Mathématiques discrètes

Définition généreuse : tous les théorèmes qui ne parlent pas d'analyse, i.e. de ϵ aussi petit qu'on veut.

Plan approximatif du semestre :

1. Théorie axiomatique des ensembles, 6 séances (le plus difficile du cours, ne prenez pas de retard)
2. Combinatoire
3. Théorie des ordres
4. Récurrences structurelles
5. Monoïdes
6. Introduction aux probabilités.
7. Chaînes de Markov.

Théorie des ensembles

Plan approximatif :

1. les axiomes et leurs conséquences directes
2. Les ordinaux
3. Les cardinaux
4. Récurrence bien fondée
5. L'axiome du choix.

Maths discrètes : détails pratiques

Évaluation, en première approximation :

- 10 DM courts (dont 6 sur les 6 séances théorie des ensembles), moyenne des 7 meilleurs (25%)
- Un partiel (35%) sans document, le 18 octobre.
- Un examen (40%) sans document.
- En TD, DM, examen, les preuves sont importantes : structure, détail, intuition, écriture soignée.
- Les notes du contrôle continu (DM 25%), ne compteront pas lors de la deuxième session.

Remarque : les DM sont à rendre individuellement (LateX ou écriture soignée), mais je vous incite à parler des DM entre vous avant de vous lancer dans l'écriture.

Chapitre I : Théorie axiomatique des ensembles

Stéphane Le Roux stephane.le_roux@ens-paris-saclay.fr

ENS Paris-Saclay

2023-2024

Pourquoi ce chapitre est intéressant (j'espère)

- Si vous poursuivez ensuite l'étude de la théorie des ensembles ou de la logique au sens large, ce chapitre est une petite introduction utile.
- Sinon, pour un.e informaticien.ne qui lit ou produit des preuves mathématiques sur des concepts informatiques, il est bon d'avoir vu au moins une fois dans sa vie sur quoi se base l'outil mathématique.

Paradoxes mathématiques

- Jusqu'au début du 20ème siècle : théorie naïve des ensembles.
- À l'époque, les maths de tous les jours étaient un mélange de langue naturelle et de formules.
- Découverte de paradoxes mathématiques, par exemple le paradoxe de Russell (1901) : soit $A := \{x \mid x \notin x\}$. Alors $A \in A$ ssi A est un x tel que $x \notin x$, ssi $A \notin A$.
- Ayant prouvé l'absurde, on pouvait alors prouver quelque chose et son contraire, donc toutes les affirmations mathématiques étaient vraies.
- D'où un besoin de formaliser précisément les maths pour arriver à une théorie (utile) où tout n'est pas vrai. Une telle formalisation dirait quels objets on a le droit de définir et comment on a le droit de les manipuler : axiomes "concrets" + règles de déduction.

Règle de déduction

Cf cours de logique au second semestre

Règles de déduction, exemples :

$$\frac{A \quad A \Rightarrow B}{B} \qquad \frac{A \quad B}{A \wedge B} \qquad \frac{A \wedge B}{A}$$

Axiomes abstraits, exemple :

$$\frac{}{A \Rightarrow A}$$

Arbre de déduction, exemple :

$$\dfrac{\dfrac{\dfrac{}{A \Rightarrow A} \qquad \dfrac{}{B \Rightarrow B}}{A \Rightarrow A \wedge B \Rightarrow B}}{A \Rightarrow A}$$

Dans ce chapitre :

- On donne à A, B, $A \Rightarrow B$, etc, un contenu mathématique plus concret exprimé formellement en théorie des ensembles.
- On n'écrit pas d'arbres de dérivation : on manipule des contenus formels de manière relativement informelle, comme dans une preuve de maths habituelle.

Formalisation des mathématiques

- Plusieurs formalisations possibles :
  - Les ensembles dans la théorie des ensembles, comme dans ce cours.
  - Les fonctions dans la théorie des types.
  - Les morphismes dans la théorie des catégories.
- Ces formalisations ont rassuré les mathématicien.nes.
- Aujourd'hui, les maths de tous les jours sont encore un mélange de langue naturelle et de formules.
  - Même pour les gens qui étudient la théorie des ensembles, qui étudient partiellement informellement un système formel.
  - Sauf pour les preuves formelles vérifiées par ordinateur (dans tous les domaines des mathématiques).
- La théorie des ensembles est construite sur la logique classique du premier ordre avec égalité (cf cours de logique au second semestre), qui permet de manipuler les objets logiques de manière précise.

Le langage primitif

Pour parler de théorie des ensembles

La signature (i.e. les lettres) du langage est constituée, d'une part, des symboles de la logique sous-jacente :

- Connecteurs logiques : $\neg$, $\wedge$
- Quantificateur universel : $\forall$
- Symbole d'égalité $=$
- Symboles de variable : $a, b, x, y, A, \alpha...$

Et d'autre part de l'unique symbole de la théorie des ensembles : l'appartenance $\in$.

Les formules du langage, i.e. les mots valides, sont définis par récurrence.

- $(a = b)$ et $(a \in b)$ sont des formules.
- Si ϕ et ψ sont des formules, alors $(\neg\phi)$ et $(\phi \wedge \psi)$ et $(\forall x \phi)$ aussi.
- On omet les parenthèses (en particulier externes) quand il n'y a pas d'ambiguité.

Notations

Notations logiques : parfois,

- $\neg((\neg\phi) \wedge (\neg\psi))$ est noté $\phi \vee \psi$
- $(\neg\phi) \vee \psi$ est noté $\phi \Rightarrow \psi$
- $(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi)$ est noté $\phi \Leftrightarrow \psi$
- $\neg\forall x(\neg\phi)$ est noté $\exists x\phi$
- $\exists x((x \in a) \wedge \phi)$ est noté $(\exists x \in a)\phi$
- $\forall x((x \in a) \Rightarrow \phi)$ est noté $(\forall x \in a)\phi$
- $(\forall x \in a)(\forall y \in a)\phi$ est noté $(\forall x, y \in a)\phi$. (De même pour $\exists$)
- $\neg(a = b)$ est noté $a \neq b$.

Notation ensembliste :

- $\neg(a \in b)$ est noté $a \notin b$.
- $\forall x(x \in a \Rightarrow x \in b)$ est noté $a \subseteq b$

Variables libres, variables liées

- Les variables libres d'une formule sont définies par récurrence.
  - Les formules $x = y$ et $x \in y$ ont x et y pour variables libres.
  - Les variables libres de $\neg\phi$ sont les mêmes que celles de ϕ
  - les variables libres de $\phi \wedge \psi$ sont celles de ϕ et celles de ψ.
  - Les variables libres de $\forall x \phi$ sont celles de ϕ sauf x.
- Les variables liées sont définies par récurrence.
  - Les formules $x = y$ et $x \in y$ n'ont pas de variables liées.
  - Les variables liées de $\neg\phi$ sont les mêmes que celles de ϕ
  - les variables liées de $\phi \wedge \psi$ sont celles de ϕ et celles de ψ.
  - Les variables liées de $\forall x \phi$ sont celles de ϕ plus x.
- Une variable peut-être à la fois libre et liée dans une même formule, par exemple x dans $(x = x) \wedge \forall x(x = x)$, mais c'est une bonne pratique de l'éviter.

Encore des notations

- Une formule ϕ pourra être écrite $\phi(x_1, \ldots, x_n)$ si ses variables libres sont parmi les x_i.
- Si x est une variable non liée dans une formule ϕ, alors pour toute variable y fraîche (i.e. pas dans ϕ), on dénote par $\phi[x \leftarrow y]$ la formule dans laquelle x a été remplacé par y.
- Si x est la seule variable libre de ϕ, alors par abus de notation, on abrège souvent $\phi[x \leftarrow y]$ en $\phi(y)$.
- $(\exists x \in a)\phi \wedge (\forall y, z \in a)((\phi[x \leftarrow y] \wedge \phi[x \leftarrow z]) \Rightarrow y = z)$ est noté $(\exists! x \in a)\phi$
- On peut utiliser un langage logique légèrement différent mais équivalent : $\Rightarrow$ est primitif, et ainsi qu'un symbole $\perp$ appelé "absurde", tel que $\neg\phi$ est une notation pour $\phi \Rightarrow \perp$.

Manipulation des formules

Vous verrez en cours de logique comment dériver formellement des théorèmes à partir des axiomes, dans plusieurs sytèmes différents et pas toujours équivalents.

Rappel : le sytème sous-jacent ici s'appelle la logique classique du premier ordre avec égalité.

Dans cette logique, $\neg\neg\phi$ et ϕ sont équivalentes, i.e. $\neg\neg\phi \Leftrightarrow \phi$. De même pour $\phi \wedge \psi$ et $\psi \wedge \phi$, etc.

Dans cette logique, si $x = y$ et $\phi(x, p_1, \ldots, p_n)$, alors $\phi(y, p_1, \ldots, p_n)$.
Sans abus de notation : si $x = y$ et $\phi(x, p_1, \ldots, p_n)$, alors $\phi[x \leftarrow y]$.

Nous allons manipuler les formules de manière habituelle (i.e. relativement informelle) lors de nos raisonnements purement logiques, mais de manière particulièrement prudente lors de nos raisonnements ensemblistes.

Axiomes de Zermelo-Fraenkel et axiome du choix (I)

ZF + AC = ZFC

- Axiome d'extensionnalité : $\forall a \forall b (\forall x (x \in a \Leftrightarrow x \in b) \Rightarrow a = b)$.
  - On note que l'implication inverse est vraie par la logique qu'on utilise.
  - On vérifie que $a \subseteq b$ et $b \subseteq a$ collectivement impliquent $a = b$.
- Axiome de l'ensemble vide : $\exists a \forall b (\neg b \in a)$.
  - Un tel ensemble a est unique par l'axiome d'extensionnalité.
  - On le note $\emptyset$.
  - On vérifie que $\emptyset \subseteq c$ pour tout c.
  - On vérifiera que $\{\emptyset\} \neq \emptyset$ quand on aura introduit la notation $\{\}$.

Axiomes de Zermelo-Fraenkel et axiome du choix (II)

ZF + AC = ZFC

Axiome de la paire : $\forall a \forall b \exists c (\forall x (x \in c \Leftrightarrow (x = a \vee x = b)))$.

- L'ensemble c est unique par l'axiome d'extensionnalité.
- On le note $\{a, b\}$.
- Le singleton $\{a\}$ est défini par $\{a, a\}$.
- $\{a, b\} = \{b, a\}$, par l'axiome d'extensionnalité.
- Le couple (a, b) est défini par $\{\{a\}, \{a, b\}\}$. On vérifie que $(a, b) = (c, d)$ ssi $a = c$ et $b = d$.
- (a, b, c) est une défini par $((a, b), c)$.
- Pour tout $x_1, \ldots, x_n$ avec $n \geq 3$, on pose $(x_1, \ldots, x_n) := ((x_1, \ldots, x_{n-1}), x_n)$.
  - Ici, l'entier n n'est pas défini dans la théorie, mais au niveau meta : c'est un n informel. (On définira les entiers naturels dans la théorie plus tard.)
  - Cette définition exclut les 0-uplets et 1-uplets.

Axiomes de Zermelo-Fraenkel et axiome du choix (III)

ZF + AC = ZFC

Axiome de la réunion : $\forall a \exists b \forall c (c \in b \Leftrightarrow \exists d (c \in d \wedge d \in a))$.

- L'ensemble b est unique par l'axiome d'extensionnalité.
- On le note $\cup a$.
- On vérifie que $\cup \emptyset = \emptyset$. (C'est une propriété, pas une convention !)
- On vérifie que $\cup \{a\} = a$.
- $a \cup b$ est défini par $\cup \{a, b\}$.
- On vérifie les propriétés algébriques suivantes.
  - $\forall x (x \in a \cup b \Leftrightarrow (x \in a \vee x \in b))$
  - $a \cup b = b \cup a$
  - $a \cup \emptyset = a$
  - $(a \cup b) \cup c = a \cup (b \cup c)$.
  - $(\cup a) \cup (\cup b) = \cup (a \cup b)$.
  - Si $a \subseteq b$, alors $\cup a \subseteq \cup b$.
- $\{a, b, c\}$ est défini par $\{a, b\} \cup \{c\}$, etc.
- On vérifie que $\{a, b, c\} = \{b, a, c\} = \{a, c, b\}$, etc.

Axiomes de Zermelo-Fraenkel et axiome du choix (IV)

ZF + AC = ZFC

Axiome de l'infini : $\exists a(\forall b(\forall c(\neg c \in b) \Rightarrow b \in a) \wedge \forall x \in a(x \cup \{x\} \in a))$

- Dans l'axiome de l'infini, on peut remplacer $\forall b(\forall c(\neg c \in b) \Rightarrow b \in a)$ par $\emptyset \in a$. On obtient $\exists a(\emptyset \in a \wedge \forall x \in a(x \cup \{x\} \in a))$. Cette version plus lisible est a priori plus forte que la première version, mais elles sont en fait équivalentes relativement au système d'axiome, si on suppose que l'ensemble vide existe.

Axiomes de Zermelo-Fraenkel et axiome du choix (V)

ZF + AC = ZFC

Schéma d'axiome de séparation :

- Pour toute formule $\phi(x, p)$, on admet l'axiome $\forall p \forall A \exists B \forall x (x \in B \Leftrightarrow (x \in A \wedge \phi))$.
- L'ensemble p est appelé un paramètre.
- L'ensemble B est unique par extensionnalité et est noté $\{x \in A \mid \phi(x, p)\}$ ou $\{x \in A \mid \phi\}$.
- On a une infinité d'axiomes construits d'après le même schéma.

Theorem

Le schéma d'axiome de séparation et l'axiome de l'infini impliquent collectivement l'axiome de l'ensemble vide.

Proof.

Par l'axiome de l'infini, il existe un ensemble a. Soit ϕ la formule $x \neq x$. D'après l'axiome de séparation, soit e l'ensemble $\{x \in a \mid \phi(x)\}$. Pour tout $x \in e$, par définition on a $x \neq x$, contradiction, donc e est vide. □

L'ensemble de tous les ensembles

n'existe pas (cf paradoxe de Russell)

Theorem

La collection de tous les ensembles n'est pas un ensemble. Plus formellement, on peut prouver $\neg\exists e\forall x(x \in e)$.

Proof.

Vers une contradiction, supposons $\exists e\forall x(x \in e)$. *(Alors* $e \in e$, *mais ce n'est pas une contradiction dans le système axiomatique actuel.) D'après l'axiome de séparation, soit l'ensemble* $a := \{x \in e \mid \phi(x)\}$ *avec* $\phi := x \notin x$. *Alors* $a \in a$ *ssi* a *est un* $x \in e$ *tel que* $\phi(x)$, *ssi* $\phi(a)$ *(car* $a \in e$*). Or* $\phi(a)$ *ssi* $a \notin a$, *contradiction.* □

La collection de tous les ensembles est appelée l'univers. (En théorie des classes, l'univers est une classe propre, comme toute collection trop grande pour être un ensemble.)

Renforcer l'axiome de séparation ?

Theorem

Dans l'axiome de séparation $\forall p \forall A \exists B \forall x (x \in B \Leftrightarrow (x \in A \wedge \phi(x, p)))$ *on ne peut pas se passer de A. Plus pécisément, ajouter l'axiome* $\exists B \forall x (x \in B \Leftrightarrow \phi(x))$ *pour toute formule* ϕ *est contradictoire.*

Proof.

(Un tel ensemble B serait noté $\{x \mid \phi(x, p)\}$*, et non plus* $\{x \in A \mid \phi(x, p)\}$*.)*
Soit $\phi(x, p) := (x = x)$*, alors l'axiome est* $\exists B \forall x (x \in B \Leftrightarrow x = x)$*, ce qui équivaut à* $\exists B \forall x (x \in B)$*, i.e. B est l'ensemble de tous les ensembles, absurde.* □

L'axiome de séparation avec plusieurs paramètres

- Soit *SAS* le schéma d'axiome de séparation qui admet $\forall p \forall A \exists B \forall x (x \in B \Leftrightarrow (x \in A \wedge \phi))$ pour tout $\phi(x, p)$.
- Soit SAS^+ le schéma qui pour toute formule $\phi(x, p_1, \ldots, p_n)$ admet l'axiome $\forall p_1, \ldots, p_n \forall A \exists B \forall x (x \in B \Leftrightarrow (x \in A \wedge \phi))$.

Theorem

SAS implique SAS^+.

Proof.

On suppose SAS. Soient des ensembles $p_1, \ldots, p_n$ *et A. Montrons que* $\exists B \forall x (x \in B \Leftrightarrow (x \in A \wedge \phi))$. *On construit un témoin B via SAS. Pour cela, soit* $\psi(x, p) := \exists y_1, \ldots, y_n (p = (y_1, \ldots, y_n) \wedge \phi(x, y_1, \ldots, y_n))$. *Par SAS, en prenant* $p := (p_1, \ldots, p_n)$, *soit B tel que* $x \in B \Leftrightarrow (x \in A \wedge \psi[p \leftarrow (p_1, \ldots, p_n)])$. *Or* $\psi[p \leftarrow (p_1, \ldots, p_n)] \Leftrightarrow \phi$, *d'où le résultat.* □

Axiomes de Zermelo-Fraenkel et axiome du choix (VI)

ZF + AC = ZFC

Axiome de l'ensemble des parties : $\forall a \exists b \forall c (c \subseteq a \Leftrightarrow c \in b)$.

- L'ensemble b est unique par l'axiome d'extensionnalité.
- On le note $\mathcal{P}(a)$.
- On vérifie que $\mathcal{P}(\emptyset) = \{\emptyset\}$.
- On vérifie que $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Theorem

Il n'existe pas d'ensemble E tel que $\mathcal{P}(E) \subseteq E$.

Proof.

Vers une contradiction, soit E un tel ensemble. Soit $A := \{x \in E \mid x \notin x\}$. $A \in \mathcal{P}(E)$ donc $A \in E$.

- *Si $A \in A$, alors $A \notin A$, contradiction.*
- *Si $A \notin A$, alors $A \in A$, car $A \in E$, contradiction.*

□

Concepts traditionels qu'on peut traiter dès à présent.

Intersection

- Par axiome de séparation, on peut définir $\cap a := \{x \in \cup a \mid \forall y \in a(x \in y)\}$.
- On pose $a \cap b = \cap\{a, b\}$.
- On vérifie que
  - $x \in a \cap b$ ssi $x \in a$ et $x \in b$.
  - $b \cap a = a \cap b$.
  - $\cap\{a\} = a$.
  - $(a \cap b) \cap c = a \cap (b \cap c)$.
  - Les lois de De Morgan (union-intersection).
- Attention, ici $\cap\emptyset = \emptyset$, et non pas l'univers entier. Si tous les ensembles qu'on considère sont sous-ensembles d'un ensemble E, on peut définir $\cap_E a := \{x \in E \mid \forall y \in a(x \in y)\}$, auquel cas $\cap_E\emptyset = E$.
- Attention :
  - $a \subseteq b$ implique $\cap b \subseteq \cap a$ par exemple si $a \neq \emptyset$ ou $b = \emptyset$, mais pas en général.
  - On n'a pas $(\cap a) \cap (\cap b) = \cap(a \cap b)$ en général.

Intersection (II)

- Si $x \subseteq y$ pour tout $y \in b \neq \emptyset$, alors $x \subseteq \cap b$.
- $a \setminus b$: Par axiome de séparation on peut définir $a \setminus b := \{x \in a \mid x \notin b\}$.
- Un ensemble A est dit co-initial pour l'inclusion dans un ensemble B, si $A \subseteq B$ et pour tout $y \in B$, il existe $x \in A$ tel que $x \subseteq y$.

Theorem

Si A est co-initial pour l'inclusion dans B, alors $\cap A = \cap B$.

Proof.

Si A est vide alors B aussi et on a le résultat. On suppose maintenant A non vide, donc B est aussi non vide.

Par double inclusion.

- *de $A \subseteq B$ on déduit $\cap B \subseteq \cap A$, car A est non vide.*
- *Pour tout $y \in B$, il existe $x \in A$ tel que $x \subseteq y$, et donc $\cap A \subseteq \cap\{x\} = x \subseteq y$. Ainsi, $\cap A \subseteq \cap B$.*

Produit cartésien

- On définit le produit cartésien par $a \times b := \{z \in \mathcal{P}(\mathcal{P}(a \cup b)) \mid \exists x \in a \exists y \in b(z = (x, y))\}$.
- Avec $a = \{x, y\}$ et $b = \{z\}$, on a bien $a \times b = \{(x, z), (y, z)\} = \{\{\{x\}, \{x, z\}\}; ; \{\{y\}, \{y, z\}\}\}$ et $\mathcal{P}(a \cup b) = \{\{x\}, \{y\}, \ldots \{x, y, z\}\}$ et $\mathcal{P}(\mathcal{P}(a \cup b)) = \{\{\{x\}, \{y\}\}; ; \{\{x\}\}; ; \{\{x\}, \{y, z\}\}; ; \{\{x\}, \{x, z\}\}; ; \ldots\}$.
- $a \times b \times c := (a \times b) \times c$, etc.
- Attention : on n'a pas $a \times (b \times c) = (a \times b) \times c$, car $(x, (y, z)) \neq ((x, y), z)$ a priori. Mais en maths usuel, on identifie les deux ensembles, car il existe une bijection simple entre eux.
- Notation : $a^1 := a$ et pour tout n on pose $a^{n+1} := a^n \times a$.

Relations

- Une relation n-aire est un ensemble de n-uplets.
- Exemple: soit $\phi(R) := \forall t \in R \exists, x, y, z(t = (x, y, z))$.
- Une relation n-aire sur des ensembles $E_1, \ldots, E_n$ est un ensemble $R \subseteq E_1 \times \cdots \times E_n$.
- Si $E_i \subseteq E_i'$ pour tout i, alors R est aussi une relation sur $E_1', \ldots, E_n'$.
- Les relations qui sont des sous-ensembles de $E_1 \times \cdots \times E_n$ constituent exactement l'ensemble $\mathcal{P}(E_1 \times \cdots \times E_n)$.
- On peut écrire $R(x_1, \ldots, x_n)$ au lieu de $(x_1, \ldots x_n) \in R$.
- Si $R \in \mathcal{P}(E_1 \times E_2)$, on dit que R est binaire , et on peut écrire xRy au lieu de $R(x, y)$.
- Alors E_1 est un domaine de R, et E_2 un codomaine.
- $E_1' \supseteq E_1$ est un autre domaine possible. Il sera parfois utile de préciser R binaire sur E_1, E_2. (Certains parlent de la relation (R, E_1, E_2).)

Relations (II)

Soit R une relation binaire.

- L'ensemble des composantes des couples de R est $\cup\cup R$. Par exemple, pour $R := \{(x, y), (a, b)\} = \{\{\{x\}, \{x, y\}\}; ; \{\{a\}, \{a, b\}\}\}$, on a $\cup R = \{\{x\}, \{x, y\}, \{a\}, \{a, b\}\}$ et $\cup\cup R = \{x, y, a, b\}$.
- Le domaine actif de R est l'ensemble $dom(R) := \{x \in \cup\cup R \mid \{x\} \in \cup R\}$.
- Le codomaine actif de R est l'ensemble $cod(R) := \{y \in \cup\cup R \mid \exists x \in dom(R)(xRy)\}$.
- $dom(R)$ et $cod(R)$ ne dépendent pas des domaines et codomaines annoncés/possibles de R.
- R^{-1} est la relation inverse de R, i.e. $R^{-1} := \{(y, x) \in cod(R) \times dom(R) \mid (x, y) \in R\}$.
- $dom(R^{-1}) = cod(R)$ et $cod(R^{-1}) = dom(R)$.
- $(R^{-1})^{-1} = R$

Fonctions

- Une relation binaire f est une fonction si $\phi(f)$ est vrai, où $\phi(f) := \forall x, y, z((xfy \wedge xfz) \Rightarrow y = z)$.
- Dans ce cas, on écrit $f(x) = y$ au lieu de $(x, y) \in f$ ou xfy.
- Si f est une fonction et A un ensemble, alors $\{(x, y) \in f \mid x \in A\}$ est un ensemble noté $f|_A$ et appelé la restriction de f à A.
- Les $f|_A$ avec $A \subseteq dom(f)$ constituent un ensemble : $\{g \in \mathcal{P}(dom(f) \times cod(f)) \mid \exists A \subseteq dom(f)(g = f|_A)\}$.
- Si f est une fonction et A un ensemble, alors
  - $\{y \in cod(f) \mid \exists x \in A(f(x) = y)\}$ est un ensemble noté $f[A]$ et appelé l'image de A par f.
  - $\{x \in dom(f) \mid f(x) \in A\}$ est un ensemble noté $f^{-1}[A]$ et appelé l'image réciproque ou pré-image de A par f.
- Une fonction f est dite injective si la relation binaire f^{-1} est une fonction. Dans ce cadre, la surjectivité n'a pas de sens.

Applications

- Si $dom(f) = A$ et $cod(f) \subseteq B$, on peut écrire $f : A \to B$. On dit alors que f, ou plutôt (f, A, B), est une application (totale) de l'ensemble de départ A vers l'ensemble d'arrivée B.
- Si $dom(f) \subseteq A$ et $cod(f) \subseteq B$, on peut écrire (notation pas universel) $f : A \rightharpoonup B$. Alors f, ou plutôt (f, A, B), est dite application partielle.
- Une application partielle $f : A \rightharpoonup B$ est dite surjective si $f[A] = B$.
- Une application totale $f : A \to B$ est dite bijective si elle est injective et surjective.
- Propriétés :
  - Si $f : A \rightharpoonup B$ est inj., alors f^{-1} est une appli. partielle inj. de B vers A.
  - Si $f : A \to B$ est inj., alors f^{-1} est une appli. partielle inj. et surj. de B vers A.
  - Si $f : A \rightharpoonup B$ est inj. et surg., alors f^{-1} est une appli. inj. totale de B vers A.
  - Si $f : A \to B$ est bij., alors f^{-1} est une appli. bij. de B vers A.
- Les aplications partielles de A vers B constituent un ensemble : $\{f \in \mathcal{P}(A \times B) \mid \phi(f)\}$.
- Les applications (totales) de A vers B constituent un ensemble : $B^A := \{f \in \mathcal{P}(A \times B) \mid \phi(f) \wedge dom(f) = A\}$.

Ensembles inductifs

- Un ensemble E est inductif si $I(E)$ est vrai, où $I(E) := \emptyset \in E \wedge \forall x \in E(x \cup \{x\} \in E))$
- Comparer avec l'axiome de l'infini : $\exists E(I(E))$

Lemma

1. *Pour tout $\mathcal{I}$ ensemble non vide d'ensembles inductifs, $\cap\mathcal{I}$ est un ensemble inductif.*
2. *Pour tout ensemble A inductif, soit $\mathcal{I}_A := \{x \in \mathcal{P}(A) \mid I(x)\}$. C'est un ensemble non vide.*
3. *Pour tout A, B ensembles inductifs, on a $\cap\mathcal{I}_A = \cap\mathcal{I}_B$. On appelle cet ensemble $\mathbb{N}$.*
4. *$\mathbb{N}$ est l'ensemble inductif le plus petit (pour l'inclusion).*

Notations :

- $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, et pour tout entier n on note $n + 1 := n \cup \{n\}$.
- Pour tout $n, m \in \mathbb{N}$ on dénote $n \in m$ par $n < m$.

Ensembles inductifs (II)

Lemma

1. *Pour tout $\mathcal{I}$ ensemble non vide d'ensembles inductifs, $\cap\mathcal{I}$ est un ensemble inductif.*
2. *Pour tout ensemble A inductif, soit $\mathcal{I}_A := \{x \in \mathcal{P}(A) \mid I(x)\}$. C'est un ensemble non vide.*

1. Direct.
2. $\mathcal{I}_A$ est non vide, car $A \in \mathcal{P}(A)$ et $I(A)$.

Ensembles inductifs (III)

Lemma

1. *Pour tout A, B ensembles inductifs, on a $\cap\mathcal{I}_A = \cap\mathcal{I}_B$. On appelle cet ensemble $\mathbb{N}$.*
2. *$\mathbb{N}$ est l'ensemble inductif le plus petit (pour l'inclusion).*

1.
   - Montrons d'abord le cas $B \subseteq A$: $\mathcal{I}_B$ est alors co-initial pour l'inclusion dans $\mathcal{I}_A$, car pour tout $x \in \mathcal{I}_A$, $x \cap B$ est inductif par clôture par intersection, et $x \cap B$ est à la fois plus petit que x et inclus dans B, donc $x \cap B \in \mathcal{I}_B$. Par un lemme précédent, $\cap\mathcal{I}_A = \cap\mathcal{I}_B$.
   - Cas général : $A \cap B$ est aussi inductif par clôture par intersection, et $A \cap B \subseteq A$, donc par le cas particulier ci-dessus, $\cap\mathcal{I}_A = \cap\mathcal{I}_{A\cap B}$. Par symmétrie, $\cap\mathcal{I}_A = \cap\mathcal{I}_B$.
2. $\mathbb{N}$ est inductif par clôture par intersection non vide. Pour tout ensemble inductif A, on a $A \in \mathcal{I}_A$, donc $\mathbb{N} = \cap\mathcal{I}_A \subseteq A$.

Divers

Ensembles T-Finis :

- Un ensemble E est T-fini si $T_{fin}(E)$ est vrai, où $T_{fin}(E) := \forall \emptyset \neq S \subseteq \mathcal{P}(E)(\exists m \in S \forall x \in S(m \subseteq x \Rightarrow m = x))$.
- Les ensembles T-finis constituent-ils un ensemble ? Non.

Ensembles transitifs :

- Un ensemble E est transitif si $Trans(E)$ est vrai, où $Trans(E) := \forall x(x \in E \Rightarrow x \subseteq E)$.
- Si E est transitif, alors $\cup E \subseteq E$.