Applications monotones

Une application monotone est une application qui conserve l'ordre. Grosso modo, quand tu as $(A, \leq)$ et $(B, \sqsubseteq)$ deux ensembles ordonnés, l'application $f : A \to B$ est monotone si

$$\forall xy \in A, \quad x \leq y \Longrightarrow f(x) \sqsubseteq f(y)$$

Il y a un grand nombre d'exemples dans le cours et en mathématiques en général, dont certains que tu connais déjà, et d'autres pas forcément. Quand on parle d'application monotone, il faut préciser par rapport à quel ensemble ordonné, d'autant que de nombreux ensembles classiques peuvent être munis d'ordres différents. Par exemple, l'ensemble des entiers naturels $\mathbb{N}$ peut être muni de l'ordre usuel $(\mathbb{N}, \leq)$, ou bien de la relation de divisibilité $(\mathbb{N}, |)$. Ainsi, au lieu de noter $f : A \to B$, je vais noter $f : (A, \leq) \to (B, \sqsubseteq)$.

- Si $f, g : (\mathbb{R}, \leq) \to (\mathbb{R}, \leq)$, alors $f(x) = x^2$ ou $g(x) = \sqrt{x}$ sont monotones.
- Un exemple intéressant en arithmétique est la fonction $h : (\mathbb{N}, |) \to (\mathbb{N}, |)$ avec $h(x) = x^2$. En effet, si $x \mid y$, cela signifie qu'il existe $k \in \mathbb{N}$ tel que $y = kx$. Alors, $y^2 = (kx)^2 = k^2x^2$. Donc $x^2 \mid y^2$, et h est monotone.
- Un exemple que nous avons croisé plusieurs fois en cours est la longueur d'un mot $\mathrm{len} : A^* \to \mathbb{N}$. Cette application est monotone pour plusieurs ensembles ordonnés, comme l'ordre préfixe[1] $\sqsubseteq_{\mathrm{pre}}$ ou l'ordre suffixe $\sqsubseteq_{\mathrm{suff}}$. On pourra alors écrire $\mathrm{len} : \left(A^*, \sqsubseteq_{\mathrm{pre}}\right) \to (\mathbb{N}, \leq)$ et $\mathrm{len} : (A^*, \sqsubseteq_{\mathrm{suff}}) \to (\mathbb{N}, \leq)$.
- Enfin, un exemple plus complexe montrant l'importance de bien spécifier les ordres. On note $\mathbb{N}^*$ pour l'ensemble des entiers naturels non nuls. Alors, la fonction identité $\mathrm{id} : \mathbb{N}^* \to \mathbb{N}^*$ qui, pour $x \in \mathbb{N}^*$, associe x est:
  - monotone de $(\mathbb{N}^*, \leq)$ dans $(\mathbb{N}^*, \leq)$, car pour tout x, y, si $x \leq y$, alors $x \leq y$;
  - monotone de $(\mathbb{N}^*, |)$ dans $(\mathbb{N}^*, |)$, car pour tout x, y, si $x \mid y$, alors $x \mid y$;
  - monotone de $(\mathbb{N}^*, |)$ dans $(\mathbb{N}^*, \leq)$. La preuve n'est pas triviale. Si $x \mid y$, alors il existe $k \in \mathbb{N}^*$ tel que $y = xk$. Puisque $k \geq 1$, cela implique que $y \geq x$, donc $x \leq y$;
  - non monotone de $(\mathbb{N}^*, \leq)$ dans $(\mathbb{N}^*, |)$. Cela ne fonctionne pas dans l'autre sens. Par exemple, $5 \leq 6$, mais 5 ne divise pas 6 !

Exercice 1: Montre que $f : (\mathbb{N}, |) \to (\mathbb{N}, |)$ définie par $f(x) = 7x^2$ est monotone.

Ensembles isomorphes

La notion d'application monotone permet de définir des ensembles isomorphes. L'idée globale derrière les ensembles isomorphes est que si tu démontres une propriété pour un ensemble, alors cette propriété est également vraie pour le second ensemble. Puisqu'on parle d'isomorphisme d'ensembles ordonnés, les propriétés concernées sont toujours liées à des ordres.

Plus formellement, deux ensembles sont isomorphes s'il existe une fonction monotone de l'un vers l'autre qui est bijective, et dont l'inverse est également monotone. Avec des symboles, cela donne la définition suivante :

[1] Pour deux mots u et v, on dit que u est un préfixe de v et on note $u \sqsubseteq_{\mathrm{pre}} v$ s'il existe w avec $uw = v$.

Définition 1: Soient $(A, \leq)$ et $(B, \sqsubseteq)$ deux ensembles ordonnés. On dit que $(A, \leq)$ et $(B, \sqsubseteq)$ sont isomorphes s'il existe $f : A \to B$ bijective et monotone, et d'inverse $f^{-1} : B \to A$ monotone.

Avant d'expliquer pourquoi cette notion est intéressante, je montre quelques exemples d'ensembles isomorphes :

- $(A, \leq)$ est isomorphe à $(A, \leq)$. En effet, l'identité est toujours monotone, et l'inverse de l'identité est l'identité. Ce n'est pas très intéressant.
- Il n'y a pas de bijection entre $(\mathbb{R}, \leq)$ et $(\mathbb{Q}, \leq)$, donc ces deux ensembles ne sont pas isomorphes.
- $(\mathbb{R}, \leq)$ est isomorphe à $(\mathbb{R}, \geq)$. Cette fois, la fonction qui permet de passer d'un ensemble à l'autre est $f(x) = -x$. Cette fonction est monotone de $(\mathbb{R}, \leq)$ vers $(\mathbb{R}, \geq)$. En effet, si $x \leq y$ alors $-y \leq -x$. Et puisque $f(f(x)) = x$, f est une involution. Elle est donc bijective, et son inverse est elle-même (exercice 15 du TD 1).
- Un exemple plus intéressant est l'écriture en binaire des nombres. Cela se traduit par un isomorphisme entre $([0, 2^n], \leq)$ et l'ensemble ordonné des mots sur $\{0, 1\}$ de longueur n ordonné par l'ordre lexicographique $(\{0, 1\}^n, \preceq)$. La bijection est la fonction qui, à un nombre, associe son écriture en binaire. Par exemple $42 = 101010$ et $32 = 010000$, donc en lisant les écritures en binaire, on sait quel nombre est le plus petit.
- Pour finir, un exemple plus compliqué. Tu connais peut-être le théorème fondamental de l'arithmétique : il te dit que tout nombre $n \in \mathbb{N}^*$ peut être décomposé de manière unique en facteurs de nombres premiers :

$$n = 2^{k_0} 3^{k_1} 5^{k_2} 7^{k_3} \ldots = \prod_{i=0}^{\infty} p_i^{k_i}$$

  où la suite $(p_i)_{i \in \mathbb{N}}$ est la suite des nombres premiers ordonnés, et $(k_i)_{i \in \mathbb{N}}$ est une suite à support fini, c'est-à-dire nulle à partir d'un certain rang. Cela veut dire qu'il existe une application bijective $\varphi : \mathbb{N}^* \to \{u : \mathbb{N} \to \mathbb{N} \mid \exists k, \forall n \geq k,\, u(n) = 0\}$ qui, à un nombre, associe sa décomposition en facteurs premiers. Son inverse $\varphi^{-1} : \{u : \mathbb{N} \to \mathbb{N} \mid \exists k, \forall n \geq k,\, u(n) = 0\} \to \mathbb{N}^*$ est défini tout simplement par

$$\varphi^{-1}(u) = \prod_{i=0}^{\infty} p_i^{u(i)}$$

  Et ce qui est utile, c'est que tu peux voir si $n = \prod_{i=0}^{\infty} p_i^{u(i)}$ divise $m = \prod_{i=0}^{\infty} p_i^{v(i)}$ si et seulement si pour tout i, $u(i) \leq v(i)$. Cela veut dire que $(\mathbb{N}^*, \leq)$ est isomorphe à $\{u : \mathbb{N} \to \mathbb{N} \mid \exists k, \forall n \geq k,\, u(n) = 0\}$ muni de l'ordre produit[2] !

Comme je le disais, quand deux ensembles sont isomorphes, ils partagent les mêmes propriétés. Cela veut dire que si x est le plus grand élément de A, alors $f(x)$ est le plus grand élément de B. Pareil pour les majorants, minorants, borne sup, borne inf, etc. Mais aussi pour les ensembles bien fondés. Cela fait de la propriété d'isomorphisme une propriété très puissante. Cependant, cela signifie également que cette propriété n'est pas toujours vérifiée. Par exemple :

- L'ensemble ordonné $([0, 1], \leq)$ n'est pas isomorphe à $(]0, 1[, \leq)$. En effet, $([0, 1], \leq)$ admet un plus petit élément 0, mais pas $(]0, 1[, \leq)$.

[2]L'ordre produit est donné en comparant chacune des coordonnées.

- L'ensemble ordonné $(\mathbb{N}, |)$ n'est pas isomorphe à $(\mathbb{N}, \leq)$ puisque $(\mathbb{N}, \leq)$ est totalement ordonné, mais $5 \nmid 3$ et $3 \nmid 5$.
- L'ensemble ordonné $(\mathbb{N}, \leq)$ n'est pas isomorphe à $(\mathbb{Z}, \leq)$ puisque $(\mathbb{N}, \leq)$ est bien fondé, mais $(\mathbb{Z}, \leq)$ ne l'est pas : il existe une suite infinie décroissante dans $(\mathbb{Z}, \leq)$, par exemple $u_n = -n$.

Voici un exemple de preuve pour montrer que deux ensembles isomorphes ont bien la même propriété de bien-fondé :

Propriété 2: Soit $(A, \leq)$ et $(B, \sqsubseteq)$ deux ensembles ordonnés isomorphes, avec $f : A \to B$ bijective monotone et d'inverse g monotone. Alors, si $(A, \leq)$ est bien fondé, $(B, \sqsubseteq)$ l'est également.

Preuve: On procède par contraposée. On suppose que $(B, \sqsubseteq)$ n'est pas bien fondé, c'est-à-dire qu'il existe $u : \mathbb{N} \to B$ avec, pour tout i, $u(i+1) \sqsubsetneq u(i)$, et montrons que $(A, \leq)$ n'est pas bien fondé.

Pour cela, regardons la suite $g \circ u : \mathbb{N} \to A$. Pour i fixé, $u(i+1) \sqsubsetneq u(i)$ veut dire deux choses : $u(i+1) \sqsubseteq u(i)$ et $u(i+1) \neq u(i)$. Puisque g est monotone, $g(u(i+1)) \leq g(u(i))$. Il reste à montrer que $g(u(i+1)) \neq g(u(i))$. Si $g(u(i+1)) = g(u(i))$, alors $f(g(u(i+1))) = f(g(u(i)))$, donc $u(i+1) = u(i)$, absurde !

Donc $g \circ u : \mathbb{N} \to A$ est bien une suite strictement décroissante dans A. Donc $(A, \leq)$ n'est pas bien fondé. ■

Exercice 2: Soit $(A, \leq)$ et $(B, \sqsubseteq)$ deux ensembles ordonnés isomorphes, avec $f : A \to B$ bijective monotone et d'inverse g monotone. Soit $X \subseteq A$. Montre que $x \in \text{Majorants}(X)$ si et seulement si $f(x) \in \text{Majorants}(f(X))$.