

Outils Logiques Groupe 3 & 4 – DM 1 (Correction)

Les exercices étoilés « $\star - \star \star \star$ » sont facultatifs.

Dans ce sujet, $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ est l'ensemble des entiers naturels, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ est l'ensemble des entiers (relatifs), et \mathbb{R} est l'ensemble des nombre réels.

Exercice 1

Pour chacun des ordres partiels suivants, dire s'il est un ordre bien fondé. Si oui, essayer de le justifier. Si ce n'est pas le cas, trouver une suite infinie décroissante.

- (1) Les entiers $(\mathbb{Z}, >)$ avec l'ordre habituel.
- (2) Les entiers naturels $(\mathbb{N}, >)$ avec l'ordre habituel.
- (3) $(\mathbb{Z}, >_{|-|})$ Les entiers avec l'ordre absolu ($n >_{|-|} m$ ssi $|n| > |m|$).
- (4) L'intervalle $[0, 1] \subset \mathbb{R}$ avec l'ordre $>$ habituel.

Solution

- (1) $(\mathbb{Z}, >)$ n'est pas un ordre bien fondé car il existe des suites infinies décroissantes dans \mathbb{Z} , par exemple $0 > -1 > -2 > -3 > \dots$
- (2) $(\mathbb{N}, >)$ est un ordre bien fondé. Montrons que *toute* suite décroissante est nécessairement finie. Soit $x_0 > x_1 > x_2 \dots$ une suite décroissante dans \mathbb{N} . Alors pour chaque i , on a que $x_i \geq x_{i+1} + 1$, c'est-à-dire $x_i - 1 \geq x_{i+1}$. Donc la suite décroît d'au moins 1 à chaque étape. Donc elle est de longueur au plus x_0 .
- (3) $(\mathbb{Z}, >_{|-|})$ est un ordre bien fondé. Montrons que *toute* suite décroissante est nécessairement finie. Soit $x_0 >_{|-|} x_1 >_{|-|} \dots$ une suite décroissante. Alors la suite $|x_0| > |x_1| > \dots$ est une suite décroissante dans $(\mathbb{N}, >)$. On conclut par le point (2) précédent.
- (4) $([0, 1], >)$ n'est pas bien fondé. En effet il existe des suites infinies décroissantes comme $1 > \frac{1}{2} > \frac{1}{3} > \frac{1}{4} > \dots$

Exercice 2 (énoncé corrigé)

Ici \mathbb{Z}_* est l'ensemble des entiers non-nuls (c'est-à-dire $\mathbb{Z}_* = \mathbb{Z} - \{0\}$).

Pour deux entiers $m, n \in \mathbb{Z}$, on dit que m est un *diviseur propre* de n si $m \neq n$ et $(-1)m \neq n$, et s'il existe un $k \in \mathbb{Z}_*$ tel que $m \times k = n$. Introduisons la relation binaire $>_d$ sur \mathbb{Z} telle que $n >_d m$ ssi m est un diviseur propre de n . Est-ce que $(\mathbb{Z}, >_d)$ est un ordre partiel? Si oui, est-il bien fondé?

Solution

Oui $(\mathbb{Z}, >_d)$ est un ordre partiel bien fondé.

On commence par l'**observation** suivante : pour tout $r, s \in \mathbb{Z}$, si $s >_d r$ alors $|s| > |r|$ pour l'ordre habituel sur \mathbb{N} . Pour montrer cette observation, supposons $s >_d r$. Donc, comme $r \neq s$ et $(-1)r \neq s$, et qu'il existe $k \in \mathbb{Z}_*$ tel que $r \times k = s$, alors $k \neq 1$ et $k \neq -1$. Donc $|k| > 1$ dans \mathbb{N} . Comme $|s| = |r \times k| = |r| \times |k|$, on déduit que $|s| > |r|$ dans \mathbb{N} .

Montrons d'abord que $(\mathbb{Z}, >_d)$ est un ordre partiel, c'est à dire que la relation $>_d$ est transitive. Pour cela, soit $n, m, m' \in \mathbb{Z}$ tels que $n >_d m$ et $m >_d m'$. Il faut montrer que $n >_d m'$. Pour cela, on vérifie

d'abord que $m' \neq n$ et $(-1)m' \neq n$ car, par l'observation, on sait que $|n| > |m|$ et $|m| > |m'|$ dans \mathbb{N} , et donc $|n| > |m'|$ dans \mathbb{N} . En suite, on sait qu'il existe $k, k' \in \mathbb{Z}_*$ tels que $n = m \times k$ et $m = m' \times k'$. Donc on a que $n = m' \times (k \times k')$, avec $(k \times k') \in \mathbb{Z}_*$. Donc $n >_d m'$.

Montrons enfin que $(\mathbb{Z}, >_d)$ est bien fondé. Considérons une suite décroissante $x_0 >_d x_1 >_d x_2 >_d \dots$ dans $(\mathbb{Z}, >_d)$. Alors, par l'observation, on a que $|x_0| > |x_1| > |x_2| > \dots$ est une suite décroissante dans $(\mathbb{N}, >)$, et on conclut qu'elle est finie par (2) de l'Exercice 1.

Exercice 3

L'ensemble X^* des mots sur un ensemble X (appelé *l'alphabet*) est l'ensemble des suites finies d'éléments de X . On considère le système de réécriture suivant sur les mots sur l'alphabet $\{a, b\}$: pour tous $u, v \in \{a, b\}^*$, on a $uaabv \rightarrow uabbv$ et $uababv \rightarrow uaabv$. Est-il un système terminant ? Justifier.

Solution

Oui il est un système terminant.

Pour montrer cela, il suffit de trouver une fonction $f: \{a, b\}^* \rightarrow \mathbb{N} \times \mathbb{N}$ telle que pour tous $u, v \in \{a, b\}^*$, on a $f(uaabv) >_{lex} f(uabbv)$ et $f(uababv) >_{lex} f(uaabv)$ pour l'ordre lexicographique habituel sur $\mathbb{N} \times \mathbb{N}$.

Soit $\mu_1: \{a, b\}^* \rightarrow \mathbb{N}$ la fonction définie telle que $\mu_1(w)$ est le nombre de caractères dans le mot w (c'est-à-dire sa longueur). Donc pour tous $u, v \in \{a, b\}^*$, on a $\mu_1(uababv) > \mu_1(uaabv)$ et $\mu_1(uaabv) = \mu_1(uabbv)$ dans \mathbb{N} .

Soit $\mu_2: \{a, b\}^* \rightarrow \mathbb{N}$ la fonction définie telle que $\mu_2(w)$ est le nombre de fois que le caractère a apparaît dans w . Donc pour tous $u, v \in \{a, b\}^*$, on a $\mu_2(uaabv) > \mu_2(uabbv)$ dans \mathbb{N} .

Soit $f: \{a, b\}^* \rightarrow \mathbb{N} \times \mathbb{N}$ la fonction définie comme $f(w) = (\mu_1(w), \mu_2(w))$. Comme $\mu_1(uaabv) = \mu_1(uabbv)$ et $\mu_2(uaabv) > \mu_2(uabbv)$ dans \mathbb{N} , on a que $f(uaabv) >_{lex} f(uabbv)$ dans $\mathbb{N} \times \mathbb{N}$. Comme $\mu_1(uababv) > \mu_1(uaabv)$ dans \mathbb{N} , on a que $f(uababv) >_{lex} f(uaabv)$ dans $\mathbb{N} \times \mathbb{N}$.

Exercice 4

Pour deux ensembles A, B , on note $B \supsetneq A$ ssi $A \subset B$ et $A \neq B$. Soit X un ensemble quelconque.

- (1) Montrer que $(\mathcal{P}(X), \supsetneq)$ (l'ensemble de parties de X muni de la relation \supsetneq) est un ordre partiel.
- (2) Montrer que si X est fini (c'est-à-dire X a un nombre fini d'éléments distincts), alors $(\mathcal{P}(X), \supsetneq)$ est un ordre bien fondé.
- (3) (★★) Montrer qu'il en est de même pour X quelconque. (Indice : utiliser le Lemme de Kuratowski-Zorn.)

Solution

- (1) Soit $A, B, C \in \mathcal{P}(X)$ tels que $C \supsetneq B$ et $B \supsetneq A$. Il faut montrer $C \supsetneq A$. Comme $B \neq C$ et $B \subset C$, il existe $x \in C$ tel que $x \notin B$. Comme $A \subset B$, on déduit que $x \notin A$. Donc $C \neq A$. En suite, montrons $A \subset C$. Pour cela, soit $x \in A$. Comme $A \subset B$, on a $x \in B$ et comme $B \subset C$, on a $x \in C$. Donc $A \subset C$.
- (2) Si X est fini, alors tout sous-ensemble de X est fini. Soit $|-|: \mathcal{P}(X) \rightarrow \mathbb{N}$ la fonction définie telle que $|A|$ est le nombre d'éléments distincts dans A . Donc si $A_0 \supsetneq A_1 \supsetneq \dots$ est une suite décroissante dans $\mathcal{P}(X)$, alors $|A_0| > |A_1| > \dots$ est une suite décroissante dans \mathbb{N} . On conclut par (2) de l'Exercice 1.