu'il existe une fonction de choix  $h$  sur  $E$ . On définit une application  $f : I \rightarrow E$  par  $f(i) = h(E_i)$ , en particulier  $f(i)$  est dans  $E_i$ .

Inversement, soit  $E$  un ensemble. D'après l'axiome du choix, le produit cartésien

$$\prod_{A \in \mathcal{P}(E) \setminus \{\emptyset\}} A$$

est non vide, d'où l'existence d'une fonction de choix sur  $E$ .

**Exemple 3.** Prenons  $E = \{0, 1\}$ . L'application  $h : \mathcal{P}(E) \setminus \{\emptyset\} \rightarrow E$  définie par

$$h(\{0\}) = 0, \quad h(\{1\}) = 1, \quad h(E) = 1,$$

est une fonction de choix sur  $E$  (il n'y a pas besoin de l'axiome du choix pour expliciter des fonctions de choix sur un ensemble fini).

**Remarque 3.** L'axiome du choix est utilisé pour établir de nombreux résultats (élémentaires ou pas) et très souvent sans même y faire référence. Par exemple, soient

$E$  un espace métrique et  $A$  une partie de  $E$ . Soit  $x$  un élément de  $E$ . Alors, si  $x$  est adhérent à  $A$  il existe une suite d'éléments de  $A$  qui converge vers  $x$ . Pour établir cette assertion, il est a priori nécessaire d'utiliser l'axiome du choix (la réciproque est vraie aussi sans recours à l'axiome du choix). En effet, pour tout  $n \in \mathbb{N}$ , il existe un élément  $y$  dans l'intersection de  $A$  avec la boule ouverte de centre  $x$  et de rayon  $\frac{1}{n+1}$ . D'après l'axiome du choix (dénumbrable), il existe donc une application de  $\mathbb{N}$  dans  $A$ , autrement dit une suite  $(y_n)_{n \in \mathbb{N}}$  d'éléments de  $A$ , telle que pour tout  $n$ , la distance de  $x$  à  $y_n$  soit inférieure à  $\frac{1}{n+1}$ , d'où l'assertion.

Cela étant, si l'on spécifie  $E$  on peut éventuellement s'en passer. Par exemple, si  $E = \mathbb{R}$  et  $A = \mathbb{Q}$ , qui est dense dans  $\mathbb{R}$ , alors pour tout  $x \in \mathbb{R}$ , en posant

$$y_n = \frac{E(10^n x)}{10^n},$$

où  $E(10^n x)$  désigne la partie entière de  $10^n x$ , la suite  $(y_n)_{n \in \mathbb{N}}$  est convergente de limite  $x$ , pour la raison que l'on a  $y_n \leq x < y_n + \frac{1}{10^n}$ . Rappelons au passage que si

$$x = u_0, u_1 u_2 \cdots u_n u_{n+1} \cdots,$$

est le développement décimal propre de  $x$ , c'est-à-dire que pour tout  $p \in \mathbb{N}$ , il existe  $n \geq p$  tel que  $u_n \neq 9$ , on a

$$y_n = u_0, u_1 u_2 \cdots u_n = \sum_{k=0}^n \frac{u_k}{10^k}.$$

C'est l'approximation décimale de  $x$  à  $10^{-n}$  près par défaut.

Comme conséquence de l'axiome du choix, établissons le résultat suivant.

**Proposition 1.** *Soient  $E$  et  $F$  des ensembles. Les conditions suivantes sont équivalentes :*

- 1) *il existe une injection de  $E$  dans  $F$ .*
- 2)  *$E$  est vide ou il existe une surjection de  $F$  sur  $E$ .*

Démonstration : Supposons qu'il existe une injection  $f : E \rightarrow F$  et que  $E$  soit non vide. Choisissons un élément  $x_0 \in E$ . Soit  $g : F \rightarrow E$  l'application définie comme suit. Pour tout  $y \in F$  qui n'est pas dans  $f(E)$ , on pose  $g(y) = x_0$ . Si  $y$  est dans  $f(E)$ , il existe un unique élément  $x \in E$  tel que  $y = f(x)$  car  $f$  est injective. On pose alors  $g(y) = x$ . L'application  $g$  est une surjection de  $F$  sur  $E$ , car si  $z \in E$ , on a  $g(f(z)) = z$ .

Inversement, si  $E$  est vide, l'application  $\emptyset \rightarrow F$  est injective. Supposons qu'il existe une surjection  $g : F \rightarrow E$ . D'après l'axiome du choix, il existe une application

$$h : \mathcal{P}(F) \setminus \{\emptyset\} \rightarrow F$$

telle que pour tout  $X$  dans  $\mathcal{P}(F) \setminus \{\emptyset\}$ , l'élément  $h(X)$  appartienne à  $X$ . Pour tout  $x \in E$ ,  $g^{-1}(x)$  est non vide car  $g$  est une surjection. Soit  $f : E \rightarrow F$  l'application définie pour tout  $x \in E$  par l'égalité

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

Vérifions que  $f$  est une injection. Soient  $x$  et  $x'$  des éléments de  $E$  tels que  $f(x) = f(x')$ . Posons  $X = g^{-1}(x)$  et  $X' = g^{-1}(x')$ . On a  $h(X) = h(X')$ . Ainsi  $f(x)$  est dans  $X \cap X'$ , d'où  $g(f(x)) = x$  et  $g(f(x)) = x'$ , puis  $x = x'$  et l'assertion.

## 4. Relations d'ordre - Lemme de Zorn

### 1. Généralités

**Définition 4.** Une relation d'ordre sur un ensemble  $E$  est une relation binaire  $\mathcal{R}$  sur  $E$  telle que pour tous  $x, y, z$  dans  $E$ , les conditions suivantes soient remplies :

- 1) on a  $x\mathcal{R}x$  (réflexivité).
- 2) Si  $x\mathcal{R}y$  et  $y\mathcal{R}x$ , alors  $x = y$  (antisymétrie).
- 3) Si  $x\mathcal{R}y$  et  $y\mathcal{R}z$ , alors  $x\mathcal{R}z$  (transitivité).

Par commodité, une relation d'ordre est souvent notée  $\leq$ . On appelle ensemble ordonné tout couple  $(E, \leq)$ , où  $E$  est un ensemble et  $\leq$  une relation d'ordre sur  $E$ . Étant donné un tel couple  $(E, \leq)$  et  $x, y$  des éléments de  $E$ , si l'on a  $x \leq y$ , on dit que  $x$  est plus petit que  $y$ , ou que  $x$  est inférieur à  $y$ . On dit aussi que  $y$  est plus grand que  $x$ , ou que  $y$  est supérieur à  $x$  et l'on écrit parfois  $y \geq x$ . Si l'on a  $x \leq y$  avec  $x$  distinct de  $y$ , on écrit souvent  $x < y$  ou  $y > x$  et ces inégalités sont dites strictes.

**Définition 5.** Soit  $(E, \leq)$  un ensemble ordonné. On dit que  $(E, \leq)$  est totalement ordonné, ou que  $\leq$  est une relation d'ordre totale sur  $E$ , si deux éléments quelconques de  $E$  sont comparables, autrement dit, si pour tous  $x$  et  $y$  dans  $E$  on a  $x \leq y$  ou  $y \leq x$ .

### Exemples 4.

1) Si  $(E, \leq)$  est un ensemble ordonné, pour toute partie  $F$  de  $E$ , le couple  $(F, \leq)$  où  $\leq$  est la relation d'ordre induite sur  $F$ , est un ensemble ordonné.

2) Soient  $\mathbb{N}$  l'ensemble des entiers naturels et  $\mathbb{Z}$  celui des entiers relatifs. On dispose dans  $\mathbb{Z}$  de la relation d'ordre, dite naturelle, telle que pour tous  $a, b \in \mathbb{Z}$ , on ait  $a \leq b$  s'il existe  $c \in \mathbb{N}$  tel que  $b = a + c$ . C'est une relation d'ordre totale. Elle induit une relation d'ordre sur  $\mathbb{N}$ .

3) Soit  $\mathbb{Q}$  l'ensemble des nombres rationnels. Il est muni de la relation d'ordre définie pour tous  $\frac{a}{b}$  et  $\frac{c}{d}$  dans  $\mathbb{Q}$ , où  $a, c$  sont dans  $\mathbb{Z}$  et  $b, d$  sont non nuls dans  $\mathbb{N}$ , par la condition

$$\frac{a}{b} \leq \frac{c}{d} \iff ad \leq bc.$$



C'est une relation d'ordre totale, qui prolonge l'ordre naturel de  $\mathbb{Z}$ .

4) Soit  $E$  un ensemble. Dans  $\mathcal{P}(E)$ , l'inclusion  $\subseteq$  est une relation d'ordre. Si  $E$  a au moins deux éléments, elle n'est pas totale.

5) Dans  $\mathbb{N}$ , la relation de divisibilité pour laquelle  $a$  divise  $b$  s'il existe  $q \in \mathbb{N}$  tel que  $b = aq$ , est une relation d'ordre qui n'est pas totale. Notons qu'elle ne définit pas une relation d'ordre sur  $\mathbb{Z}$ , car pour tout entier relatif  $a$  non nul,  $a$  divise  $-a$  et  $-a$  divise  $a$ , pour autant,  $a$  est distinct de  $-a$ .

6) Soient  $E$  un ensemble et  $(F, \leq)$  un ensemble ordonné. Dans l'ensemble des applications de  $E$  dans  $F$ , la relation encore notée  $\leq$ , pour laquelle  $f \leq g$  si pour tout  $x \in E$  on a  $f(x) \leq g(x)$ , est une relation d'ordre. Elle n'est pas totale si  $E$  et  $F$  ont chacun au moins deux éléments. On l'appelle l'ordre fonctionnel.

7) Soient  $(E_i, \leq)$  pour  $i = 1, \dots, n$ , des ensembles ordonnés, et  $E = E_1 \times \dots \times E_n$  le produit cartésien des  $E_i$ . Cet ensemble est muni de deux relations d'ordre standard.

7.1) L'ordre produit, défini pour tous  $(x_1, \dots, x_n)$  et  $(y_1, \dots, y_n)$  dans  $E$  par la condition

$$(x_1, \dots, x_n) \leq (y_1, \dots, y_n) \iff x_i \leq y_i \quad \text{pour tout } i = 1, \dots, n.$$

Il n'est pas total en général.

7.2) L'ordre lexicographique, pour lequel on a  $(x_1, \dots, x_n) \leq (y_1, \dots, y_n)$  si et seulement si  $(x_1, \dots, x_n) = (y_1, \dots, y_n)$  ou bien,  $i$  étant le plus petit indice tel que  $x_i \neq y_i$ , on a  $x_i < y_i$ . C'est une relation d'ordre totale si les  $E_i$  sont totalement ordonnés.

Soit  $(E, \leq)$  un ensemble ordonné.

### Définition 6 (Éléments maximaux - Éléments minimaux).

- 1) Un élément  $a \in E$  est dit maximal si pour tout  $x \in E$ , dès que l'on a  $a \leq x$ , alors  $a = x$ .
- 2) Un élément  $a \in E$  est dit minimal si pour tout  $x \in E$ , dès que l'on a  $x \leq a$ , alors  $a = x$ .

### Exemples 5.

- 1) Dans  $\mathbb{N}$  muni de la relation de divisibilité, 0 est le seul élément maximal.
- 2) Dans  $\mathbb{N} \setminus \{1\}$  muni de la relation de divisibilité, les éléments minimaux sont les nombres premiers.
- 3) Dans  $(\mathcal{P}(E) \setminus \{\emptyset\}, \subseteq)$  les éléments minimaux sont les singletons.
- 4) Dans  $(\mathbb{R}, \leq)$  il n'y a pas d'élément maximal ni d'élément minimal.

Considérons désormais une partie  $F$  de  $E$ .

**Définition 7 (Plus petit élément - Plus grand élément).**

- 1) On dit que  $F$  possède un plus petit élément s'il existe  $a \in F$  tel que pour tout  $x \in F$  on ait  $a \leq x$ .
- 2) On dit que  $F$  possède un plus grand élément s'il existe  $a \in F$  tel que pour tout  $x \in F$  on ait  $x \leq a$ .

**Lemme 2.** Si  $F$  possède un plus petit (resp. un plus grand) élément, celui-ci est unique.

Démonstration : Cela résulte de la propriété d'antisymétrie.

Si  $F$  possède un plus petit (resp. un plus grand) élément, on dit alors que c'est le plus petit (resp. le plus grand) élément de  $F$ .

**Exemples 6.**

- 1) Dans  $\mathcal{P}(E)$  muni de la relation d'inclusion, l'ensemble vide est le plus petit élément, et  $E$  est le plus grand élément.
- 2) Dans  $\mathbb{N}$  muni de son ordre naturel, 0 est le plus petit élément, et il n'y a pas de plus grand élément. Toute partie non vide de  $\mathbb{N}$  possède un plus petit élément.

**Définition 8 (Majorants - Minorants).**

- 1) On dit que  $F$  est majorée s'il existe  $m \in E$  tel que pour tout  $x \in F$  on ait  $x \leq m$ . Un tel élément s'appelle un majorant de  $F$ .
- 2) On dit que  $F$  est minorée s'il existe  $m \in E$  tel que pour tout  $x \in F$  on ait  $m \leq x$ . Un tel élément s'appelle un minorant de  $F$ .
- 3) On dit que  $F$  est bornée si  $F$  est minorée et majorée.

**Remarque 4.** Si  $F$  admet un majorant (resp. un minorant)  $m$  qui est dans  $F$ , alors  $m$  est le plus grand (resp. le plus petit) élément de  $F$ .

**Définition 9 (Borne supérieure - Borne inférieure).**

- 1) Si l'ensemble des majorants de  $F$  admet un plus petit élément, cet élément s'appelle la borne supérieure de  $F$ .
- 2) Si l'ensemble des minorants de  $F$  admet un plus grand élément, cet élément s'appelle la borne inférieure de  $F$ .

**Exemples 7.**

- 1) Dans  $\mathcal{P}(E)$  tout sous-ensemble admet une borne supérieure (la réunion) et une borne inférieure (l'intersection).
- 2) Toute partie non vide et majorée de  $\mathbb{R}$  possède une borne supérieure. Toute partie non vide et minorée de  $\mathbb{R}$  possède une borne inférieure.

**Lemme 3.** Soit  $m$  un élément de  $E$ . Alors  $m$  est la borne supérieure de  $F$  si et seulement si les conditions suivantes sont satisfaites :

- 1) pour tout  $x \in F$ , on a  $x \leq m$ .
- 2) Pour tout  $y \in E$  tel que  $y < m$ , il existe  $x \in F$  tel que  $y$  ne soit pas supérieur ou égal à  $x$ .

Démonstration : Si  $m$  est la borne supérieure de  $F$ , alors  $m$  majore  $F$ , d'où la première condition. Par ailleurs, si  $y \in E$  vérifie l'inégalité  $y < m$ , alors  $y$  ne majore pas  $F$ , d'où la seconde condition. Inversement,  $m$  est un majorant de  $F$  (condition 1) et c'est le plus petit (condition 2), d'où le lemme.

### Remarques 5.

- 1) Si  $E$  est totalement ordonné, la seconde condition signifie qu'il existe  $x \in F$  tel que l'on ait  $y < x$ .
- 2) On a un énoncé analogue pour les bornes inférieures.

## 2. Lemme de Zorn

Il s'agit de l'énoncé suivant établi par Zorn vers 1934.

**Théorème 2.** Soit  $E$  un ensemble ordonné non vide tel que toute partie totalement ordonnée possède un majorant dans  $E$ . Alors,  $E$  a un élément maximal.

Nous admettrons ce résultat qui est en fait équivalent à l'axiome du choix. De nombreuses applications de l'axiome du choix utilisent directement ce lemme. En voici quelques-unes.

### 2.1) Injection entre deux ensembles

**Théorème 3.** Soient  $E$  et  $F$  des ensembles. Il existe une injection de  $E$  dans  $F$  ou une injection de  $F$  dans  $E$ .

Démonstration : Soit  $\mathcal{H}$  l'ensemble des couples  $(A, f)$  tel que l'on ait  $A \subseteq E$  et que  $f : A \rightarrow F$  soit une injection. On munit  $\mathcal{H}$  de la relation d'ordre  $\leq$  définie pour tous  $(A, f)$  et  $(B, g)$  dans  $\mathcal{H}$  par la condition

$$(A, f) \leq (B, g) \iff A \subseteq B \quad \text{et} \quad g \text{ restreinte à } A \text{ est } f.$$

L'ensemble  $\mathcal{H}$  n'est pas vide, car le couple formé de la partie  $\emptyset$  et de l'application  $\emptyset \rightarrow F$ , est dans  $\mathcal{H}$ . Soient  $I$  un ensemble et  $\{(A_i, f_i) \mid i \in I\}$  une partie totalement ordonnée de  $\mathcal{H}$ . Elle possède un majorant dans  $\mathcal{H}$ , à savoir le couple formé de la réunion des  $A_i$  et de l'application  $f : \cup A_i \rightarrow F$  définie par  $f(x) = f_i(x)$  si  $x \in A_i$ , cela est licite car les  $(A_i, f_i)$  forment une partie totalement ordonnée de  $\mathcal{H}$ . D'après le lemme de Zorn,  $\mathcal{H}$

possède un élément maximal  $(A, f)$ . Si  $A = E$ , alors  $f : E \rightarrow F$  est une injection et on a le résultat. Supposons  $A \neq E$ . Vérifions alors que  $f : A \rightarrow F$  est une surjection de  $A$  sur  $F$ . Il existe  $x \in E \setminus A$ . Procédons par l'absurde en supposant  $f$  non surjective. Il existe  $y \in F \setminus f(A)$ . Posons  $B = A \cup \{x\}$  et considérons l'application  $g : B \rightarrow F$  définie par les égalités  $g(a) = f(a)$  si  $a \in A$  et  $g(x) = y$ . C'est une application injective. Le couple  $(A, f)$  est strictement plus petit que  $(B, g)$ , d'où une contradiction et l'assertion. Par suite,  $f$  est une bijection de  $A$  sur  $F$  et l'application  $f^{-1} : F \rightarrow A \subseteq E$  est une injection de  $F$  dans  $E$ , d'où le résultat.

## 2.2) Base d'un espace vectoriel

Soit  $E$  un espace vectoriel sur un corps commutatif  $K$ . On va établir que  $E$  admet une base. C'est une conséquence du résultat plus précis suivant, appelé parfois théorème de la base incomplète.

**Théorème 4.** *Soient  $S$  un système générateur de  $E$  et  $L$  une partie libre de  $E$  contenue dans  $S$ . Il existe une base  $B$  de  $E$  telle que l'on ait  $L \subseteq B \subseteq S$ .*

Le fait que  $E$  possède des bases est une conséquence de cet énoncé en prenant  $L = \emptyset$  et  $S = E$ .

Démonstration : Soit  $\mathcal{L}$  l'ensemble des parties libres de  $S$  contenant  $L$ , que l'on ordonne par la relation d'inclusion. Il est non vide car  $L$  est dans  $\mathcal{L}$ . Soient  $I$  un ensemble et  $\{L_i \mid i \in I\}$  une partie totalement ordonnée non vide de  $\mathcal{L}$ . La réunion des  $L_i$  contient  $L$ . C'est une partie libre de  $E$ . En effet, soient  $x_1, \dots, x_r$  des éléments distincts de la réunion des  $L_i$  et  $\alpha_1, \dots, \alpha_r$  des éléments de  $K$  tels que la somme des  $\alpha_j x_j$  soit nulle. Parce que les  $L_i$  forment une partie totalement ordonnée de  $\mathcal{L}$ , il existe  $j_0$  tel que tous les  $x_i$  soient dans  $L_{j_0}$ , donc tous les  $\alpha_j$  sont nuls. D'après le lemme de Zorn,  $\mathcal{L}$  a donc un élément maximal  $B$ . Vérifions que c'est un système générateur de  $E$ . Considérons pour cela un élément  $x \in S$ . Si  $x$  n'est pas dans le sous-espace vectoriel de  $E$  engendré par  $B$ , alors  $B \cup \{x\}$  est une partie libre de  $E$ , ce qui conduit à une contradiction. Par suite, tout élément de  $S$  est combinaison linéaire des éléments de  $B$ . Puisque  $S$  est un système générateur, il en est de même de  $B$ . C'est donc une base de  $E$ .

Il résulte de cet énoncé que les bases de  $E$  sont exactement les parties libres maximales de  $E$ , ou bien les parties génératrices minimales. On peut démontrer par un procédé analogue que toutes les bases d'un même espace vectoriel sont en bijection.

## 2.3) Idéal maximal d'un anneau

Soit  $A$  un anneau commutatif. Rappelons qu'une partie  $I$  de  $A$  est un idéal de  $A$  si  $I$  est un sous-groupe additif de  $A$  et si pour tous  $a \in A$  et  $x \in I$ , l'élément  $ax$  est dans  $I$ .

L'idéal  $I$  est dit maximal si  $I$  est un élément maximal dans l'ensemble des idéaux de  $A$ , distincts de  $A$ , ordonné par l'inclusion.

**Théorème 5 (Krull).** *Tout idéal de  $A$ , distinct de  $A$ , est contenu dans un idéal maximal.*

Démonstration : Soit  $I$  un idéal de  $A$  distinct de  $A$ . Considérons l'ensemble  $\mathcal{F}$  des idéaux de  $A$  distincts de  $A$  qui contiennent  $I$ . Cet ensemble est ordonné par l'inclusion et il est non vide car  $I$  appartient à  $\mathcal{F}$ . Soit  $L = \{A_i \mid i \in S\}$  une partie non vide totalement ordonnée de  $\mathcal{F}$ . Soit  $U$  la réunion des  $A_i$  pour  $i \in S$ . Puisque  $L$  est totalement ordonnée,  $U$  est un idéal de  $A$ , qui est distinct de  $A$ , car 1 n'appartient à aucun des  $A_i$  (vu que  $A_i$  est un élément de  $\mathcal{F}$ ). Par suite,  $U$  est un élément de  $\mathcal{F}$  et c'est un majorant de  $L$ . D'après le lemme de Zorn,  $\mathcal{F}$  possède un élément maximal. C'est un idéal maximal de  $A$  qui contient  $I$ , d'où le résultat.

## 5. L'ensemble des entiers naturels

### 1. Axiomes de Peano

Nous admettrons l'existence d'un ensemble

$$(1) \quad \mathbb{N} = \{0, 1, 2, \dots\},$$

appelé ensemble des entiers naturels, vérifiant les trois conditions suivantes :

- 1) il est muni d'une injection  $S : \mathbb{N} \rightarrow \mathbb{N}$ , qui à un entier  $n$  associe son successeur noté  $n + 1$ .
- 2) Tout entier autre que 0 a un (unique) prédécesseur
- 3) Il vérifie le principe de récurrence, c'est-à-dire avec l'usage des quantificateurs :

$$\forall A \subseteq \mathbb{N}, \quad \left( (0 \in A) \text{ et } (\forall n \in \mathbb{N}, n \in A \implies n + 1 \in A) \right) \implies A = \mathbb{N}.$$

Dans l'égalité (1), on sous-entend que  $S(0) = 1, S(1) = 2, \dots$ . Les trois propriétés ci-dessus, qui caractérisent  $\mathbb{N}$ , sont connus sous le nom d'axiomes de Peano. Giuseppe Peano était un mathématicien et linguiste italien qui vécut de 1858 à 1932. Le principe de récurrence est souvent utilisé comme suit. Soit  $P$  un prédicat sur  $\mathbb{N}$ , c'est-à-dire une propriété qui, pour chaque entier naturel, peut être vraie ou fausse. Supposons que  $P(0)$  soit vraie et que la relation

$$P(n) \implies P(n + 1)$$

soit vraie pour tout  $n \in \mathbb{N}$ . Alors,  $P(n)$  est vraie pour tout  $n$ . On utilise parfois une variante de ce principe, qui consiste à établir  $P(0)$ , puis à prouver que pour tout  $n \in \mathbb{N}$ , la conjonction des relations  $P(0), \dots, P(n)$  implique  $P(n + 1)$ .

**Exemple 7.** Illustrons ce principe en démontrant que pour tout  $n \in \mathbb{N}$ , 169 divise  $3^{3n+3} - 26n - 27$ . Notons  $P(n)$  cette propriété. Elle est vraie si  $n = 0$ . Soit  $n \in \mathbb{N}$  tel que  $P(n)$  soit vraie. On a

$$3^{3(n+1)+3} - 26(n+1) - 27 - (3^{3n+3} - 26n - 27) = 26(3^{3n+3} - 1).$$

Par ailleurs, 13 divise  $3^3 - 1$  donc aussi  $3^{3(n+1)} - 1$ . Par suite, 169 divise  $26(3^{3n+3} - 1)$ . Parce que  $P(n)$  est vraie, il en est donc de même de  $P(n+1)$ , d'où l'assertion.

L'énoncé suivant est très utile en pratique.

**Proposition 2 (Construction par récurrence).** Soient  $E$  un ensemble,  $f : E \rightarrow E$  une application et  $x$  un élément de  $E$ . Il existe une unique application  $g : \mathbb{N} \rightarrow E$  telle que  $g(0) = x$  et que pour tout  $n \in \mathbb{N}$  on ait  $g(n+1) = f(g(n))$ .

On commence par établir le lemme suivant. Pour tout  $n \in \mathbb{N}$ , notons  $[0, n]$  les entiers  $k \in \mathbb{N}$  tels que  $0 \leq k \leq n$ .

**Lemme 4.** Pour tout  $n \in \mathbb{N}$ , il existe une unique application  $g_n : [0, n] \rightarrow E$  telle que  $g_n(0) = x$  et que pour tout  $k < n$  on ait  $g_n(k+1) = f(g_n(k))$ . De plus,  $g_{n+1}$  restreinte à  $[0, n]$  est  $g_n$ .

Démonstration : Soit  $P(n)$  la propriété d'existence et d'unicité de  $g_n$ . Elle est vraie pour  $n = 0$ . Soit  $n \in \mathbb{N}$  tel que  $P(n)$  soit vraie. Soit  $g_{n+1} : [0, n+1] \rightarrow E$  l'application définie par les conditions

$$g_{n+1}(k) = g_n(k) \quad \text{si } k \in [0, n] \quad \text{et} \quad g_{n+1}(n+1) = f(g_n(n)).$$

On a  $g_{n+1}(0) = x$ . Soit  $k$  un entier tel que  $k < n+1$ . Si  $k < n$ , on a  $k < k+1 \leq n$ , d'où

$$g_{n+1}(k+1) = g_n(k+1) = f(g_n(k)) = f(g_{n+1}(k)).$$

Par ailleurs, on a

$$g_{n+1}(n+1) = f(g_n(n)) = f(g_{n+1}(n)).$$

Cela prouve que l'application  $g_{n+1}$  vérifie la condition demandée. Il reste à vérifier son unicité. D'après le caractère d'unicité de  $P(n)$ , la restriction de  $g_{n+1}$  à  $[0, n]$  doit être  $g_n$ . Par ailleurs, on doit avoir  $g_{n+1}(n+1) = f(g_{n+1}(n))$ , d'où l'égalité  $g_{n+1}(n+1) = f(g_n(n))$  comme attendu et le résultat.

**Fin de démonstration de la proposition.** Reprenons les notations du lemme. Soit  $g : \mathbb{N} \rightarrow E$  l'application définie pour tout  $n \in \mathbb{N}$  par

$$g(n) = g_n(n).$$

On a les égalités

$$g(0) = g_0(0) = x \quad \text{et} \quad g(n+1) = g_{n+1}(n+1) = f(g_{n+1}(n)) = f(g_n(n)) = f(g(n)),$$

donc  $g$  satisfait la condition de l'énoncé. L'unicité de  $g$  résulte directement du principe de récurrence.

L'application  $g$  est une suite d'éléments de  $E$ . En posant  $g(n) = x_n$ , on dit que la suite  $(x_n)_{n \in \mathbb{N}}$  est définie par récurrence par les relations  $x_0 = x$  et  $x_{n+1} = f(x_n)$ .

On peut alors munir  $\mathbb{N}$  de trois lois de composition interne, c'est-à-dire d'applications  $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ , appelées addition, multiplication et exponentiation et notées respectivement

$$(a, b) \mapsto a + b, \quad (a, b) \mapsto a.b \text{ ou } ab, \quad (a, b) \mapsto a^b.$$

Elles sont définies par récurrence en posant

$$a + 0 = a \quad \text{et} \quad a + S(b) = S(a + b),$$

$$a.0 = 0 \quad \text{et} \quad a.S(b) = a.b + a,$$

$$a^0 = 1 \quad \text{et} \quad a^{S(b)} = a^b.a.$$

Par récurrence, l'addition est définie à partir de l'application  $S$  (celle notée  $f$  dans la proposition 2), la multiplication à partir de l'addition et l'exponentiation à partir de la multiplication. En particulier, on a

$$0^0 = 1.$$

### Remarques 6.

1) La notation  $n + 1$  pour désigner  $S(n)$  est compatible avec celle de l'addition. En effet, en partant de l'addition de  $n$  et de 1, on a

$$n + 1 = n + S(0) = S(n + 0) = S(n).$$

2) Étant entendu que  $S(2) = 3$  et que  $S(3) = 4$ , on a  $2 + (1 + 1) = 2 + S(1) = S(3) = 4$ , d'où  $2 + 2 = 4$ .

Par ailleurs,  $\mathbb{N}$  est muni de la relation d'ordre telle pour tous  $a, b \in \mathbb{N}$ , on a  $a \leq b$  s'il existe  $c \in \mathbb{N}$  tel que  $b = a + c$ . C'est un bon ordre, autrement dit :

**Proposition 3.** *Toute partie non vide de  $\mathbb{N}$  possède un plus petit élément.*

Démonstration : Soit  $X$  une partie de  $\mathbb{N}$ . Supposons qu'elle ne possède pas de plus petit élément. Soit  $A$  l'ensemble des minorants stricts de  $X$ , c'est-à-dire l'ensemble des

entiers  $n \in \mathbb{N}$  tels que pour tout  $m \in X$  on ait  $n < m$ . Démontrons que  $A = \mathbb{N}$ , ce qui entraînera que  $X$  est vide et le résultat. Parce que 0 est le plus petit élément de  $\mathbb{N}$ , il n'est pas dans  $X$ . On en déduit que 0 est dans  $A$ . Soit  $n \in \mathbb{N}$  tel que  $n$  soit dans  $A$ . Pour tout  $m \in X$  on a  $n < m$ , d'où  $n+1 \leq m$ . S'il existait  $m \in X$  tel que  $n+1 = m$ , alors  $n+1$  serait le plus petit élément de  $X$ , ce qui contredit l'hypothèse faite sur  $X$ . On a donc  $n+1 < m$  pour tout  $m \in X$ , d'où l'on déduit que  $n+1$  est dans  $A$ . D'après le principe de récurrence, on a donc  $A = \mathbb{N}$ .

**Remarque 7 (bon ordre).** Soit  $(E, \leq)$  un ensemble ordonné. On dit qu'il est bien ordonné, ou que la relation  $\leq$  est un bon ordre sur  $E$ , si toute partie non vide de  $E$  possède un plus petit élément. On peut démontrer que sur tout ensemble il existe un bon ordre (théorème de Zermelo, 1904). Cet énoncé est en fait équivalent à l'axiome du choix. Une des implications est facile à établir, car si  $E$  est bien ordonné, l'application  $\mathcal{P}(E) \setminus \{\emptyset\} \rightarrow E$  qui à  $X$  associe le plus petit élément de  $X$  est une fonction de choix sur  $E$ . En particulier, il existe sur  $\mathbb{R}$  un bon ordre (difficile d'en imaginer un). Le fait que  $\mathbb{N}$  soit bien ordonné, ce qui, on vient de le voir, est une conséquence du principe de récurrence, est à la base de toute l'arithmétique.

## 2. Notion de cardinal

Pour tous  $m$  et  $n$  dans  $\mathbb{N}$ , notons  $[m, n]$  l'ensemble des entiers  $k \in \mathbb{N}$  tels que l'on ait  $m \leq k \leq n$ . Si  $n < m$ , on a  $[m, n] = \emptyset$ . Un ensemble  $E$  est dit fini, s'il existe  $n \in \mathbb{N}$  tel que  $E$  soit en bijection avec  $[1, n]$ . S'il existe, un tel entier  $n$  est unique :

**Lemme 5.** Soient  $n$  et  $p$  des entiers naturels.

- 1) Il existe une injection de  $[1, n]$  dans  $[1, p]$  si et seulement si on a  $n \leq p$ .
- 2) Il existe une surjection de  $[1, n]$  sur  $[1, p]$  si et seulement si on a  $n \geq p > 0$  ou bien  $n = p = 0$ .
- 3) Il existe une bijection de  $[1, n]$  sur  $[1, p]$  si et seulement si on a  $n = p$ .

Démonstration : 1) Si on a  $n \leq p$ , l'application de  $[1, n]$  dans  $[1, p]$  qui à  $x$  associe  $x$  est injective.

Établissons l'implication réciproque par récurrence sur  $n$  et indépendamment de  $p$ . Notons  $P(n)$  la propriété affirmant que cette implication est vraie pour tout  $p$ . La propriété  $P(0)$  est vraie, car l'application  $[1, 0] \rightarrow [1, p]$  est injective et on a  $0 \leq p$ . Soit  $n \in \mathbb{N}$  tel que  $P(n)$  soit vraie. Vérifions que  $P(n+1)$  l'est aussi. Soit  $f : [1, n+1] \rightarrow [1, p]$  une injection.

Supposons  $f(n+1) = p$ . On a  $p > 0$  (sinon  $p = 0$ ,  $[1, p] = \emptyset$  or  $n+1 \neq 0$ ). Puisque  $f$  est injective, l'image de  $[1, n]$  par  $f$  est donc  $[1, p-1]$ . L'hypothèse de récurrence implique  $n \leq p-1$ , d'où  $n+1 \leq p$  et le résultat dans ce cas.

Supposons  $f(n+1) = a < p$ . Il existe une injection  $\tau : [1, p] \rightarrow [1, p]$  telle que  $\tau(x) = x$  si  $x \neq a, p$ ,  $\tau(a) = p$  et  $\tau(p) = a$ . L'application  $g = \tau \circ f : [1, n+1] \rightarrow [1, p]$  est une injection



et vérifie l'égalité  $g(n+1) = p$ . D'après l'alinéa précédent, on a donc  $n+1 \leq p$ , d'où le fait que  $P(n+1)$  soit vraie.

2) S'il existe une surjection de  $[1, n]$  sur  $[1, p]$ , alors il existe une injection de  $[1, p]$  dans  $[1, n]$  (prop. 1), d'où  $p \leq n$  (assertion 1). De plus, si  $p = 0$ , on a  $n = 0$ . Inversement, si  $n = p = 0$ , l'application vide de  $[1, n]$  dans  $[1, p]$  est surjective. Si on a  $n \geq p > 0$ , il existe une injection de  $[1, p]$  dans  $[1, n]$ , donc aussi une surjection de  $[1, n]$  sur  $[1, p]$  (prop. 1).

3) La troisième assertion est une conséquence des deux premières.

Si  $E$  fini, on dit que  $n$  est le cardinal de  $E$  et on notera  $|E| = n$ . Sinon, on dit que  $E$  est infini. Dans ce cas, on peut encore définir la notion de cardinal, de sorte que deux ensembles ont le même cardinal si et seulement si ils sont en bijection. On le note comme dans le cas fini  $|E|$ . On dit que le cardinal de  $E$  est inférieur à celui de  $F$  s'il existe une injection de  $E$  dans  $F$ . On note alors  $|E| \leq |F|$ . On verra plus loin que si on a  $|E| \leq |F|$  et  $|F| \leq |E|$ , alors  $|E| = |F|$  (théorème de Cantor-Bernstein).

**Définition 10.** On dit qu'un ensemble est dénombrable s'il est en bijection avec  $\mathbb{N}$ .

Un ensemble dénombrable est donc un ensemble dont on peut numéroter les éléments.

**Lemme 6.** Soit  $E$  un ensemble dénombrable.

1) Toute partie infinie de  $E$  est dénombrable.

2) L'image de  $E$  par une application est finie ou dénombrable.

Démonstration : On peut supposer  $E = \mathbb{N}$ .

1) Soit  $A$  une partie infinie de  $\mathbb{N}$ . Pour tout  $a \in A$ , notons  $[a+1, +\infty[$  l'ensemble des éléments de  $A$  supérieurs ou égaux à  $a+1$ . Le procédé de construction par récurrence, utilisé avec ses notations au moyen de l'élément  $x = \text{Min } A$  et de l'application  $f : A \rightarrow A$  définie par

$$f(n) = \text{Min}(A \cap [n+1, +\infty[),$$

entraîne l'existence d'une unique suite  $(a_n)_{n \in \mathbb{N}}$  d'éléments de  $A$  telle que

$$a_n = \text{Min}(A \setminus \{a_0, \dots, a_{n-1}\}).$$

Vérifions que l'application  $\mathbb{N} \rightarrow A$  qui à  $n$  associe  $a_n$  est une bijection. Si  $m \neq n$  on a  $a_m \neq a_n$ . Par ailleurs, soit  $a$  un élément de  $A$ . Procédons par l'absurde en supposant que pour tout  $n \in \mathbb{N}$  on ait  $a \neq a_n$ . Pour tout  $n \in \mathbb{N}$ ,  $a$  appartient donc à  $A \setminus \{a_0, \dots, a_{n-1}\}$ , d'où  $a_n \leq a$ . Puisque  $[0, a]$  est fini et que la suite  $(a_n)_{n \in \mathbb{N}}$  est infinie, on obtient une contradiction, d'où l'assertion.

2) Soit  $f : \mathbb{N} \rightarrow F$  une surjection. Il s'agit de vérifier que  $F$  est fini ou dénombrable. Pour tout  $x \in F$ ,  $f^{-1}(x)$  est une partie non vide de  $\mathbb{N}$ . Soit  $m(x)$  son plus petit élément. L'application  $m : F \rightarrow \mathbb{N}$  ainsi obtenu satisfait l'égalité  $f \circ m = \text{Id}_F$ . Par suite,  $m$  est

injective et  $m$  est donc une bijection de  $F$  sur son image  $m(F)$ . D'après la première assertion,  $m(F)$  est fini ou dénombrable, il en est donc de même de  $F$ .

**Exemples 8.** Voici des exemples classiques d'ensembles dénombrables :

1)  $\mathbb{N} \times \mathbb{N}$ , car par exemple l'application  $\mathbb{N}^2 \rightarrow \mathbb{N}$  qui à  $(a, b)$  associe  $2^a(2b+1) - 1$  est une bijection de  $\mathbb{N}^2$  sur  $\mathbb{N}$ . En effet, il est immédiat de vérifier que  $f$  est une injection. Par ailleurs si  $n$  est un entier naturel, il existe  $a$  et  $b$  dans  $\mathbb{N}$  tels que l'on ait  $n+1 = 2^a(2b+1)$  (cf. la décomposition d'un entier en facteurs premiers). Il en résulte que tout produit fini d'ensembles dénombrables est dénombrable.

2) L'ensemble  $\mathbb{Z}$ , car c'est un quotient de  $\mathbb{N}^2$  (voir le paragraphe 6 et le lemme 6).

3) Le corps  $\mathbb{Q}$  des nombres rationnels, car c'est un quotient de  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ . Il n'y a donc pas plus de rationnels que d'entiers relatifs, bien qu'il y ait déjà une infinité de rationnels dans l'intervalle  $[0, 1]$ .

4) L'ensemble des parties finies de  $\mathbb{N}$ , car l'application qui à une partie finie  $A$  de  $\mathbb{N}$  associe

$$\sum_{r \in A} 2^r,$$

est une bijection de cet ensemble sur  $\mathbb{N}$  (existence et unicité de l'écriture des entiers en base 2 et le fait qu'une somme vide soit nulle).

**Lemme 7.** *Soit  $E$  un ensemble infini. Il existe une injection de  $\mathbb{N}$  dans  $E$ .*

Démonstration : Supposons qu'il n'existe pas d'injection de  $\mathbb{N}$  dans  $E$ . D'après le théorème 3 (qui utilise l'axiome du choix), il existe alors une injection de  $E$  dans  $\mathbb{N}$ . Par suite,  $E$  est fini ou dénombrable (lemme 6), contradiction.

**Remarque 7.** On peut aussi établir le lemme 7 en considérant une fonction de choix  $\varphi : \mathcal{P}(E) \setminus \{\emptyset\} \rightarrow E$ . En effet, notons  $X$  l'ensemble des parties finies de  $E$  et considérons l'application  $f : X \rightarrow X$  définie par

$$f(A) = A \cup \{\varphi(E \setminus A)\}.$$

Elle est bien définie car  $E$  étant infini, pour tout  $A \in X$  la partie  $E \setminus A$  est non vide. D'après le principe de construction par récurrence, il existe une unique fonction  $g : \mathbb{N} \rightarrow X$  telle que  $g(0) = \emptyset$  et  $g(n+1) = f(g(n))$ . L'application  $h : \mathbb{N} \rightarrow E$  définie par

$$h(n) = \varphi(E \setminus g(n)),$$

est alors une injection de  $\mathbb{N}$  dans  $E$ .

**Corollaire 1.** Soit  $E$  un ensemble infini. Il existe un sous-ensemble de  $E$ , distinct de  $E$ , en bijection avec  $E$ .

Démonstration : Il existe une injection  $h : \mathbb{N} \rightarrow E$ . Soit  $f : E \rightarrow E \setminus \{h(0)\}$  l'application définie par les conditions suivantes. Posons

$$f(x) = x \quad \text{si} \quad x \notin h(\mathbb{N}).$$

Si  $x$  est dans  $h(\mathbb{N})$ , il existe un unique  $n \in \mathbb{N}$  tel que  $x = h(n)$  et on pose

$$f(x) = h(n+1).$$

L'application  $f$  est une bijection de  $E$  sur  $E \setminus \{h(0)\}$ .

Au sens de la théorie des cardinaux,  $|\mathbb{N}|$  est donc le plus petit infini possible. Il existe des cardinaux plus grands. Par exemple, on a  $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$  (th. 1). On a aussi  $|\mathbb{N}| < |\mathbb{R}|$  :

**Proposition 4.** L'ensemble  $\mathbb{R}$  n'est pas dénombrable.

Démonstration : Supposons  $\mathbb{R}$  dénombrable. Soit  $f : \mathbb{N} \rightarrow \mathbb{R}$  une bijection. Pour tout  $n \in \mathbb{N}$ , notons

$$f(n) = b_{n,0}, b_{n,1} b_{n,2} \cdots b_{n,k} b_{n,k+1} \cdots$$

le développement décimal propre de  $f(n)$ . Pour tout  $k \in \mathbb{N}$ , posons

$$u_k = 0 \quad \text{si} \quad b_{k,k} \neq 0 \quad \text{et} \quad u_k = 1 \quad \text{si} \quad b_{k,k} = 0.$$

Posons par ailleurs

$$x = u_0, u_1 u_2 \cdots u_n u_{n+1} \cdots$$

Pour tout  $n \in \mathbb{N}$ , on a  $f(n) \neq x$ , car le  $n+1$ -ième terme du développement décimal propre de  $f(n)$ , qui est  $b_{n,n}$ , est distinct de  $u_n$ , d'où une contradiction et le résultat.

**Remarque 8.** L'ensemble  $\mathbb{N}^{\mathbb{N}}$  des suites d'entiers naturels n'est pas dénombrable, pour la raison qu'il est en bijection avec  $\mathbb{R}$  (voir le paragraphe 7). On peut aussi le démontrer directement. En effet, supposons que l'on ait

$$\mathbb{N}^{\mathbb{N}} = \{f_0, f_1, \cdots, f_n, \cdots\},$$

où les  $f_i$  sont des applications de  $\mathbb{N}$  dans  $\mathbb{N}$  distinctes deux à deux. Soit  $f : \mathbb{N} \rightarrow \mathbb{N}$  l'application définie par

$$f(n) = 1 + f_n(n).$$

Il existe  $k \in \mathbb{N}$  tel que  $f = f_k$ , d'où  $f_k(k) = f(k) = 1 + f_k(k)$  et une contradiction.

En fait, d'après le théorème de Cantor (th. 1), il existe une infinité de cardinaux distincts. On dit qu'un ensemble a la puissance du continu s'il est en bijection avec  $\mathbb{R}$ . On a longtemps conjecturé que toute partie infinie de  $\mathbb{R}$  est dénombrable ou bien a la puissance du continu. On désignait cette assertion comme étant l'hypothèse du continu. En fait, cette hypothèse n'est ni vraie ni fausse. On ne peut pas la déduire des axiomes de la théorie des ensembles et si on l'accepte, elle n'entraîne pas de contradiction (cela a été établi par Gödel en 1938 et Cohen en 1963).

### 3. Analyse combinatoire

Elle concerne l'étude du calcul des cardinaux des ensembles finis.

**Proposition 5.** *Soient  $E$  et  $F$  des ensembles finis.*

- 1) *Si  $E$  et  $F$  sont disjoints, on a  $|E \cup F| = |E| + |F|$ .*
- 2) *On a  $|E \times F| = |E| \cdot |F|$ .*
- 3) *Soit  $F^E$  l'ensemble des applications de  $E$  dans  $F$ . Alors,  $F^E$  est fini et on a l'égalité  $|F^E| = |F|^{|E|}$ .*

Démonstration : 1) Posons  $|E| = n$ . On procède par récurrence sur le cardinal de  $F$ . Si  $|F| = 0$ ,  $F$  est vide et  $E \cup F = E$ . On a  $|E| = |E| + 0$ , donc l'égalité à établir est vraie dans ce cas. Posons  $|F| = p + 1$  où  $p \in \mathbb{N}$  et supposons l'assertion vraie pour tout ensemble  $F'$  de cardinal  $p$ . Il existe une bijection  $f : [1, p + 1] \rightarrow F$ . Posons  $c = f(p + 1)$ . La restriction de  $f$  à  $[1, p]$  est une bijection de  $[1, p]$  sur  $F' = F \setminus \{c\}$ . On a  $|F'| = p$  et d'après l'hypothèse de récurrence, on a  $|E \cup F'| = n + p$ . Il existe donc une bijection de  $[1, n + p]$  sur  $E \cup F'$ . En la prolongeant en une application  $g : [1, n + p + 1] \rightarrow E \cup F$  en posant  $g(n + p + 1) = c$ , on obtient une bijection de  $[1, n + p + 1]$  sur  $E \cup F$  car  $E$  et  $F$  sont disjoints, d'où le résultat.

2) Le produit cartésien  $E \times F$  est la réunion disjointe de  $E \times \{x\}$  où  $x$  parcourt  $F$ . Pour tout  $x \in F$ , le cardinal de  $E \times \{x\}$  est  $|E|$ . L'assertion 1 entraîne alors le résultat.

3) On établit cette assertion par récurrence sur  $|E|$  et en fixant  $F$ . Posons  $|F| = p$ . Considérons la propriété  $P(n)$  affirmant que pour tout ensemble  $E$  de cardinal  $n$ ,  $F^E$  est fini de cardinal  $p^n$ . Elle est vraie si  $n = 0$ , car il existe une unique application de  $\emptyset$  dans  $F$ . Elle est aussi vraie si  $n = 1$  par définition d'une application. Soit  $n$  un entier naturel non nul tel que  $P(n)$  soit vraie. Supposons  $|E| = n + 1$ . Il existe deux ensembles  $E'$  et  $E''$  respectivement de cardinal  $n$  et 1, tels que  $E$  soit la réunion disjointe de  $E'$  et  $E''$ . Les ensembles  $F^E$  et  $F^{E'} \times F^{E''}$  sont en bijection. D'après la seconde assertion et l'hypothèse de récurrence, on a donc

$$|F^E| = |F^{E'}| |F^{E''}| = p^n \cdot p = p^{n+1},$$

donc  $P(n + 1)$  est vraie.

**Corollaire 2 (Principe des Bergers).** Soient  $F$  un ensemble fini,  $f : E \rightarrow F$  une application et  $n$  un entier naturel. Supposons que pour tout  $y \in F$ , on ait  $|f^{-1}(y)| = n$ . Alors,  $E$  est fini et on a  $|E| = n|F|$ .

Démonstration : Si  $n = 0$ ,  $E$  est vide et l'énoncé est vrai. Supposons  $n \geq 1$ . Pour chaque  $y \in F$ , numérotons de 1 à  $n$  les éléments de  $f^{-1}(y)$ . L'application  $[1, n] \times F \rightarrow E$  qui à  $(i, y)$  associe le  $i$ -ème élément de  $f^{-1}(y)$  est une bijection, d'où l'assertion.

**Corollaire 3.** Soit  $E$  un ensemble de cardinal  $n$ . L'ensemble  $\mathcal{P}(E)$  est fini de cardinal  $2^n$ .

Démonstration : L'application de  $\mathcal{P}(E)$  à valeurs dans l'ensemble  $\{0, 1\}^E$  qui à une partie de  $E$  associe sa fonction caractéristique est une bijection.

Pour tous  $n$  et  $p$  dans  $\mathbb{N}$ , notons  $A(n, p)$  le nombre d'injections de  $[1, p]$  dans  $[1, n]$ .

**Proposition 6 (Nombre d'injections).** On a

$$A(n, p) = \prod_{0 \leq i < p} (n - i) = \begin{cases} \frac{n!}{(n-p)!} & \text{si } p \leq n \\ 0 & \text{sinon.} \end{cases}$$

Démonstration : La seconde égalité est immédiate. Vérifions la première par récurrence sur  $p$ . Elle est vraie si  $p = 0$ , car l'unique application de l'ensemble vide dans  $[1, n]$  est injective et le produit vide vaut 1. Supposons qu'elle soit vraie pour un entier  $p \in \mathbb{N}$ . Notons  $I$  (resp.  $I'$ ) l'ensemble des injections de  $[1, p+1]$  (resp.  $[1, p]$ ) dans  $[1, n]$ . Considérons l'application de restriction  $\varphi : I \rightarrow I'$ . Pour tout  $g \in I'$ ,  $\varphi^{-1}(g)$  est formée des  $f \in I$  qui ont même valeur que  $g$  sur  $[1, p]$ . Il y en a autant que de valeurs possibles pour  $f(p+1)$ , c'est-à-dire tout élément de  $[1, n]$  autre que  $g([1, p])$ . Il y en a donc  $n - p$ . Il résulte alors du principe des bergers et de l'hypothèse de récurrence que l'on a

$$A(n, p+1) = (n - p)A(n, p) = \prod_{0 \leq i < p+1} (n - i).$$

**Corollaire 4.** Le nombre de bijections d'un ensemble de cardinal  $n$  sur lui même est  $n!$ .

**Proposition 7 (Coefficients binomiaux).** Soient  $n$  et  $p$  des entiers tels que  $0 \leq p \leq n$ . Pour tout ensemble  $E$  de cardinal  $n$ , le nombre de parties de  $E$  de cardinal  $p$  est  $\frac{n!}{p!(n-p)!}$ .

De nos jours, on note (au lieu de  $C_n^p$ )

$$\binom{n}{p} = \frac{n!}{p!(n-p)!}.$$

Par convention, on pose  $\binom{n}{p} = 0$  si  $p > n$ . Quels soient  $n$  et  $p$ , l'entier  $\binom{n}{p}$  est donc le nombre de parties à  $p$  éléments dans un ensemble de cardinal  $n$ . On dit que  $\binom{n}{p}$  est le coefficient binomial d'indices  $n$  et  $p$ .

Démonstration : Soit  $p$  un entier naturel. Notons  $\mathcal{P}$  l'ensemble des parties de  $E$  de cardinal  $p$  et  $I$  l'ensemble des injections de  $[1, p]$  dans  $E$ . Pour tout  $f \in I$ ,  $f([1, p])$  est dans  $\mathcal{P}$ . Soit  $\varphi : I \rightarrow \mathcal{P}$  l'application définie par

$$\varphi(f) = f([1, p]).$$

Pour tout  $A \in \mathcal{P}$ ,  $\varphi^{-1}(A)$  est l'ensemble des injections de  $[1, p]$  dans  $A$  et il y en a  $p!$ . D'après le principe des bergers, on a donc

$$|I| = p!|\mathcal{P}|.$$

La proposition 6 entraîne alors le résultat.

**Lemme 8.** *Quels que soient  $n$  et  $p$  dans  $\mathbb{N}$ , on a*

$$\binom{n}{p} = \binom{n}{n-p} \text{ (si } p \leq n) \quad \text{et} \quad \binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}.$$

Démonstration : Soit  $E$  un ensemble de cardinal  $n$ . L'application  $A \mapsto E \setminus A$  est une bijection entre l'ensemble des parties de  $E$  de cardinal  $p$  et celui des parties de  $E$  de cardinal  $n - p$ , d'où la première égalité.

Soient  $E$  un ensemble de cardinal  $n + 1$ ,  $a$  un élément de  $E$ ,  $\mathcal{P}$  l'ensemble des parties de  $E$  de cardinal  $p + 1$  et  $\mathcal{P}'$  le sous-ensemble de  $\mathcal{P}$  formé des parties qui contiennent  $a$ . Posons  $\mathcal{P}'' = \mathcal{P} \setminus \mathcal{P}'$  et  $E' = E \setminus \{a\}$ . Par définition,  $\mathcal{P}''$  est l'ensemble des parties à  $p + 1$  éléments de  $E'$ , d'où

$$|\mathcal{P}''| = \binom{n}{p+1}.$$

Par ailleurs, l'application  $A \mapsto E' \cap A$  est une bijection de  $\mathcal{P}'$  sur l'ensemble des parties de cardinal  $p$  de  $E'$ . On a donc

$$|\mathcal{P}'| = \binom{n}{p}.$$

On obtient la seconde égalité car  $\mathcal{P}$  est la réunion disjointe de  $\mathcal{P}'$  et  $\mathcal{P}''$ .

La seconde égalité du lemme peut être utilisée pour calculer les coefficients  $\binom{n}{p}$ , en construisant ce qu'on appelle le triangle de Pascal. Il s'agit d'un tableau triangulaire dans lequel les lignes sont les entiers  $n = 0, 1, \dots$  et les colonnes les entiers  $p = 0, 1, \dots$ . Chaque

terme est la somme de celui qui exactement au-dessus et de celui qui à gauche de celui-là. Les cases vides contiennent la valeur 0. Il est souvent présenté sous la forme suivante.

	$p = 0$	$p = 1$	$p = 2$	$p = 3$	$p = 4$	$p = 5$	$p = 6$	$p = 7$	$p = 8$
$n = 0$	1								
$n = 1$	1	1							
$n = 2$	1	2	1						
$n = 3$	1	3	3	1					
$n = 4$	1	4	6	4	1				
$n = 5$	1	5	10	10	5	1			
$n = 6$	1	6	15	20	15	6	1		
$n = 7$	1	7	21	35	35	21	7	1	
$n = 8$	1	8	28	56	70	56	28	8	1

Rappelons la formule classique du binôme de Newton, qui sera démontrée dans le cours sur les anneaux. Pour tous  $a$  et  $b$  dans un anneau tels que  $ab = ba$  et tout  $n \in \mathbb{N}$ , on a

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

**Exemple 9.** Soient  $k$  et  $r$  des entiers naturels. Posons, pour tout  $n \in \mathbb{N}$ ,

$$S_k(n) = 1^k + 2^k + \cdots + n^k.$$

On a l'égalité

$$1 + \sum_{k=0}^{r-1} \binom{r}{k} S_k(n) = (n+1)^r.$$

En effet, on a

$$1 + \sum_{k=0}^{r-1} \binom{r}{k} S_k(n) = 1 + \sum_{j=1}^n \sum_{k=0}^{r-1} \binom{r}{k} j^k,$$

$$\sum_{k=0}^{r-1} \binom{r}{k} j^k = (j+1)^r - j^r,$$

d'où l'égalité annoncée. On en déduit par exemple que l'on a

$$S_1(n) = \frac{n(n+1)}{2}, \quad S_2(n) = \frac{n(n+1)(2n+1)}{6}, \quad S_3(n) = S_1(n)^2.$$

En particulier, la somme des cubes des  $n$  premiers entiers est un carré.

## 6. Relations d'équivalence

Soit  $E$  un ensemble.

**Définition 11.** Une relation d'équivalence sur  $E$  est une relation binaire  $\mathcal{R}$  sur  $E$  telle que pour tous  $x, y, z$  dans  $E$ , les conditions suivantes soient remplies :

- 1) on a  $x\mathcal{R}x$  (réflexivité).
- 2) La relation  $x\mathcal{R}y$  implique  $y\mathcal{R}x$  (symétrie).
- 3) Si  $x\mathcal{R}y$  et  $y\mathcal{R}z$ , alors  $x\mathcal{R}z$  (transitivité).

Soit  $\mathcal{R}$  une relation d'équivalence sur  $E$ . On appelle graphe de  $\mathcal{R}$  l'ensemble des couples  $(x, y) \in E \times E$  tels que l'on ait  $x\mathcal{R}y$ . Pour tout  $x \in E$ , la classe d'équivalence de  $x$  modulo  $\mathcal{R}$ , ou plus simplement, la classe de  $x$  modulo  $\mathcal{R}$ , est l'ensemble des  $y \in E$  tels que l'on ait  $x\mathcal{R}y$ . L'ensemble des classes d'équivalence de  $E$  modulo  $\mathcal{R}$  est appelé l'ensemble quotient de  $E$  modulo  $\mathcal{R}$ , on le note parfois  $E/\mathcal{R}$ . On dispose de l'application  $s : E \rightarrow E/\mathcal{R}$  qui à tout  $x \in E$  associe sa classe modulo  $\mathcal{R}$ . On l'appelle la surjection canonique. Quels que soient  $x, y$  dans  $E$ , on a  $x\mathcal{R}y$  si et seulement si  $s(x) = s(y)$ . L'ensemble des classes d'équivalence de  $E$  modulo  $\mathcal{R}$  forme une partition de  $E$  (une partition de  $E$  est un ensemble de parties non vides de  $E$ , deux à deux disjointes, dont la réunion est  $E$ ). En fait, l'ensemble des partitions de  $E$  et l'ensemble des relations d'équivalence sur  $E$  sont en bijection.

### 6.1. Relation d'équivalence associée à une application

Soit  $f : E \rightarrow F$  une application. Prenons pour  $\mathcal{R}$  la relation suivante : pour tout  $(x, y) \in E \times E$ , on a

$$x\mathcal{R}y \iff f(x) = f(y).$$

C'est une relation d'équivalence sur  $E$ , appelée la relation d'équivalence associée à  $f$ . Toute relation d'équivalence sur  $E$  est associée à une application, à savoir la surjection canonique correspondante. Il existe une unique application  $\bar{f} : E/\mathcal{R} \rightarrow F$  telle que l'on ait  $\bar{f} \circ s = f$ . C'est une bijection de  $E/\mathcal{R}$  sur  $f(E)$ .

### 6.2. L'ensemble $\mathbb{Z}$ des entiers relatifs

Construisons l'ensemble  $\mathbb{Z}$  des entiers relatifs à partir de  $\mathbb{N}$ . Pour cela, on définit sur  $\mathbb{N} \times \mathbb{N}$  la relation d'équivalence  $\mathcal{R}$  telle que l'on ait

$$(x, y)\mathcal{R}(x', y') \iff x + y' = y + x'.$$

On pose par définition

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\mathcal{R}.$$

On appelle entier relatif, ou entier rationnel, tout élément de  $\mathbb{Z}$ . Il reste à définir les opérations algébriques usuelles sur  $\mathbb{Z}$  et à montrer que  $\mathbb{N}$  s'identifie canoniquement à un



sous-ensemble de  $\mathbb{Z}$ . Soit  $s : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}$  la surjection canonique. On définit la somme et le produit de deux entiers relatifs

$$z = s((x, y)) \quad \text{et} \quad z' = s((x', y'))$$

par les formules

$$z + z' = s((x + x', y + y')) \quad \text{et} \quad zz' = s((xx' + yy', xy' + x'y)).$$

Il s'agit de vérifier qu'elles sont bien définies i.e. qu'elles ne dépendent pas des représentants choisis de  $z$  et  $z'$  : soient  $(u, v)$  et  $(u', v')$  dans  $\mathbb{N} \times \mathbb{N}$  tels que l'on ait

$$(x, y)\mathcal{R}(u, v) \quad \text{et} \quad (x', y')\mathcal{R}(u', v').$$

On a alors  $x + v = y + u$  et  $x' + v' = y' + u'$ , d'où

$$x + x' + v + v' = y + y' + u + u'$$

i.e.  $s((x + x', y + y')) = s((u + u', v + v'))$ . De plus, on a

$$xx' + yy' + uv' + u'v = xy' + x'y + uu' + vv'.$$

En effet, on a

$$\begin{aligned} (x + v)x' + (y + u)y' &= (y + u)x' + (x + v)y', \\ (x' + v')u + (y' + u')v &= (y' + u')u + (x' + v')v. \end{aligned}$$

En sommant ces deux égalités, on obtient

$$xx' + yy' + uv' + u'v + (x'v + uy' + x'u + y'v) = xy' + x'y + uu' + vv' + (x'v + uy' + x'u + y'v),$$

d'où l'assertion en simplifiant.

On vérifie ensuite que la somme et le produit de deux éléments de  $\mathbb{Z}$  vérifient les propriétés attendues de ces opérations, commutativité, associativité, existence d'un élément neutre qui n'est autre que la classe de  $(0, 0)$ . Par ailleurs, l'application  $\mathbb{N} \rightarrow \mathbb{Z}$  qui à  $n \in \mathbb{N}$  associe la classe d'équivalence du couple  $(n, 0)$  est injective et est compatible avec la définition des opérations algébriques sur  $\mathbb{N}$  et  $\mathbb{Z}$ . On peut donc identifier  $\mathbb{N}$  à un sous-ensemble de  $\mathbb{Z}$  et convenir de poser pour tout  $n \in \mathbb{N}$ ,

$$n = s((n, 0)).$$

Tout élément  $x = s((a, b)) \in \mathbb{Z}$  admet un représentant de la forme  $(n, 0)$  ou  $(0, n)$ . En effet, si  $b \geq a$ , il existe  $c \in \mathbb{N}$  tel que  $b = a + c$ , et on a  $(a, b)\mathcal{R}(0, c)$ . De même, si  $a \geq b$  en écrivant que  $a = b + c$ , on obtient  $(a, b)\mathcal{R}(c, 0)$ . Les égalités

$$s((n, 0)) + s((0, n)) = s((0, 0))$$

entraînent alors que tout entier relatif a un opposé. De plus, pour tout  $x \in \mathbb{Z}$ , en notant  $-x$  l'opposé de  $x$ , l'un des éléments  $x$  et  $-x$  est dans  $\mathbb{N}$ , d'où l'égalité habituelle

$$\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}.$$

On munit ensuite  $\mathbb{Z}$  d'une structure d'ensemble ordonné au moyen de celle rappelée dans les exemples 4.

### 6.3. L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$

Soit  $n$  un entier naturel. La relation binaire sur  $\mathbb{Z}$  définie par

$$x\mathcal{R}y \iff n \text{ divise } x - y,$$

est une relation d'équivalence. Si on a  $x\mathcal{R}y$ , on dit que  $x$  et  $y$  sont congrus modulo  $n$  et l'on écrit que l'on a la congruence  $x \equiv y \pmod{n}$ . Pour tout  $x \in \mathbb{Z}$ , la classe de  $x$  modulo  $n\mathbb{Z}$  est

$$\{x + nk \mid k \in \mathbb{Z}\}.$$

On la note souvent  $x + n\mathbb{Z}$ , ou  $\bar{x}$  lorsque que l'entier  $n$  est sous-entendu. On dit aussi que c'est la classe de  $x$  modulo  $n$ . L'ensemble  $\mathbb{Z}/n\mathbb{Z}$  est formé des classes d'équivalence modulo  $n$ . On dispose de la surjection canonique  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  qui à un entier  $a$  associe sa classe modulo  $n$ . Dans le cas où  $n = 0$ , et dans ce cas seulement, c'est une bijection.

**Lemme 9.** *Supposons  $n \geq 1$ . Alors,  $\mathbb{Z}/n\mathbb{Z}$  est fini de cardinal  $n$  et on a*

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Démonstration : C'est une conséquence du théorème de la division euclidienne (voir le chapitre suivant). Considérons en effet un élément  $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$  où  $a \in \mathbb{Z}$ . Il existe des entiers  $q$  et  $r$  tels que l'on ait  $a = nq + r$  avec  $0 \leq r < n$ . Puisque  $a - r \in n\mathbb{Z}$ , on a donc  $\bar{a} = \bar{r}$ . Par ailleurs, quels que soient  $a$  et  $b$  distincts compris entre 0 et  $n - 1$ , l'entier  $n$  ne divise pas  $a - b$ , autrement dit, on a  $\bar{a} \neq \bar{b}$ , d'où le résultat.

## 7. Théorème de Cantor-Bernstein

**Théorème 6 (Cantor-Bernstein).** *Soient  $E$  et  $F$  des ensembles. Supposons qu'il existe une injection de  $E$  dans  $F$  et une injection de  $F$  dans  $E$ . Alors, il existe une bijection de  $E$  sur  $F$ .*

Démonstration : Elle utilise le lemme suivant :

**Lemme 10.** *Toute application croissante de  $\mathcal{P}(E)$  dans  $\mathcal{P}(E)$  (pour l'inclusion) admet un point fixe.*

Démonstration : Soit  $u : \mathcal{P}(E) \rightarrow \mathcal{P}(E)$  une telle application. Posons

$$S = \left\{ A \in \mathcal{P}(E) \mid A \subseteq u(A) \right\} \quad \text{et} \quad M = \bigcup_{A \in S} A.$$

Démontrons que  $u(M) = M$ . Pour tout  $A \in S$ , vu que  $A$  est contenu dans  $M$  et que  $u$  est croissante, on a les inclusions  $A \subseteq u(A) \subseteq u(M)$ , ce qui entraîne que  $M$  est contenu dans  $u(M)$ . Par ailleurs,  $u$  étant croissante,  $u(M)$  est aussi contenu dans  $u(u(M))$ , donc  $u(M)$  est dans  $S$ . Il en résulte que  $u(M)$  est contenu dans  $M$ , d'où le résultat.

**Démonstration du théorème :** Soient  $f$  une injection de  $E$  dans  $F$  et  $g$  une injection de  $F$  dans  $E$ . Considérons l'application  $u : \mathcal{P}(E) \rightarrow \mathcal{P}(E)$  définie par

$$u(A) = E - g(F - f(A)).$$

Si on  $A \subseteq B$ , alors  $f(A) \subseteq f(B)$ , d'où  $F - f(B) \subseteq F - f(A)$  puis  $u(A) \subseteq u(B)$  i.e.  $u$  est croissante. Il existe donc  $M \in \mathcal{P}(E)$  tel que  $u(M) = M$ . On a ainsi

$$(2) \quad E - M = g(F - f(M)).$$

Soit alors  $h : E \rightarrow F$  l'application définie comme suit. Si  $x$  est dans  $M$ , on pose

$$h(x) = f(x).$$

Si  $x$  n'est pas dans  $M$ , d'après (2) et le fait que  $g$  soit une injection, il existe  $y \in F - f(M)$  unique tel que  $x = g(y)$ . On pose alors

$$h(x) = y.$$

C'est une bijection de  $E$  sur  $F$ , d'où le résultat.

Voyons quelques conséquences de ce théorème.

1) L'ensemble  $\mathcal{P}(\mathbb{N})$  à la puissance du continu. Posons  $I = ]0, 1[$ . Soit  $g : \mathcal{P}(\mathbb{N}) \rightarrow I$  l'application qui à une partie non vide  $A$  de  $\mathbb{N}$  associe

$$g(A) = 0, s_0 s_1 \cdots s_n s_{n+1} \cdots,$$

où  $s_n = 1$  si  $n \in A$  et  $s_n = 0$  sinon. On pose  $g(\emptyset) = \frac{1}{2}$ . C'est une injection d'après l'unicité du développement décimal propre d'un nombre réel. Par ailleurs, l'application

$f : I \rightarrow \mathcal{P}(\mathbb{N})$  définie pour tout  $r = 0, r_1 r_2 \cdots r_n r_{n+1} \cdots$  (le développement décimal propre de  $r$ ), par

$$f(r) = \left\{ 2^{r_1}, 3^{r_2}, \dots, p_n^{r_n}, \dots \right\},$$

où  $p_n$  est le  $n$ -ième nombre premier, est une injection. Il en résulte que  $I$  et  $\mathcal{P}(\mathbb{N})$  sont en bijection. Par ailleurs,  $I$  est en bijection avec  $\mathbb{R}$ . En effet, vérifions que la fonction  $f : I \rightarrow \mathbb{R}$  définie par

$$f(x) = -\frac{1}{x} - \frac{1}{x-1}$$

est une bijection. C'est une fonction continue sur  $I$ , donc  $f(I)$  est un intervalle de  $\mathbb{R}$ . La fonction  $f$  est dérivable sur  $I$  et pour tout  $x \in I$ , on a  $f'(x) > 0$ . Ainsi,  $f$  est strictement croissante sur  $I$ , donc est injective. Par ailleurs,  $f(I)$  n'est pas majoré ni minoré, car on a

$$\lim_{\substack{x \rightarrow 0 \\ >}} f(x) = -\infty \quad \text{et} \quad \lim_{\substack{x \rightarrow 1 \\ <}} f(x) = +\infty.$$

On a donc  $f(I) = \mathbb{R}$ , d'où notre assertion.

2) Retrouvons le fait que les ensembles  $\mathcal{P}(\mathbb{N})$  et  $\mathbb{N}^{\mathbb{N}}$  sont en bijection. L'application  $\mathcal{P}(\mathbb{N}) \rightarrow \mathbb{N}^{\mathbb{N}}$  qui à  $A \in \mathcal{P}(\mathbb{N})$  associe la fonction caractéristique de  $A$  est une injection. Inversement, l'application  $g : \mathbb{N}^{\mathbb{N}} \rightarrow \mathcal{P}(\mathbb{N})$  définie pour toute suite  $(u_n)_{n \in \mathbb{N}}$  de  $\mathbb{N}^{\mathbb{N}}$  par

$$g(u) = \left\{ 2^{u_0}, 3^{u_1}, \dots, p_n^{u_{n-1}}, \dots \right\}$$

où  $p_n$  est le  $n$ -ième nombre premier, est une injection.

3) Le produit cartésien  $\mathbb{R} \times \mathbb{R}$  est en bijection avec  $\mathbb{R}$ . Il n'y a donc pas plus de points dans un plan que sur une droite. En effet, d'après ce qui précède  $\mathbb{R}$  est en bijection avec  $\mathbb{N}^{\mathbb{N}}$ . Par ailleurs,  $\mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$  est en bijection avec  $\mathbb{N}^{\mathbb{N}}$  via l'application d'entrelacement

$$((x_i), (y_i)) \mapsto (x_0, y_0, x_1, y_1, \dots).$$