

# MATHÉMATIQUES POUR L'INFORMATIQUE

Pour avoir 20/20, engrangez 20 points. N'oubliez pas de soigner la rédaction, elle compte autant que le reste de la réponse. Si ce que vous écrivez constitue juste une intuition de la réponse et pas une réponse rédigée, précisez-le.

Vous avez droit à vos cours et TDs. Vous avez le droit de réutiliser sans redémontrer le résultat de tout théorème, proposition, exercice... vu en cours ou TD, à condition de rappeler exactement le résultat et dans quelles circonstances il s'applique.

Vous avez 2h.

## Treillis

**Définition 1.** *Un ensemble ordonné est un treillis si toute paire d'éléments  $\{a, b\}$  admet une borne supérieure et une borne inférieure. On note alors généralement  $a \sqcup b$  la borne inférieure de  $a$  et  $b$  et  $a \sqcap b$  la borne supérieure de  $a$  et  $b$ .*

**Rappel** Si  $E$  est un ensemble ordonné par une relation  $\preceq$  et  $A$  est un sous-ensemble de  $E$ , la borne supérieure de  $A$  dans  $E$ , si elle existe, est un élément  $s$  de  $E$  tel que

- $\forall a \in A, a \preceq s$  (i.e.  $s$  est un majorant de  $A$ )
- $\forall b \in E, (\forall a \in A, a \preceq b) \implies s \preceq b$  ( $s$  est un minorant de l'ensemble des majorants de  $A$ ).

**Note** On n'a pas supposé que l'ordre était total. En particulier, a priori, ni  $a \sqcup b$  ni  $a \sqcap b$  n'est  $a$  ou  $b$ .

**Exercice 1.** Soit  $E$  un ensemble. Montrer que  $\mathcal{P}(E)$ , ordonné par  $\subseteq$ , est un treillis.

Commençons par remarquer que  $\subseteq$  est bien un ordre partiel sur  $\mathcal{P}(E)$ .

Considérons alors deux sous-ensembles  $A$  et  $B$  de  $E$ . Prouvons que  $A \cap B$  est une borne inférieure pour  $\subseteq$  et  $A \cup B$  une borne supérieure.

**Borne inférieure** Soit  $C$  un ensemble tel que  $C \subseteq A$  et  $C \subseteq B$ . Alors tout élément de  $C$  appartient à  $A$  et  $B$ , donc à  $A \cap B$ . Nous en déduisons donc que  $C \subseteq A \cap B$ . En d'autres termes, tout minorant de  $\{A, B\}$  est plus petit que  $A \cap B$ . Comme  $A \cap B \subseteq A$  et  $A \cap B \subseteq B$ , nous en déduisons que  $A \cap B$  est bien la borne inférieure de  $\{A, B\}$ .

**Borne supérieure** Même histoire.

**Bilan** Toute paire d'éléments de  $\mathcal{P}(E)$  admet une borne supérieure et une borne inférieure pour  $\subseteq$ . En d'autres termes,  $\mathcal{P}(E)$  est un treillis pour  $\subseteq$ .

**Exercice 2.** Considérons l'ensemble  $\mathbf{N}$  des entiers. Montrer que  $\mathbf{N}$ , ordonné par la divisibilité, est un treillis.

Comme précédemment, commençons par remarquer que  $\mathbf{N}$  est bien ordonné par la divisibilité  $|$ . Considérons deux éléments  $a$  et  $b$  dans  $\mathbf{N}$  et prouvons que  $\text{ppcm}(a, b)$  est la borne supérieure de  $\{a, b\}$  et  $\text{pgcd}(a, b)$  est la borne inférieure de  $\{a, b\}$ .

**Borne supérieure** Par définition,  $a | \text{ppcm}(a, b)$ ,  $b | \text{ppcm}(a, b)$  et pour tout  $c$  tel que  $a | c$  et  $b | c$ , on a  $\text{ppcm}(a, b) | c$ . Nous en déduisons que  $\text{ppcm}(a, b)$  est bien la borne supérieure de  $a$  et  $b$ .

**Borne inférieure** Même histoire.

**Bilan** Toute paire d'entiers admet une borne sup et une borne inf, ce qu'il fallait démontrer.

**Exercice 3. (environ 5 points)** Soit  $E$  un treillis. Montrer que  $\sqcup$  et  $\sqcap$  sont commutatives.

Nous noterons  $\preceq$  la relation d'ordre. Considérons  $a$  et  $b$  dans  $E$ .

**Min** Notons  $m = a \sqcup b$  et  $n = b \sqcup a$ . Alors, par définition,

- i.  $m \preceq a$
- ii.  $m \preceq b$
- iii.  $\forall k, k \preceq a \wedge k \preceq b \implies k \preceq m$
- iv.  $n \preceq a$
- v.  $n \preceq b$
- vi.  $\forall k, k \preceq a \wedge k \preceq b \implies k \preceq n$

D'après i., ii. et vi., nous déduisons que  $m \preceq n$ . D'après iv., v. et iii., nous déduisons que  $n \preceq m$ . Comme  $\preceq$  est une relation d'ordre, elle est réflexive. Nous en déduisons donc que  $n = m$ , c'est-à-dire que  $\sqcup$  est commutative.

**Max** Même histoire.

**Exercice 4. (environ 5 points)** Soit  $E$  un treillis. Montrer que  $\sqcup$  et  $\sqcap$  sont associatives.

Nous noterons  $\preceq$  la relation d'ordre. Considérons  $a, b$  et  $c$  dans  $E$ .

**Min** Notons  $m = a \sqcup (b \sqcup c)$ . Alors, par définition,

- i.  $m \preceq a$
  - ii.  $m \preceq b \sqcup c$
  - iii.  $\forall k, k \preceq a \wedge k \preceq b \sqcup c \implies k \preceq m$
- Notons alors  $m' = b \sqcup c$ . Alors, par définition,

- iv.  $m' \preceq b$
  - v.  $m' \preceq c$
  - vi.  $\forall k, k \preceq b \wedge k \preceq c \implies k \preceq m'$
- De même, avec  $n = (a \sqcup b) \sqcup c$  et  $n' = a \sqcup b$ , nous avons

- vii.  $n \preceq n'$
- viii.  $n \preceq c$
- ix.  $\forall k, k \preceq n' \wedge k \preceq c \implies k \preceq n$
- x.  $n' \preceq a$
- xi.  $n' \preceq b$
- xii.  $\forall k, k \preceq a \wedge k \preceq b \implies k \preceq n'$

Comme  $\preceq$  est une relation d'ordre, elle est transitive. En particulier, d'après i., ii., iv. et v., nous avons  $m \preceq a$ ,  $m \preceq b$  et  $m \preceq c$ . D'après xii., nous en déduisons que  $m \preceq n'$ . D'après ix. nous en déduisons de plus que  $m \preceq n$ .

De la même manière, nous prouvons que  $n \preceq m$ .

Comme  $\preceq$  est une relation d'ordre, elle est antisymétrique. En particulier, comme  $m \preceq n$  et  $n \preceq m$ , nous pouvons déduire que  $m = n$ . C'est-à-dire que  $\sqcup$  est associative.

**Max** C'est la même histoire.

**Exercice 5. (environ 3 points)** Soit  $E$  un treillis. Montrer que  $\forall x, y \in E, x \sqcap (x \sqcup y) = x = (x \sqcap y) \sqcup x$ .

Soient  $x$  et  $y$  dans  $E$ . Notons  $m = x \sqcap (x \sqcup y)$ ,  $m' = x \sqcup y$ ,  $n = (x \sqcap y) \sqcup x$  et  $n' = x \sqcap y$ . Alors, par définition

- i.  $x \preceq m$
- ii.  $m' \preceq m$
- iii.  $\forall k, x \preceq k \wedge m' \preceq k \implies m \preceq k$

- iv.  $m' \preceq x$
- v.  $m' \preceq y$
- vi.  $\forall k, k \preceq x \wedge k \preceq y \implies k \preceq m'$

Commençons par remarquer que  $x \preceq x$  et, par iv.,  $m' \preceq x$ . De iii., nous déduisons donc que  $m \preceq x$ . Or, d'après i., nous avons aussi  $x \preceq m$ . Par conséquent, comme  $\preceq$  est antisymétrique, nous déduisons  $m = x$ .

L'autre moitié est du même genre.

## Projections

**Définition 2.** Si  $E$  et  $F$  sont deux ensembles, on définit les fonctions de projection  $\pi_1: E \times F \rightarrow E$  et  $\pi_2: E \times F \rightarrow F$  par  $\forall (e, f) \in E \times F, \pi_1(e, f) = e$  et  $\pi_2(e, f) = f$ .

**Exercice 6.** Prouver que cette définition de  $\pi_1$  (respectivement  $\pi_2$ ) est bien une définition de fonction.

On pourra commencer par réécrire  $\pi_1$  (respectivement  $\pi_2$ ) sous la forme d'une correspondance  $\{E \times F, E, \Gamma_1\}$  (respectivement  $\{E \times F, F, \Gamma_2\}$ ) et prouver que cette correspondance est bien une fonction.

Notons  $\pi_1 = \{E \times F, E, \Gamma_1\}$  où  $\forall (e, f) \in E \times F, \Gamma_1(\{(e, f)\}) = \{e\}$ . Par définition d'une fonction, pour prouver que  $\pi_1$  est une fonction, il suffit donc de prouver que pour tout couple  $(e, f)$  de  $E \times F$ ,  $\Gamma_1(\{(e, f)\})$  est soit vide, soit un singleton. Comme il s'agit toujours du singleton  $\{e\}$ ,  $\pi_1$  est effectivement une fonction.

Même histoire pour  $\pi_2$ .

**Exercice 7.** Les fonctions  $\pi_1$  et  $\pi_2$  sont elles injectives ? surjectives ? prouvez-le.

**Injectivité** Si l'ensemble  $E$  contient au moins deux éléments distincts  $\{a, b\}$  et  $F$  contient au moins un élément  $\{f\}$ , alors  $\pi_2(a, f) = f = \pi_2(b, f)$  donc  $\pi_2$  n'est pas injective. De même, si  $F$  contient au moins deux éléments distincts et  $E$  au moins un élément,  $\pi_1$  n'est pas injective.

À l'inverse, si  $E$  et  $F$  contiennent tous les deux au plus un élément,  $E \times F$  contient au plus un élément,  $\pi_1$  et  $\pi_2$  sont bien injectives. Il s'agit d'un cas dégénéré.

**Surjectivité** Soient  $e$  dans  $E$  et  $f$  dans  $F$ . Alors  $\pi_1(e, f) = e$  et  $\pi_2(e, f) = f$ . En d'autres termes,  $e$  admet un antécédent par  $\pi_1$  dans  $E \times F$  et  $f$  admet un antécédent par  $\pi_2$  dans  $E \times F$ . Ce qui signifie que  $\pi_1$  et  $\pi_2$  sont surjectives.

## Numérotation hexadécimale

La numérotation hexadécimale est une notation des nombres qui, au lieu d'utiliser les chiffres de 0 à 9, comme la numérotation décimale, emploie les seize chiffres  $\bar{0}, \bar{1}, \dots, \bar{9}, \bar{a}, \bar{b}, \dots, \bar{f}$ . Ainsi, le nombre 0 s'écrit  $\bar{0}$  en hexadécimal, le nombre 9 s'écrit  $\bar{9}$ , le nombre 15 s'écrit  $\bar{f}$  et le nombre 255 s'écrit  $\bar{ff}$ .

**Exercice 8.** Définir par induction l'ensemble  $\mathcal{H}$  des nombres hexadécimaux.

$\mathcal{H}$  peut se définir par induction en employant comme base l'ensemble des chiffres  $\mathcal{C} = \{\bar{0}, \bar{1}, \dots, \bar{9}, \bar{a}, \bar{b}, \dots, \bar{f}\}$  et comme opérateurs d'induction la concaténation.

**Exercice 9.** Définir par induction la fonction  $v: \mathcal{H} \rightarrow \mathbf{N}$  qui à tout nombre hexadécimal associe sa valeur.

$$\text{On pourra employer } v \text{ définie par } \begin{cases} v(\bar{0}) = 0 \\ v(\bar{1}) = 1 \\ \vdots \\ v(\bar{f}) = 15 \\ v(x \cdot y) = 16 \times v(x) + v(y) \end{cases}$$

# Logique

**Exercice 10. (environ 8 points)** Dans le cadre de la logique des propositions, prouver que, pour toute formule  $f$ ,  $\emptyset \vdash (\text{NON } f) \text{ IMPLIQUE } f$ .

Ceci n'est pas prouvable.

En effet, si nous supposons que ceci était prouvable, nous pourrions en déduire que  $\emptyset \vDash (\text{NON } f) \text{ IMPLIQUE } f$  donc, en particulier, avec une variable  $a$ , que  $(\text{NON } a) \text{ IMPLIQUE } a$  est une tautologie. En d'autres termes, en interprétant  $a$  comme  $F$ , on aurait  $V \text{ IMPLIQUE } F \text{ est vrai}$ , ce qui est absurde.

Nous en déduisons donc qu'il s'agissait d'une question piège.

**Exercice 11. (environ 6 points)** Dans le cadre de la logique des propositions, prouver que, pour toutes formules  $f$  et  $g$ ,  $\emptyset \vDash (f \text{ ET } (f \text{ IMPLIQUE } g)) \text{ IMPLIQUE } g$ .

Soit une interprétation  $I$ . Alors

- si  $I(f) = V$  et  $I(g) = V$ ,  $I((f \text{ ET } (f \text{ IMPLIQUE } g)) \text{ IMPLIQUE } g) = V$  (car  $I(h \text{ IMPLIQUE } g)$  est  $V$  dès que  $I(g) = V$ )
- si  $I(f) = F$  et  $I(g) = V$ ,  $I((f \text{ ET } (f \text{ IMPLIQUE } g)) \text{ IMPLIQUE } g) = V$  pour les mêmes raisons
- si  $I(f) = V$  et  $I(g) = F$ ,  $I((f \text{ ET } (f \text{ IMPLIQUE } g)) \text{ IMPLIQUE } g) = V$  (car  $I(h \text{ IMPLIQUE } i)$  est  $V$  dès que  $I(h) = F$ , avec ici  $h = f \text{ ET } \dots$ , qui est  $F$  dès que  $I(f)$  est  $F$ .)
- si  $I(f) = F$  et  $I(g) = F$ ,  $I((f \text{ ET } (f \text{ IMPLIQUE } g)) \text{ IMPLIQUE } g) = V$  pour les mêmes raisons.

En d'autres termes, dans tous les cas,  $I((f \text{ ET } (f \text{ IMPLIQUE } g)) \text{ IMPLIQUE } g) = V$ . Le séquent est donc valide.

**Exercice 12. (environ 16 points)** Si nous souhaitions définir un ensemble de règles de déduction pour la logique des prédicats, parmi les règles suivantes, lesquelles devrions-nous utiliser ? Justifiez vos choix à l'aide d'arguments simples.

Notez que ces règles ne suffisent pas.

- i.  $\frac{P \vdash (x \text{ DANS } E) \text{ IMPLIQUE } f(x)}{P \vdash \text{ POUR TOUT } x \text{ DANS } E, f(x)}$
- ii.  $\frac{P \vdash (x \text{ DANS } E) \text{ IMPLIQUE } f(x)}{P \vdash \text{ POUR TOUT } x \text{ DANS } E, f(x)}$   $x$  apparaît dans  $P$
- iii.  $\frac{P \vdash (x \text{ DANS } E) \text{ IMPLIQUE } f(x)}{P \vdash \text{ POUR TOUT } x \text{ DANS } E, f(x)}$   $x$  n'apparaît pas dans  $P$
- iv.  $\frac{P \vdash f(x)}{P \vdash \text{ POUR TOUT } x \text{ DANS } E, f(x)}$   $x \in E$
- v.  $\overline{P \vdash x \text{ DANS } E} \quad x \in E$
- vi.  $\overline{P \vdash \text{ IL EXISTE } x \text{ DANS } E, f(x)} \quad x \in E$
- vii.  $\frac{P \vdash x \text{ DANS } E \quad P \vdash f(x)}{P \vdash \text{ IL EXISTE } x \text{ DANS } E, f(x)}$
- viii.  $\frac{P \vdash y \text{ DANS } E \quad P \vdash f(y)}{P \vdash \text{ IL EXISTE } x \text{ DANS } E, f(x)}$   $x$  apparaît dans  $P$
- ix.  $\frac{P \vdash y \text{ DANS } E \quad P \vdash f(y)}{P \vdash \text{ IL EXISTE } x \text{ DANS } E, f(x)}$   $x$  n'apparaît pas dans  $P$

- x.  $\frac{P \vdash y \text{ DANS } E \quad P \vdash f(y)}{P \vdash \text{IL EXISTE } x \text{ DANS } E, f(x)}$
- xi.  $\frac{P \vdash y \text{ DANS } E \quad P \vdash f(y)}{P \vdash \text{IL EXISTE } x \text{ DANS } E, f(x)}$   $y$  apparaît dans  $P$
- xii.  $\frac{P \vdash y \text{ DANS } E \quad P \vdash f(y)}{P \vdash \text{IL EXISTE } x \text{ DANS } E, f(x)}$   $y$  n'apparaît pas dans  $P$

Les règles intéressantes correspondent à ce que vous faites en mathématiques lorsque vous rédigez des preuves.

- iii. (“pour prouver que pour tout  $x$  dans  $E$ ,  $f(x)$  est vrai, il suffit de prouver que, si nous supposons  $x$  dans  $E$ , alors  $f(x)$  est bien vrai – le tout sans aucune autre hypothèse sur  $x$ ”).
- v. (“si  $x \in E$  alors on peut prouver que  $x$  DANS  $E$ ”)
- ix. (“pour prouver qu’il existe  $x$  dans  $E$  tel que  $f(x)$  est vrai, il suffit de trouver un  $y$  dans  $E$ , de prouver qu’on a bien  $f(y)$  – sans aucune hypothèse sur  $x$ , puisque nous n’avons pas encore prouvé l’existence de  $x$ ”). En pratique, cette règle est un peu trop restrictive car elle interdit à  $y$  et  $x$  d’être le même nom.  
En pratique, on emploiera donc une règle légèrement plus complexe, appelée l’ “introduction de  $\exists$ ”.

Citons en vitesse quelques aberrations :

- iv. est une confusion entre  $\exists$  et  $\forall$
- vi. oublie de prouver que  $f(x)$  est vrai
- vii. force à prouver que  $x \in E$  – exactement avec le nom  $x$ .

Moins aberrant mais faux tout de même :

- ii. si  $x$  apparaît dans  $P$ , on a fait des hypothèses sur  $x$  – avant d’avoir déclaré ce qu’était  $x$
- viii. si  $x$  apparaît dans  $P$ , on a fait des hypothèses sur  $x$  – avant d’avoir prouvé l’existence de  $x$
- xi. il n’est pas obligatoire que  $y$  apparaisse dans  $P$ . Par exemple, pour prouver que  $1 = 1$  (avec 1 dans le rôle de  $y$ ), il n’est pas nécessaire d’avoir des hypothèses sur 1. Par contre, on aura quelque chose du genre  $\forall z, z = z$  dans  $P$ .
- xii. il faut que  $y$  vienne de quelque part, donc  $y$  apparaîtra probablement dans  $P$ .

Et enfin, les presque vraies :

- i. et x., à peu près pour la même raison que viii.