5 Équivalence et Ordres

Dans cette partie on considère une relation binaire R sur un ensemble A à la fois comme domaine et comme image, soit un sous ensemble de $A \times A$.

5.1 Définitions

On définit ici les principales propriétés des relations binaires.

Définition 1 (Propriétés d'une relation) *On introduit les propriétés suivantes pour une relation.*

Réflexivité
R *est* réflexive *ssi* $\forall x \in A, R(x,x)$

Transitivité
R *est* transitive *ssi* $\forall x\ y\ z \in A, R(x,y) \Rightarrow R(y,z) \Rightarrow R(x,z)$

Symétrie
R *est* symétrique *ssi* $\forall x\ y \in A, R(x,y) \Rightarrow R(y,x)$

Irreflexivité
R *est* irréflexive $\forall x \in A, \neg R(x,x)$

Anti-symétrie
R *est* anti-symétrique $\forall x\ y \in A, R(x,y) \Rightarrow R(y,x) \Rightarrow x = y$

Exemple 1

- *La relation d'égalité est réflexive, transitive et symétrique.*
- *La relation* $n \leq m$ *sur les entiers est réflexive, transitive et anti-symétrique.*
- *La relation stricte* $n < m$ *sur les entiers est transitive, irréflexive et antisymétrique.*

5.2 Equivalence

Définition 2 (Relation d'équivalence) *Un relation est une* relation d'équivalence *si elle est réflexive, symétrique et transitive.*

L'égalité est une relation d'équivalence et nous allons montrer qu'une relation d'équivalence peut servir d'égalité.

Exemple 2 *On peut définir une relation sur les couples d'entiers* $\mathbb{N}\times\mathbb{N}$ *par :*

$$\stackrel{def}{=}$$

$$(n_1,m_1) \equiv (n_2,m_2) \quad = \quad n_1+m_2=n_2+m_1$$

D'un point de vue géométrique, les couples (n_1,m_1) et (n_2,m_2) sont équivalents si les différences n_1-m_1 et n_2-m_2 sont égales.

On montre aisément que c'est une relation d'équivalence, la seule difficulté est la transitivité : si $(n_1,m_1) \equiv (n_2,m_2)$ et $(n_2,m_2) \equiv (n_3,m_3)$ alors par définition $n_1+m_2=n_2+m_1$ et $n_2+m_3=n_3+m_2$. On a alors $n_1+m_2+n_3=n_2+m_1+n_3$ donc $n_1+n_2+m_3=n_2+m_1+n_3$ et donc $n_1+m_3=m_1+n_3$ donc $(n_1,m_1) \equiv (n_3,m_3)$.

On peut regrouper tous les éléments de A qui sont équivalents entre eux.

Définition 3 (Classe d'équivalence) *Soit R une relation d'équivalence sur A. Une classe d'équivalence pour R est un ensemble C non vide tel que $\forall x \in C, \forall y \in A, y \in C \Leftrightarrow R(x,y)$.*
Soit $x \in A$, l'ensemble $\{y \in A \mid R(x,y)\}$ est une classe d'équivalence (appelée la classe d'équivalence pour R de x).

Exercice 1 *Donner les classes d'équivalence de $(0,1)$ et $(1,0)$ pour l'équivalence de l'exemple 2.*

5.2.1 Partition

Deux classes d'équivalence sont soit égales, soit disjointes et chaque élément de A appartient à une classe d'équivalence (la sienne). On dit qu'elles forment une *partition* de l'ensemble A.

Définition 4 (Partition) *Soit P un ensemble de parties de A (c'est-à-dire $P \subseteq \wp(A)$). On dit que P est une partition de A si tous les éléments de P sont non vides, disjoints 2 à 2 et couvrent tout l'ensemble A.*

- $\forall Y \in P, Y \neq \emptyset$
- $\forall Y_1\ Y_2 \in P, Y_1 \neq Y_2 \Rightarrow Y_1 \cap Y_2 = \emptyset$,
- $A = \cup P$

Exemple 3 *Dans une classe mixte d'étudiants, Soit X le sous-ensemble des filles et Y le sous-ensemble des garçons alors $\{X;Y\}$ forme une partition de l'ensemble des étudiants. Si on prend le sous-ensemble N de ceux qui font de la natation et le sous-ensemble B de ceux qui font du basket, en général $\{B;N\}$ ne sera pas une partition (certains étudiants peuvent ne pratiquer aucune de ces activités ou au contraire en pratiquer 2).*

Proposition 1 *Soit une relation d'équivalence R sur A. Soit X l'ensemble des classes d'équivalence de R défini par :*

$$X \overset{def}{=} \{C \in \wp(A) \mid C \text{ classe d'équivalence de } R\}$$

alors X forme une partition de A.

Preuve: *Les classes d'équivalence sont non vides par définition. Chaque élément $x \in A$ appartient à la classe d'équivalence de x et donc à $\cup X$. Soient deux classes C_1 et C_2, montrons que si elles ont un élément commun alors elles sont égales. Supposons qu'il existe $x \in C_1 \cap C_2$. Soit $y \in C_1$ alors on a $R(x,y)$ car $x \in C_1$ donc on a aussi $y \in C_2$ car $x \in C_2$ et $R(x,y)$ donc $C_1 \subseteq C_2$. De manière symétrique on a aussi $C_2 \subseteq C_1$, donc $C_1 = C_2$.* □

De manière réciproque, si on se donne une partition P d'un ensemble A alors on peut définir une relation d'équivalence R de A telle que la partition P corresponde au découpage en classes d'équivalence de R. Il suffit de poser :

$$R(x,y) \overset{def}{=} \exists C \in P, x \in C \wedge y \in C$$

On vérifie que c'est bien une relation d'équivalence.

5.2.2 Espace quotient

Lorsqu'une équivalence R sur un ensemble A est définie, on souhaite identifier les éléments qui sont équivalents. On s'intéresse à l'ensemble des classes d'équivalence que l'on appelle l'*espace quotient* de l'espace A par la relation R et on le note $A/_R$. Un élément de cet ensemble correspond à un sous-ensemble de A d'objets équivalents entre eux. Pour chaque élément C de $A/_R$, il existe $x \in A$ tel que C est la classe d'équivalence de x, mais ce x n'est pas unique: C est aussi la classe d'équivalence de y pour tout y tel que $R(x,y)$.

Exemple 4

- *L'ensemble des entiers relatifs $\mathbb{Z}$ peut se construire à partir de $\mathbb{N}$ comme l'espace quotient de $\mathbb{N}\times\mathbb{N}$ par la relation introduite précédemment.*
- *De même l'ensemble des rationnels se construit comme l'espace quotient de $\mathbb{Z}\times \mathbb{N}^*$ par la relation $(p_1,q_1) \equiv (p_2,q_2) \overset{def}{=} p_1q_2=q_1 p_2$*

Application compatible avec une équivalence.

Soit A un ensemble et R une relation d'équivalence sur A. On veut construire une application f de $A/_R$ dans X. Comme pour les autres applications, si $a=b$ alors $f(a)=f(b)$. Comme $a,b \in A/_R$, a et b sont des classes d'equivalence. Si on prend un représentant dans A de a (noté x) et un représentant dans A de b (noté y), on n'a pas forcément $x=y$, mais on sait que $R(x,y)$. Si on calcule la valeur de $f(a)$ à partir d'un représentant x de a en utilisant une application $g \in A \to X$ alors on doit s'assurer que $\forall\, x\ y \in A, R(x,y) \Rightarrow g(x)=g(y)$.

Ceci nous donne un principe de construction d'application dont le domaine est un ensemble quotient.

Proposition 2 *Soit g une application de $A \to X$ telle que $\forall\, x\ y \in A, R(x,y) \Rightarrow g(x)=g(y)$, alors il existe une unique application $f \in A/_R \to X$ telle que $\forall\, a \in A/_R, \forall\, x \in a, f(a)=g(x)$*

Exemple 5 *Si on considère les entiers relatifs représentés comme des couples d'entiers, on peut définir l'opération opposée par $opp(n,m)=(m,n)$ qui est une application de $\mathbb{N}\times\mathbb{N} \to \mathbb{N}\times\mathbb{N}$.*

On vérifie que si $(n_1,m_1)\equiv(n_2,m_2)$ alors par définition de l'équivalence, on a $n_1+m_2=m_1+n_2$ et donc $opp(n_1,m_1)\equiv opp(n_2,m_2)$

Si $\mathbb{Z} \overset{def}{=} \mathbb{N}\times\mathbb{N}/_{\equiv}$ alors on introduit opp_1 une application de $\mathbb{N}\times \mathbb{N} \to \mathbb{Z}$ en associant à (n,m) la classe d'équivalence de $opp(n,m)$. On a alors si $(n_1,m_1)\equiv(n_2,m_2)$ alors $opp_1(n_1,m_1)\equiv opp_1(n_2,m_2)$. On peut alors passer au quotient pour construire une application de $\mathbb{Z}\to\mathbb{Z}$.

Ce principe est important en informatique, en effet lorsque l'on représente une notion avancée dans un ordinateur, on doit souvent utiliser une représentation concrète (sous forme de terme par exemple). Il est courant que l'égalité sur la représentation concrète soit différente de l'égalité *mathématique* que l'on souhaite modéliser.

Par exemple, si on représente des rationnels en machine, on utilisera deux entiers pour le numérateur et le

dénominateur. Mais on peut alors avoir plusieurs représentations pour le même objet : (1,2), (8,16)…

De même un ensemble fini peut se représenter par une séquence, mais plusieurs séquences peuvent représenter le même ensemble : [1;2], [2;1;1] …

On peut parfois trouver des représentations *canoniques* par exemple dans le cas des rationnels, demander que numérateur et dénominateur n'aient pas de facteur commun (on dit que la fraction est irréductible), ou bien dans le cas des ensembles, demander que la séquence soit ordonnée avec un ordre total strict. Néanmoins ce n'est pas toujours le meilleur choix d'un point de vue informatique, car maintenir la contrainte d'être irréductible ou d'être trié nécessite des opérations supplémentaires (après une addition, ou une union par exemple) qui peuvent être trop coûteuses. On peut donc se contenter que les opérations programmées respectent bien la relation d'équivalence sur la représentation qui correspond à l'égalité de la notion mathématique que l'on souhaite modéliser.

Exercice 2 (Construction de $\mathbb{Q}$)
Soit $E=\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ on définit la relation $(a,b)\equiv(c,d) \stackrel{def}{=} ad=bc$.

1. *Montrer que $\equiv$ est une relation d'equivalence sur E.*
2. *Quelle est la classe d'équivalence de (0,1) ? de (1,1) ?*
3. *Soit les applications `plus` et `mult` dans $E \times E \to E$ définies par :*
   $$\texttt{plus}((a,b),(c,d))=(ad+bc,bd) \qquad \texttt{mult}((a,b),(c,d))=(ac,bd)$$
   Montrer que ces applications sont compatibles avec la relation $\equiv$.
4. *Montrer que pour tout a, b et c dans E, on a*
   $$\texttt{mult}(\texttt{plus}(a,b),c)\equiv \texttt{plus}(\texttt{mult}(a,c),\texttt{mult}(b,c))$$
5. *(Optionnel) Soit la fonction `inv` de E dans E définie par :*
   $$\texttt{inv}((a,b))=(b,a)$$
   - *Quel est l'ensemble de définition de `inv` ?*
   - *Montrer que $\forall x\in E, x\not\equiv(0,1) \Rightarrow \texttt{mult}(x,\texttt{inv}(x))\equiv(1,1)$*

5.3 Construction d'ordres

5.3.1 Définitions générales sur les ordres

Définition 5 (Ordre) *Une relation binaire est un pre-ordre si elle est transitive et anti-symétrique. C'est un ordre si elle est de plus réflexive. Un ordre strict est un pre-ordre qui est de plus irréflexif.*

Définition 6 (Ensemble ordonné) *Un ensemble ordonné est un couple $(E,\leq)$ avec $\leq$ une relation d'ordre sur E.*

Exemple 6

- *La relation usuelle $n \leq m$ sur les entiers est un ordre (on peut le vérifier pour les différentes définitions que ce soit par un système d'inférence ou bien en utilisant l'addition)*
- *Un même ensemble peut être muni de plusieurs ordres, par exemple sur les entiers on peut considérer l'ordre $n \leq m$ si n divise m.*
- *La relation $P \subseteq Q$ sur les ensembles est un ordre.*
- *Si R est un ordre alors la relation inverse R^{-1} est aussi un ordre.*

Définition 7 (Ordre strict associé à un ordre) *Si on se donne une relation d'ordre $\leq$ sur un ensemble A alors on peut définir l'ordre strict associé par $x<y \stackrel{def}{=} x \leq y \wedge x\neq y$ qui est une relation irreflexive et*

transitive.

Un ordre peut être *total* s'il permet de comparer deux éléments différents quelconques de A, il est dit *partiel* dans le cas contraire.

Définition 8 (Ordre total, partiel) *Un ordre est* total *ssi* $\forall x\ y, (x \leq y \vee y \leq x)$. *Un ordre qui n'est pas total est dit* partiel.

Exemple 7 *L'ordre usuel sur les entiers est total, celui d'inclusion sur les ensembles est partiel car par exemple* $\{1,2\}$ *et* $\{2,3\}$ *sont incomparables*.

Exercice 3 (Ordre préfixe sur les mots) *On définit une relation* $m_1 < m_2$ *sur les mots si* m_1 *est un préfixe de* m_2, *c'est-à-dire que le mot* m_2 *commence par le mot* m_1.

1. *Proposer une formule logique correspondant à la relation* $m_1 < m_2$.
2. *Montrer que* $m_1 < m_2$ *est un ordre*.
3. *Cet ordre est-il total ou partiel?*

Définition 9 (Application monotone) *Soient deux ensembles ordonnés* $(A_1,\leq_1)$ *et* $(A_2,\leq_2)$ *et une application* $f \in A_1 \to A_2$. *On dit que* f *est* monotone *si et seulement si*

$$\forall x\ y, x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$$

f *est* strictement monotone *si et seulement si*

$$\forall x\ y, x <_1 y \Rightarrow f(x) <_2 f(y)$$

ou de manière équivalente si elle est monotone et que de plus

$$\forall x\ y, x \neq y \Rightarrow f(x) \neq f(y)$$

Une suite monotone *d'éléments d'un ensemble ordonné* $(A,\leq)$ *est une application monotone de* $(\mathbb{N},\leq)$ *dans* $(A,\leq)$.

5.3.2 Diagramme de Hasse

Une relation binaire R sur un ensemble fini A peut se représenter graphiquement en représentant les éléments de A par des points et en mettant une flèche de x à y lorsque $R(x,y)$.

Dans le cas d'un ordre, certaines flèches sont obligatoires (reflexivité, transitivité). Pour simplifier le diagramme, on peut donc les ignorer. Formellement, cela revient à définir une relation *successeur* $S(x,y)$ associée à une relation d'ordre.

$$S(x,y) \stackrel{def}{=} R(x,y) \wedge x \neq y \wedge \forall\ z, R(x,z) \wedge R(z,y) \Rightarrow (z=x \wedge z=y)$$

Le diagramme de Hasse d'un ordre R est la représentation graphique de la relation successeur S. Cette relation détermine de manière unique la relation R comme la plus petite relation reflexive et transitive qui contient S.

5.3.3 Majorants et minorants

Lorsqu'on a une relation d'ordre sur un ensemble, il est intéressant de considérer les éléments les plus grands ou bien les plus petits.

Définition 10 (Majorants) *Soit* $X \subseteq A$, *on appelle ensemble des majorants de* X *dans* A, *l'ensemble des éléments de* A *qui sont plus grands que tous les élements de* X, *c'est-à-dire :*

$$\mathtt{maj}(X)=\{x \in A \mid \forall y \in X, y \leq x\}$$

On définit de même l'ensemble des minorants :

$$\mathtt{min}(X)=\{x \in A \mid \forall y \in X, x \leq y\}$$

Exemple 8 *L'ensemble des entiers impairs n'a pas de majorant dans $\mathbb{N}$ mais admet $\{0;1\}$ comme ensemble de minorants. L'ensemble des majorants et des minorants de l'ensemble vide est égal à l'espace A tout entier.*

Il faut noter que l'ensemble des majorants de X peut contenir des éléments qui ne sont pas dans X.

Définition 11 (élément maximal, maximum) *Soit $X \subseteq A$.*

- *un élément a est* maximal *dans X s'il appartient à X et s'il n'y a pas dans X d'éléments plus grand que a.*

$$\mathtt{maximal}(a,X) \overset{def}{=} a \in X \wedge \forall x \in X, a \leq x \Rightarrow a=x$$

- *un élément a est* maximum *dans X s'il appartient à X et s'il est plus grand que tous les éléments de X.*

$$\mathtt{maximum}(a,X) \overset{def}{=} a \in X \wedge \forall x \in X, x \leq a$$

Proposition 3 *Si $X \subseteq A$ admet un élément maximum alors cet élément est aussi maximal, c'est l'unique élément de $\mathtt{maj}(X) \cap X$.*

Preuve: *Soit a un élément maximum de X dans A alors par définition $a \in X$ et $\forall x \in X, x \leq a$ c'est-à-dire $a \in \mathtt{maj}(X)$. Les éléments maximum sont par définition les éléments de $\mathtt{maj}(X) \cup X$. Montrons maintenant que $\mathtt{maj}(X) \cap X$ est réduit à un élément. Supposons x et y dans $\mathtt{maj}(X) \cap X$. Comme $x \in X$ et $y \in \mathtt{maj}(X)$, on a $x \leq y$. De même en inversant les rôles de x et de y on trouve $y \leq x$ et donc $x=y$.* □

Il faut faire attention que certaines propriétés ne sont vraies que dans le cas d'un ordre total. Un élément maximal n'est pas toujours maximum. Si on regarde $X=\{\{1\};\{2\}\}$, les éléments de A sont incomparables et tous les deux sont des éléments maximaux de X qui n'admet pas d'élément maximum. Même si un ensemble a un seul élément maximal, cela ne veut pas dire qu'il est maximum. Par exemple, on peut prendre un ensemble X de sous ensembles de $\mathbb{N}$ qui contient tous les ensembles $X_n \overset{def}{=} \{k \in \mathbb{N} \mid k \text{ est pair} \wedge k \leq 2n\}$ ainsi que l'ensemble $Y \overset{def}{=} \{1\}$. On a $X_n \subseteq X_{n+1}$ et $X_n \neq X_{n+1}$ donc aucun ensemble X_n n'est maximal. Les ensembles X_n et Y sont incomparables pour tout n et donc Y est maximal. C'est l'unique élément maximal mais il n'est pas maximum.

Exercice 4 *Montrer que si $\leq$ est un ordre total alors un élément maximal est aussi maximum.*
Preuve: *Soit a un élément maximal, on a $a \in X$ et $\forall x \in X, a \leq x \Rightarrow x$ Il faut montrer que $\forall x \in X, x \leq a$. Comme l'ordre est total on peut raisonner par cas suivant que $x \leq a$ ou $a \leq x$. Dans le premier cas, $x \leq a$ on a la propriété attendue. Dans le second cas $a \leq x$, comme a est maximal, on en déduit $a=x$ et donc $x \leq a$ également.* □

Définition 12 (Borne supérieure) *On dit que $a \in A$ est la* borne supérieure *d'un ensemble X, si et seulement si a est un majorant de X et a est le minimum des majorants (s'il existe). C'est-à-dire :*

- $\forall x \in X, x \leq a$
- $\forall x \in X, (\forall y \in X, y \leq x) \Rightarrow a \leq x$

De même la *borne* inférieure se définit comme le plus grand des minorants.

Remarques.

- Un élément maximal ou maximum de X appartient à l'ensemble X, par contre ce n'est pas forcément le cas de la borne supérieure.
- Si un ensemble X admet un élément maximum alors celui-ci est aussi sa borne supérieure. En effet le maximum m est un majorant et c'est aussi le plus petit car tout majorant est plus grand que tous les éléments de X donc en particulier plus grand que m.
- Un ensemble peut ne pas avoir de borne supérieure, soit parce qu'il n'a pas de majorant (ensemble des entiers pairs) soit parce qu'il n'a pas de majorant minimal. Si on pose $x_n=\Sigma_{k=0}^{n}\ 1/n!$ et $X=\cup_n \{x_n\}$. La suite $(x_n)_n$ est une suite de rationnels croissante dont la limite est l'exponentielle e. L'ensemble des majorants dans $\mathbb{Q}$ est donc non vide (il contient au moins 2). Par contre, il n'y a pas d'élément minimal dans $\mathbb{Q}$ (sinon e serait rationnel).

Proposition 4 *Soit E un ensemble et $A=\wp(E)$ ordonné par la relation d'inclusion. Tout sous ensemble X de A admet une borne supérieure qui est $\cup X$.*

Preuve: *Par définition de $\cup X$. On a $\forall Y\in X,\ Y\subseteq \cup X$ et $\cup X$ est le plus petit ensemble qui contient tous les $Y\in X$ au sens où s'il existe Z tel que on a $\forall Y\in X,\ Y\subseteq Z$ alors $\cup X\subseteq Z$.* □

De même en considérant l'ordre inverse, on montre que toute partie X de $\wp(E)$ admet une borne inférieure qui est $\cap X$.

Pour l'ordre de la divisibilité, la borne supérieure de $\{x;y\}$ est exactement le plus petit multiple commun des deux nombres.

Exercice 5 *On se donne un ensemble A, un ordre $\leq$ sur cet ordre et un ensemble X. Dans chacun des cas suivants, dire si l'ordre est total et donner pour X l'ensemble des majorants, des minorants, des éléments maximaux, des éléments minimaux, et lorsqu'ils existent : le minimum, le maximum, la borne supérieure et la borne inférieure.*

1. $A=\mathbb{N}^*$, $x\leq y \Leftrightarrow x$ ***div*** y, $X=\{3,4,6\}$
2. $A=\wp(\{a,b,c\})$, $x\leq y \Leftrightarrow x\subseteq y$, $X=\{x\in A / 1\leq$ ***card***$(x)\leq 2\}$
3. $A=\wp(\mathbb{N})$, $x\leq y \Leftrightarrow x\subseteq y$, $X=\{[n,+\infty[\ / \ n\in\mathbb{N}\}$

5.3.4 Ordre sur un ensemble produit

Soient deux ensembles ordonnés $(A_1,\leq_1)$ et $A_2,\leq_2)$. Il y a plusieurs manières de définir un ordre sur l'ensemble produit $A_1\times A_2$.

Définition 13 (Ordre produit) *On définit l'ordre produit par $(x_1,x_2)\leq (y_1,y_2)$ si et seulement si $x_1\leq_1 y_1 \wedge x_2\leq_2 y_2$.*

Sur le plan $\mathbb{Z}\times\mathbb{Z}$, les points plus petits que x,y seront tous ceux placés dans le quart de plan en bas à gauche de x,y.

Définition 14 (Ordre lexicographique) *On définit l'ordre lexicographique par $(x_1,x_2)\leq (y_1,y_2)$ si et seulement si $x_1<_1 y_1 \vee (x_1=y_1 \wedge x_2\leq_2 y_2)$*

Sur le plan $\mathbb{Z}\times\mathbb{Z}$, les points plus petits que x,y seront tous les points placés dans le demi-plan ouvert à gauche de x,y plus les points de la demi-droite verticale dessous x,y.

Exercice 6

- *Montrer que l'ordre produit et l'ordre lexicographique définissent des ordres.*
- *On suppose que $\leq_1$ et $\leq_2$ sont des ordres totaux, en est-il de même de l'ordre produit ? de l'ordre lexicographique ?*

5.4 Ordres bien fondés

Les ordres bien fondés sont des ordres pour lesquels il n'existe pas de suite infinie strictement décroissante. Ils jouent un rôle essentiel dans les preuves par induction mais aussi dans la terminaison des programmes. Si un programme contient une boucle et que l'on peut montrer qu'à chaque itération une certaine expression décroit pour un ordre bien fondé alors on garantit que la boucle devra forcément s'arréter.

Définition 15 (Ordre bien fondé) *Un ordre $\leq$ sur un ensemble A est bien fondé s'il n'existe pas de suite infinie $(x_n)_{n\in\mathbb{N}}$ strictement décroissante c'est-à-dire telle que $\forall\, n\in\mathbb{N}, x_{n+1} < x_n$.*

L'ordre usuel sur les entiers naturels est un ordre bien fondé, par contre ce n'est pas le cas sur $\mathbb{Z}$. L'ordre d'inclusion sur les parties de $\mathbb{N}$ n'est pas bien fondé, en effet il suffit de regarder la suite des $[n,\infty[$ qui est une suite infinie strictement décroissante.

Un ordre sur un ensemble fini est bien fondé, en effet dans une suite infinie strictement décroissante, si $i<j$ alors $x_j<x_i$ et par irreflexivité de l'ordre strict on a $x_j\neq x_i$. Les éléments sont donc deux à deux distincts ce qui est impossible si l'ensemble est fini.

La caractérisation suivante des ordres bien fondés est parfois plus simple à manipuler.

Proposition 5 *Un ordre $\leq$ sur un ensemble A est bien fondé si et seulement si toute partie non vide admet au moins un élément minimal.*

Preuve: *On rappelle que $a\in X$ est un élément minimal de X si et seulement si $\forall\, x\in X, x\leq a \Rightarrow x = a$. Soit X une partie non vide de A et supposons qu'elle n'admette pas d'élément minimal. Alors pour tout $a\in A$, il existe $x\in X$ tel que $x\leq a \wedge x\neq a$ c'est-à-dire $x < a$. Comme $X\neq\emptyset$ on peut construire une suite $(x_n)_{n\in\mathbb{N}}$ d'objets de X en choisissant x_0 arbitraire dans X et en choisissant pour x_{n+1} un élément de X strictement plus petit que x_n. On construit ainsi une suite infinie strictement décroissante qui contredit le fait que $\leq$ est bien-fondée. Réciproquement, si tout ensemble non-vide admet un élément minimal, soit $(x_n)_{n\in\mathbb{N}}$ une suite infinie décroissante. C'est un ensemble non vide donc qui admet un élément minimal x_i. On a $x_{i+1}<x_i$ ce qui contredit que x_i est minimal.* □

Proposition 6 *L'ordre produit de deux ordres bien fondés est bien fondé. De même pour l'ordre lexicographique.*

Preuve: *On peut montrer que tout sous-ensemble X de $A_1\times A_2$ admet un élément minimal. Pour cela on regarde $X_1=\{x\in A_1 \mid \exists\, y\in A_2, (x,y)\in X\}$ c'est un ensemble non-vide qui admet donc un élément minimal x_1. On regarde ensuite $Y_1=\{y\in A_2 \mid (x_1,y)\in X\}$ c'est un ensemble non vide qui admet donc un élément minimal y_1. On peut montrer que (x_1,y_1) est minimal dans X. Soit $(x,y)\in X$ tel que $(x,y)\leq (x_1,y_1)$, on a par définition de l'ordre produit $x\leq x_1$ et $y\leq y_1$. Comme $x\in X_1$ et x_1 est minimal on a $x=x_1$ et donc $y\in Y_1$ et par minimalité de y_1 on en déduit que $y=y_1$.*

La même construction s'applique pour l'ordre lexicographique. Montrons que (x_1,y_1) *est minimal. Soit* $(x,y) \in X$ *tel que* $(x,y) \leq (x_1,y_1)$*, on a par définition de l'ordre lexicographique* $x < x_1$ *ou bien* $x = x_1$ *et* $y \leq y_1$*. Comme* $x \in X_1$ *et* x_1 *est minimal on a forcément* $x=x_1$ *et donc* $y \in Y_1$ *et par minimalité de* y_1 *on en déduit que* $y=y_1$*.* □

Les ordres bien fondés permettent de déduire un principe d'induction généralisé. Si on doit prouver $\forall\, x \in A, P(x)$ et que A est muni d'un ordre bien fondé, alors il suffit de prouver $P(x)$ pour tout $x \in A$ en supposant de plus que $P(y)$ est vérifié pour tous les y strictement inférieurs à x.

Proposition 7 *Soit* A *un ensemble muni d'un ordre bien fondé* $\leq$ *et* $P(x)$ *une propriété des élements de* A*. Si* $\forall\, x \in A, (\forall\, y \in A, y < x \Rightarrow P(y)) \Rightarrow P(x)$ *alors* $\forall\, x \in A, P(x)$

Preuve: *La preuve se fait par l'absurde en montrant que* $X=\{x \in A \mid \neg\, P(x)\}$ *est vide. En effet s'il n'est pas vide alors il admet un élément minimal* $x \in X$*. Comme* x *est minimal alors* $\forall\, y \in A, y < x \Rightarrow y \notin X$ *et donc* $\forall\, y \in A, y < x \Rightarrow P(y)$ *et donc l'hypothèse d'induction permet de prouver que* $P(x)$ *est vrai qui contredit le fait que* $x \in X$*.* □

Exemple 9 *On cherche à définir la fonction d'Ackermann par les équations suivantes :*

$$\texttt{ack}(0,m)=m+1 \qquad \texttt{ack}(n+1,0)=\texttt{ack}(n,1) \qquad \texttt{ack}(n+1,m+1)=\texttt{ack}(n,\texttt{ack}(n+1,m))$$

On peut définir la relation correspondante par cloture :

$$\texttt{Ack}(0,m,m+1) \qquad \frac{\texttt{Ack}(n,1,y)}{\texttt{Ack}(n+1,0,y)} \qquad \frac{\texttt{Ack}(n+1,m,y) \quad \texttt{Ack}(n,y,z)}{\texttt{Ack}(n+1,m+1,z)}$$

Pour montrer que cette fonction est totale, il faut établir que : $\forall\, n\, m \in \mathbb{N}, \exists\, y \in \mathbb{N}, \texttt{Ack}(n,m,y)$*. Une tentative par récurrence sur* n *ou sur* m *ne fonctionne pas. On peut utiliser plutôt une induction bien fondée sur le couple* (n,m) *en utilisant l'ordre lexicographique. On peut donc supposer que* $\forall\, n_1\, m_1 \in \mathbb{N}, (n_1,m_1) < (n,m) \Rightarrow \exists\, y \in \mathbb{N}, \texttt{Ack}(n_1,m_1,y)$*. Il faut alors montrer* $\exists\, y \in \mathbb{N}, \texttt{Ack}(n,m,y)$ *On raisonne par cas :*

- *Si* $n=0$ *il suffit de prendre* $y=m+1$
- *Si* $n>0$ *et* $m=0$ *alors par hypothèse d'induction appliquée à* $(n-1,1)<(n,0)$*, on a* $\exists\, y \in \mathbb{N}, \texttt{Ack}(n-1,1,y)$ *et donc* $\exists\, y \in \mathbb{N}, \texttt{Ack}(n,0,y)$
- *Si* $n>0$ *et* $m>0$ *alors par hypothèse d'induction appliquée à* $(n,m-1)<(n,m)$*, on a* $\exists\, y \in \mathbb{N}, \texttt{Ack}(n,m-1,y)$*, soit* y *tel que* $\texttt{Ack}(n,m-1,y)$*, on applique l'hypothèse d'induction une nouvelle fois à* $(n-1,y)<(n,m)$*, on a* $\exists\, z \in \mathbb{N}, \texttt{Ack}(n-1,y,z)$ *et on en déduit* $\exists\, z \in \mathbb{N}, \texttt{Ack}(n,m,z)$*.*

Il n'est pas toujours aisé de construire des ordres bien fondés. Prenons l'ensemble A^* des mots finis sur un alphabet A qui est un ensemble ordonné. On peut définir l'ordre lexicographique sur A^* par $m_1 \leq m_2$ si et seulement si m_1 est un préfixe de m_2 ou bien il existe un indice i inférieur à la longueur de m_1 et à la longueur de m_2 telle que $m_1[i]<m_2[i] \wedge \forall\, k < i, m_1[k]=m_2[k]$.

Si on se donne un alphabet à deux lettres $\{a;b\}$ avec $a < b$ alors on a

$$\epsilon < a \qquad a < aa \qquad ab < b \qquad aab < ab$$

Si on se restreint aux mots de longueur inférieure à une taille donnée n et si l'ordre sur l'alphabet est bien fondé alors il en est de même de l'ordre lexicographique sur les mots de longueur inférieure à n. Il suffit de généraliser la construction sur le produit pour construire un mot minimal dans chaque ensemble non

vide. Par contre l'ordre lexicographique sur les mots n'est pas bien fondé si on considère des ensembles de mots dont la taille n'est pas bornée. En effet il suffit de considérer la suite $(a^n b)_{n\in\mathbb{N}}$ qui est strictement décroissante car pour tout n on a $a^{n+1}b < a^n\, b$.

L'ordre préfixe par contre est bien fondé (il ne nécessite pas d'ordre sur l'alphabet sous-jacent); l'ordre préfixe n'est pas total alors que l'ordre lexicographique l'est.

Remarques.

Les ordres sont une notion importante en informatique. En effet, la terminaison d'un programme est un problème indécidable, il faut donc pour chaque programme apporter une preuve spécifique du fait que le calcul s'arrêtera quelle que soit l'entrée. Exhiber un ordre bien fondé tel que le calcul construit une chaine décroissante de valeurs est une manière de résoudre ce problème.

Les ordres bien fondés servent également pour effectuer des preuves par induction.

Les ordres interviennent également dans le problème de l'ordonnancement en machine: l'ordinateur a plusieurs tâches à compléter, chacune se découpe en instructions élémentaires, et certaines instructions doivent être effectuées avant d'autres ce qui correspond à un ordre partiel. Le processeur doit exécuter les instructions de manière séquentielle, c'est-à-dire en construisant un ordre total qui doit respecter les contraintes.

5.5 Treillis et théorèmes de point fixe

Définition 16 *Un ensemble ordonné $(A,\leq)$ est un treillis si deux éléments x et y ont une borne supérieure (notée $x\sqcup y$) et une borne inférieure (notée $x \sqcap y$).*

Exemple 10

- *Un ensemble totalement ordonné est un treillis avec lorsque $x\leq y$: $x\sqcap y = x$ et $x\sqcup y = y$. Les opérations $\sqcap$ et $\sqcup$ correspondent respectivement au minimum et au maximum.*
- *L'ensemble $\wp(E)$ des parties d'un ensemble E muni de l'ordre inclusion est un treillis avec $A\sqcup B = A \cup B$ et $A\sqcap B = A \cap B$.*
- *L'ensemble des entiers muni de la relation de divisibilité est un treillis avec $x\sqcap y = \texttt{pgcd}(x,y)$ et $x\sqcup y = \texttt{ppcm}(x,y)$*

Les opérations $\sqcap$ et $\sqcup$ satisfont des propriétés particulières :

Proposition 8 *Soit $(A,\leq)$ un treillis. Les propriétés suivantes sont dérivables :*

- *Les opérations $\sqcup$ et $\sqcap$ sont symétriques et associatives :*
  - $\forall x\, y\in A,\ x\sqcup y = y\sqcup x \qquad \forall x\, y\in A, x\sqcap y = y\sqcap x$
  - $\forall x\, y\, z\in A,\ x\sqcup(y\sqcup z) = (x\sqcup y)\sqcup z \qquad \forall x\, y\, z\in A,\ x\sqcap(y\sqcap z) = (x\sqcap y)\sqcap z$
- *Lois d'absorption :* $\forall x\, y\in A,\ x\sqcup(x\sqcap y) = x \qquad \forall x\, y\in A,\ x\sqcap(x\sqcup y) = x$

Une conséquence des lois d'absorption est l'idempotence des opérations :

$$\forall x\in A,\ x\sqcap x = x \qquad \forall x\in A,\ x\sqcup x = x$$

Preuve: *On a $x\sqcap x = x\sqcap(x\sqcup(x\sqcap x)) = x$. on déduit ensuite $x = x\sqcup(x\sqcap x) = x\sqcup x$.* □

Réciproquement, si on se donne deux opérations $\sqcap$ et $\sqcup$ qui sont symétriques, associatives et qui vérifient les lois d'absorption alors il est possible de définir une relation d'ordre $x\leq y \ =^{def}\ x\sqcap y = x$ ce qui est

équivalent à $x \sqcup y = y$.

5.5.1 Cas particuliers de treillis

Un treillis $(A,\leq)$ est dit *borné* s'il possède un élément minimum (noté $\bot$) et un élément maximum (noté $\top$) qui sont différents. Un treillis borné vérifie les propriétés suivantes :

- $\forall\, x \in A, x \sqcup \top = \top$, $\forall\, x \in A, x \sqcap \bot = \bot$
- $\forall\, x \in A, x \sqcap \top = x$, $\forall\, x \in A, x \sqcup \bot = x$

Preuve: *Les premières propriétés sont une traduction de la propriété de maximum de $\top$ et de minimum de $\bot$. Les dernières se déduisent de la règle d'absorption : $x=x \sqcap (x \sqcup \top)$ et comme $x \sqcup \top = \top$ on en déduit le résultat.* □

Un treillis $(A,\leq)$ est *distributif* si de plus chaque opération est distributive par rapport à l'autre, c'est-à-dire que l'on a :

- $\forall\, x\ y\ z \in A, x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$
- $\forall\, x\ y\ z \in A, x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$

Un treillis $(A,\leq)$ borné est *complémenté* s'il existe une application $x \mapsto \overline{x}$ telle que

- $\forall\, x \in A, x \sqcup \overline{x} = \top$
- $\forall\, x \in A, x \sqcap \overline{x} = \bot$

Définition 17 (Algèbre de Boole) *Un treillis qui est complémenté et distributif s'appelle une* algèbre de Boole.

Exemple 11 *Dans le cas du treillis sur les parties d'un ensemble E, l'opération de complément est l'application qui à un sous-ensemble A de E, associe son complément $E \setminus A$.*

Dans un treillis complémenté on a $\overline{\top}=\bot$ et $\overline{\bot}=\top$.
Preuve: *On a $\overline{\top} = \overline{\top} \sqcap \top = \bot$ et $\overline{\bot} = \overline{\bot} \sqcup \bot = \top$.* □

Dans un treillis distributif complémenté, il n'existe qu'une seule application de complément. Cette application vérifie les lois suivantes dites lois de *de Morgan* :

- $\forall\, x, \overline{\overline{x}}=x$
- $\forall\, x\ y, \overline{x \sqcap y}=\overline{x} \sqcup \overline{y}$
- $\forall\, x\ y, \overline{x \sqcup y}=\overline{x} \sqcap \overline{y}$
- $\forall\, x\ y, x \leq y \Leftrightarrow \overline{y} \leq \overline{x}$

Preuve: *On montre d'abord qu'il n'y a qu'une seule application de complément. Supposons que l'on ait deux compléments y_1 et y_2 pour x. On a alors $x \sqcup y_1 = \top$, $x \sqcup y_2 = \top$, $x \sqcap y_1 = \bot$ et $x \sqcap y_2 = \bot$. On a alors $(x \sqcup y_1) \sqcap y_2 = \top \sqcap y_2 = y_2$ et par distributivité $(x \sqcup y_1) \sqcap y_2 = (x \sqcap y_2) \sqcup (y_1 \sqcap y_2) = \bot \sqcup (y_1 \sqcap y_2) = y_1 \sqcap y_2$. Don $y_2=y_1 \sqcap y_2$ et donc $y_2 \leq y_1$. Le même raisonnement en changeant y_1 et y_2 nous donne $y_1 \leq y_2$ et finalement $y_1 = y_2$.*

$\overline{x}= \overline{x} \sqcup \bot = \overline{x} \sqcup (\overline{x} \sqcap x) = (\overline{x} \sqcup \overline{x}) \sqcap (\overline{x} \sqcup x) = \top \sqcap (\overline{x} \sqcup x) = \overline{x} \sqcup x$ donc $x \leq \overline{x}$.
$\overline{x}= \overline{x} \sqcap \top = \overline{x} \sqcap (\overline{x} \sqcup x) = (\overline{x} \sqcap \overline{x}) \sqcup (\overline{x} \sqcap x) = \bot \sqcup (\overline{x} \sqcap x) = \overline{x} \sqcap x$ donc $\overline{x} \leq x$ et finalement $\overline{x} = x$.
Pour montrer les lois de de Morgan, on peut utiliser l'unicité du complément et on prouve $(x \sqcap y) \sqcap (\overline{x} \sqcup$

$\bar{y}) = \bot$ $(x \sqcap y) \sqcup (\bar{x} \sqcup \bar{y}) = \top$.
On a $(x \sqcap y) \sqcap (\bar{x} \sqcup \bar{y}) = (x \sqcap y \sqcap \bar{x}) \sqcup (x \sqcap y \sqcap \bar{y}) = (\bot \sqcap y) \sqcup (x \sqcap \bot) = \bot \sqcup \bot = \bot$.
$x \leq y \Leftrightarrow x \sqcap y = x \Leftrightarrow x \sqcap \overline{y} = x \Leftrightarrow x \sqcup \bar{y} = \bar{x} \Leftrightarrow \bar{y} \leq \bar{x}$. □

5.5.2 Théorèmes de point fixe

Définition 18 (Treillis complet) *Un treillis $(A,\leq)$ est* complet *si tout ensemble (pas seulement les ensembles finis) admet une borne supérieure. On notera $\sqcup X$ la borne supérieure de l'ensemble X.*

Exemple 12 *L'ensemble des parties de E est un treillis complet. La borne supérieure est l'union.*

Un intervalle fermé de $\mathbb{R}$ forme un treillis complet pour l'ordre usuel.

Proposition 9 *Dans un treillis complet, tout ensemble admet une borne inférieure. On note $\sqcap X$, la borne inférieure de l'ensemble X.*

Preuve: *Soit une partie X de A. On introduit Y l'ensemble des minorants de X et a la borne supérieure de Y. On montre que a est la borne inférieure de X.*

Il faut montrer que $\forall x \in X, a \leq x$. Soit $x \in X$, on a $\forall y \in Y, y \leq x$ donc $a \leq x$.

On suppose maitenant que y vérifie $\forall x \in X, b \leq x$, on a alors $y \in Y$ et donc $y \leq a$. □

La borne supérieure de l'ensemble A entier est un élément maximum noté $\top$ et la borne inférieure de A est un élément minimum noté $\bot$. Un treillis complet est donc borné.

Proposition 10 (Point fixe de fonction monotone) *Soit A un* treillis complet *et f une application* monotone *de A dans A, alors l'ensemble des point-fixes de f (ie $\{x \in A \mid f(x)=x\}$) est non-vide et admet un plus petit et un plus grand élément.*

Preuve: *On regarde l'ensemble des pre-point-fixes, ie $F =^{def} \{x \in A \mid f(x) \leq x\}$. Cet ensemble contient au moins $\top$. On note a sa borne inférieure. On a*

1. $\forall x, f(x) \leq x \Rightarrow a \leq x$.
2. $\forall y \ (\forall x, f(x) \leq x \Rightarrow y \leq x) \Rightarrow y \leq a$.

On montre d'abord que $f(a) \leq a$. Pour cela il suffit de montrer que $f(a)$ est un minorant de F. Soit donc $x \in F$, on a $f(x) \leq x$, comme a est un minorant de F, on a et de plus $a \leq x$ et donc $f(a) \leq f(x)$ et par transitivité $f(a) \leq x$ et finalement $f(a) \leq a$. Donc $a \in F$.

Pour montrer $a \leq f(a)$ on utilise la première propriété de la borne inférieure avec $x=f(a)$. il suffit de montrer $f(f(a)) \leq f(a)$ qui est une conséquence de la monotonie et de la propriété $f(a) \leq a$ montrée précédemment.

Donc a est un point fixe, c'est le plus petit car si on a un autre point fixe x, il appartient à F et donc il est plus grand que a.

De même le plus grand point fixe, se construit comme la borne supérieure de l'ensemble des post-point fixes, c'est-à-dire de $G =^{def} \{x \in A \mid x \leq f(x)\}$ □

Une application de ce théorème est la définition d'une relation R par clôture. Dans une telle définition on se donne des règles d'inférence qui caractérisent la relation. Ces règles d'inférence peuvent se traduire sous la forme d'une équation $R = F(R)$. Prenons l'exemple de la définition par cloture de l'ordre sur les entiers :

$$\texttt{le}(x,y)$$

$$\texttt{le}(x,x) \qquad \texttt{le}(x,y+1)$$

L'espace est l'ensemble des parties de $\mathbb{N}\times\mathbb{N}$ muni de l'ordre d'inclusion. On traduit les règles d'inférence en la propriété attendue :

$$\forall\ x\ z,\ \texttt{le}(x,z) \Leftrightarrow (\ x=z \vee \exists\ y,z=y+1 \wedge \texttt{le}(x,y))$$

On peut donc introduire la fonction F sur les relations binaires d'entiers par:

$$F(\texttt{le})=\{(x,z)\in\mathbb{N}\times\mathbb{N}\ \mid x=z \vee \exists\ y,z=y+1 \wedge \texttt{le}(x,y)\}$$

Cette fonction est monotone (c'est-à-dire que $\forall\ \texttt{le}_1\ \texttt{le}_2 \subseteq A\times A, \texttt{le}_1 \subseteq \texttt{le}_2 \Rightarrow F(\texttt{le}_1)\subseteq F(\texttt{le}_2)$) et admet donc un plus point fixe qui vérifie la propriété attendue.

Définition 19 (Continuité) *Une application f d'un treillis A dans un treillis B est* continue *si elle préserve les bornes supérieures des ensembles non-vides, c'est-à-dire que si $X\subseteq A$ est non vide et si X admet une borne supérieure a alors l'ensemble $f(X)$ (qui est non-vide) admet aussi une borne supérieure et celle-ci est égale à $f(a)$.*

Une fonction continue sur un treillis est monotone. En effet si $x\leq y$ alors la borne supérieure de $\{x;y\}$ est y et donc la borne supérieure de $\{f(x);f(y)\}$ est $f(y)$ et donc $f(x)\leq f(y)$.

Pour n'importe quelle fonction monotone f sur un treillis complet on a $\sqcup(f(X)) \leq f(\sqcup X)$ par contre le contraire n'est pas toujours vérifié.

Exemple 13 (Fonction non continue) *Soit A l'ensemble des suites infinies de 0 et de 1 et F la fonction qui à la suite s associe le réel $\Sigma_{n=0}^{\infty}\ s[n]1/2^n$ avec $s[n]$ la n-ème valeur de la suite s. L'ensemble des réels muni de l'ordre total usuel est un treillis. Cette fonction est monotone si on considère l'ordre point à point sur les séquences. On considère maintenant l'ensemble des suites s_n telles que $s_n[n]=1$ et $s_n[k]=0$ si $k\neq n$. On a $\sqcup_n s_n$ est la suite qui vaut 1 partout et donc pour cette suite la valeur de F est 2 alors que pour chaque suite s_n on a $F(s_n)=1/2^n \leq 1$.*

La continuité permet de caractériser le plus petit point-fixe.

Proposition 11 (Point fixe de fonction continue) *Soit A un* treillis complet *et f une application* continue *de A dans A, alors le plus petit point fixe de f est égal à la borne supérieure de l'ensemble $\{f^n(\bot)/n\in\mathbb{N}\}$.*

Preuve: *On note a la borne supérieure de $F =^{def} \{f^n(\bot)/n\in\mathbb{N}\}$ et on montre que c'est un point fixe. On a $\bot\leq f(\bot)$ et donc par monotonicité $f^n(\bot)\leq f^{n+1}(\bot)$ On en déduit que la borne supérieure de F est égale à la borne supérieure de $f(F)=\{f^{n+1}(\bot)/n\in\mathbb{N}\}$. On a donc $a=f(a)$.*
On remarque que pour cette preuve, on a juste besoin de l'existence d'une borne supérieure pour un suite croissante d'objets. □

En informatique, on utilise souvent la construction de point fixe de fonction monotone sur des ensembles finis.

Proposition 12 (Point fixe dans un ensemble fini) *Soit A un ensemble ordonné fini, qui admet un élément minimum $\bot$ et f une application monotone de A dans A. La fonction f admet un plus petit point fixe qui est de la forme $f^k(\bot)$ avec k inférieur au cardinal de A.*

Preuve: *On regarde la suite croissante* $\{f^n(\bot)|n\in\mathbb{N}\}$*, elle contient au plus un nombre d'éléments égal au cardinal de* A *et donc il existe* k *tel que* $f^{k+1}(\bot)=f^k(\bot)$ *et donc* $f^k(\bot)$ *est un point fixe de* f*.* □