INF 302 : Langages & Automates

Introduction du cours - Rappels sur les notions mathématiques pour INF 232

Yliès Falcone

ylies.falcone@univ-grenoble-alpes.fr — www.ylies.fr

Univ. Grenoble-Alpes
-
Laboratoire d'Informatique de Grenoble - www.liglab.fr

Plan Chap. 0 - rappels Mathématiques

Objectifs

Objectifs

- Appréhender les bases mathématiques indispensables pour INF 232 (mais aussi pour l'informatique).
- Apprendre à formaliser, raisonner et rédiger des démonstrations.
- Fixer une notation.

Pourquoi des mathématiques ?

C.A.R. Hoare, The mathematics of programming, 1985

- Computers are mathematical machines. . .
- Computer programs are mathematical expressions.
- Programming is a mathematical activity.

Plan Chap. 0 - rappels Mathématiques

Pourquoi les ensembles ?

La théorie des ensembles s'impose depuis le début du 20ème siècle comme l'outil universel pour justifier les différentes branches des mathématiques.

Historique

- Georg Cantor (1845-1918) à l'origine des travaux sur la théorie des ensembles.
- Zermelo (1871-1953), Fraenkel (1891-1965) et von Neumann 1903-1957) développent une théorie axiomatique des ensembles ; principalement en réaction au paradoxe de Russell :

$$Russel = \{X \mid X \notin X\}\,.$$

Définition et notation des ensembles

Définition (Ensemble)

Un ensemble est une collection d'objets distinguables entre eux et pour lesquels il existe un critère d'appartenance.

Définition (Description extensionelle)

Description par énumération des éléments.

Exemple (Description extensionelle)

$\{0\}$, $\{0, 1\}$, $\{0, 2, 4\}$

Définition (Description intensionelle)

Description à l'aide d'un *prédicat* sur les objets, i.e., une fonction qui prend chaque objet et s'évalue à vrai ou faux.

Exemple (Description intensionelle)

$\{x \in \mathbb{N} \mid \exists k \in \mathbb{N} : n = 2 * k\}$

Ces définitions supposent de manière implicite un **univers** U qui contient tous les objets que l'on considère et un ensemble vide $\emptyset$ qui ne contient aucun élément.

Opérations Ensemblistes et inclusion

Définition (Union)

L'**union** des ensembles A et B, notée $A \cup B$, est définie comme l'ensemble :

$$A \cup B = \{x \in U \mid x \in A \text{ ou } x \in B\}$$

Définition (Intersection)

L'**intersection** des ensembles A et B, notée $A \cap B$, est définie comme l'ensemble :

$$A \cap B = \{x \in U \mid x \in A \text{ et } x \in B\}$$

Définition (Différence)

La **différence** entre l'ensemble A et l'ensemble B, noté $A \setminus B$:

$$A \setminus B = \{x \in U \mid x \in A \text{ et } x \notin B\}$$

Définition (Complémentation)

Le **complémentaire** de l'ensemble A, noté $\overline{A}$ est :

$$\overline{A} = U \setminus A$$

Définition (Inclusion)

L'ensemble A est **inclus** dans l'ensemble B, noté $A \subseteq B$:

$$\forall x \in U : x \in A \implies x \in B$$

Définition (Inclusion stricte)

L'ensemble A est **strictement inclus** dans l'ensemble B, noté $A \subset B$:

$$A \subseteq B \text{ et } B \not\subseteq A$$

Propriétés des opérations ensemblistes et de l'inclusion

Nous considérons quatre sous-ensembles A, B, C, D de U.

- **Absorption** : $\forall A, B \in \mathcal{P}(U) : A \subseteq B \implies (A \cup B = B)$ et $(A \cap B = A)$.
- **Élément absorbant** : $\forall A \in \mathcal{P}(U) : (A \cap \emptyset = \emptyset)$ et $(A \cup U = U)$.
- **Élément neutre** : $\forall A \in \mathcal{P}(U) : (A \cup \emptyset = A)$ et $(A \cap U = A)$.
- **Commutativité** de l'union et l'intersection :

$$\forall A, B \in \mathcal{P}(R) : A \cup B = B \cup A,$$
$$\forall A, B \in \mathcal{P}(R) : A \cap B = B \cap A.$$

- **Associativité** de l'union et l'intersection :

$$\forall A, B, C \in \mathcal{P}(R) : A \cup (B \cup C) = (A \cup B) \cup C,$$
$$\forall A, B, C \in \mathcal{P}(R) : A \cap (B \cap C) = (A \cap B) \cap C.$$

- **Distributivité** de l'union sur l'intersection, et vice-versa :

$$\forall A, B, C \in \mathcal{P}(R) : A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
$$\forall A, B, C \in \mathcal{P}(R) : A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Les éléments absorbants et neutres sont uniques.

Propriétés des opérations ensemblistes et de l'inclusion

Nous considérons quatre sous-ensembles A, B, C, D de U.

- **Idempotence** de l'union et l'intersection :

$$\forall A \in \mathcal{P}(U) : A \cup A = A,$$
$$\forall A \in \mathcal{P}(U) : A \cap A = A.$$

- Formules **de Morgan** pour la *dualité* entre l'union et l'intersection :

$$\forall A, B \in \mathcal{P}(U) : \overline{A \cup B} = \overline{A} \cap \overline{B},$$
$$\forall A, B \in \mathcal{P}(U) : \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

- **Monotonie** de l'union et l'intersection :

$$\forall A, B, C, D \in \mathcal{P}(U) : (A \subseteq B) \wedge (C \subseteq D) \implies A \cup C \subseteq B \cup D,$$
$$\forall A, B, C, D \in \mathcal{P}(U) : (A \subseteq B) \wedge (C \subseteq D) \implies A \cap C \subseteq B \cap D,$$
$$\forall A, B, C \in \mathcal{P}(U) : A \subseteq B \implies A \setminus C \subseteq B \setminus C.$$

- **Anti-monotonie** de la différence ensembliste sur le deuxième argument :

$$\forall A, B, C \in \mathcal{P}(U) : A \subseteq B \implies C \setminus B \subseteq C \setminus A$$

Démonstration de la monotonie de $\cup$

$$\forall A, B, C, D \in \mathcal{P}(U) : (A \subseteq B) \wedge (C \subseteq D) \implies A \cup C \subseteq B \cup D$$

Démonstration.

Soient $A, B, C, D \in \mathcal{P}(U) : (A \subseteq B) \wedge (C \subseteq D)$.
On souhaite montrer que $A \cup C \subseteq B \cup D$, i.e.,

$$\forall x \in U : x \in A \cup C \implies x \in B \cup D.$$

Soit $x \in U$ tel que $x \in A \cup C$. On distingue deux cas :

- $x \in A$. De l'hypothèse $A \subseteq B$, on déduit $x \in B$. Et donc $x \in B \cup D$.
- $x \notin A$. Comme $x \in A \cup C$, nous avons $x \in C$. De l'hypothèse $C \subseteq D$, nous déduisons $x \in D$. Et donc $x \in B \cup D$.

□

Ensemble des parties

Définition (Ensemble des parties)

L'ensemble des parties de A, noté $\mathcal{P}(A)$, est l'ensemble de tous ses sous-ensembles :

$$\mathcal{P}(A) = \{E \mid E \subseteq A\}$$

Exemple (Ensemble des parties)

- $\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$
- $\mathcal{P}(\{3,1,2\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$
- $\mathcal{P}\emptyset = \{\emptyset\}$

Cardinal de l'ensemble des parties

Le cardinal de l'ensemble des parties d'un ensemble A est :

$$2^{|A|}$$

Démonstration.

Par récurrence sur la taille de l'ensemble considéré. □

Propriétés de l'ensemble des parties

- L'ensemble des parties d'un ensemble n'est jamais vide :

$$\forall A \in \mathcal{P}(U) : \mathcal{P}(A) \neq \emptyset.$$

- L'ensemble des parties d'un ensemble contient cet ensemble ainsi que l'ensemble vide :

$$\forall A \in \mathcal{P}(U) : A \in \mathcal{P}(A) \wedge \emptyset \in \mathcal{P}(A).$$

- L'ensemble des parties de deux ensembles sont égaux ssi ces ensembles sont égaux :

$$\forall A, B \in \mathcal{P}(U) : \mathcal{P}(A) = \mathcal{P}(B) \iff A = B.$$

- L'ensemble des parties de l'union de deux ensembles :

$$\mathcal{P}(A \cup B) = \{X \cup Y \mid X \in \mathcal{P}(A) \wedge Y \in \mathcal{P}(B)\}.$$

- L'ensemble des parties de l'intersection de deux ensembles :

$$\mathcal{P}(A \cap B) = \{X \cap Y \mid X \in \mathcal{P}(A) \wedge Y \in \mathcal{P}(B)\}.$$

Attention, en général $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$.

Plan Chap. 0 - rappels Mathématiques

Plan Chap. 0 - rappels Mathématiques

Couple

Définition (Couple)

Soit a et b deux éléments de U, le couple (a, b) est défini mathématiquement (en théorie des ensembles) comme l'ensemble $\{a, \{a, b\}\}$.

Dans la suite, nous n'aurons pas besoin de cette définition rigoureuse, on pourra considérer (et l'on considérera) le couple comme une notion primitive. Les deux éléments du couple seront appelés les *composantes* du couple.

Deux couples sont égaux ssi leur composantes sont égales deux à deux.

Produit cartésien

Définition (Produit cartésien)

Le produit cartésien de deux ensembles E et F, noté $E \times F$, est défini comme :

$$E \times F = \{(e, f) \mid e \in E \wedge f \in F\}.$$

Étant donnés des éléments $a_1, a_2, \ldots, a_n$ ($n \in \mathbb{N}^*$, i.e., $n \in \mathbb{N}$ et $n > 0$), on forme le n-uplet $(a_1, a_2, \ldots, a_n)$. De même, le produit cartésien formé des ensembles $E_1, E_2, \ldots, E_n$ ($n \in \mathbb{N}^*$) est l'ensemble des n-uplets $(a_1, a_2, \ldots, a_n)$ avec $\forall i \in \{1, \ldots, n\} : a_i \in E_i$.

Exemple (Produit cartésien)

Donnons quelques exemples de produits cartésiens d'ensembles.

- $\mathbb{N}_2 \times \mathbb{N}_3 = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$.
- $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ est le plan Euclidien.
- $\forall A \in \mathcal{P}(U) : A \times \emptyset = \emptyset \times A = \emptyset$.

Plan Chap. 0 - rappels Mathématiques

Relation

Définition (Relation)

Une relation $\mathcal{R}$ entre deux ensembles E et F est un sous-ensemble de $E \times F$.

Exemple (Relation)

Étant donné un ensemble E, "être un sous-ensemble" ($\subseteq$) est bien une relation sur $\mathcal{P}(E)$ et lui même.

Pour des ensembles finis, on représentera les relations par des graphes/matrices.
Pour n ensembles en relation, on parle de relations n-aires. Étant donnés des ensembles $A_1, A_2, \ldots, A_n$, avec $n \in \mathbb{N}$, $\mathcal{R} \subseteq A_1, A_2, \ldots, A_n$ est une relation n-aire.

- Lorsque $n = 0$, la relation est alors une *constante*, soit V (vrai) soit F (faux).
- Lorsque $n = 1$, $\mathcal{R}$ est un sous-ensemble de A_1, on parle alors de *prédicat*.

Définition (Relation inverse)

L'inverse d'une relation $\mathcal{R} \subseteq A \times B$ est notée $\mathcal{R}^{-1}$, et est définie par :

$$\mathcal{R}^{-1} = \{(b, a) \in B \times A \mid (a, b) \in \mathcal{R}\}$$

Domaine et co-domaine d'une relation

Soit $\mathcal{R}$ une relation entre deux ensembles E et F.

Définition (Domaine)

Le domaine de $\mathcal{R}$, noté $\mathrm{dom}(\mathcal{R})$, est :

$$\mathrm{dom}(\mathcal{R}) = \{e \in E \mid \exists f \in F : e\mathcal{R}f\}$$

Définition (Co-domaine)

Le co-domaine de $\mathcal{R}$ (ou aussi appelé image de $\mathcal{R}$, noté $\mathrm{codom}(\mathcal{R})$, est :

$$\mathrm{codom}(\mathcal{R}) = \{f \in F \mid \exists e \in E : e\mathcal{R}f\}$$

Propriétés des relations

Soit $\mathcal{R}$ une relation binaire sur un ensemble E.

- *Réflexivité*. Une relation est réflexive lorsque

$$\forall e \in E : e\mathcal{R}e.$$

- *Symétrie*. Une relation est symétrique lorsque

$$\forall e_1, e_2 \in E : e_1\mathcal{R}e_2 \implies e_2\mathcal{R}e_1.$$

- *Anti-symétrie*. Une relation est antisymétrique lorsque

$$\forall e_1, e_2 \in E : (e_1\mathcal{R}e_2 \wedge e_2\mathcal{R}e_1) \implies e_1 = e_2.$$

- *Transitivité*. Une relation est transitive lorsque

$$\forall e_1, e_2, e_3 \in E : (e_1\mathcal{R}e_2 \text{ et } e_2\mathcal{R}e_3) \implies e_1\mathcal{R}e_3.$$

- *Asymétrie*. Une relation est asymétrique lorsque

$$\forall e_1, e_2 \in E : e_1\mathcal{R}e_2 \implies \neg\, e_2\mathcal{R}e_1.$$

- *Irréflexivité*. Une relation est irréflexive lorsque

$$\forall e \in E : \neg\, e\mathcal{R}e.$$

Plan Chap. 0 - rappels Mathématiques

Relations d'équivalence

Considérons un ensemble E, un élément x de E et une relation $\mathcal{R}$ sur E.

Définition (Relation d'équivalence)

Une relation d'équivalence est une relation réflexive, symétrique et transitive.

Exemple (Relation d'équivalence)

- La relation d'égalité est une relation d'équivalence.
- La relation "a le même signe que" est une relation d'équivalence sur $\mathbb{Z}$.

Définition (Classe d'équivalence)

La *classe d'équivalence* associée à x est l'ensemble $\{y \in E \mid x\mathcal{R}y\}$.

Propriétés

- Tout élément appartient à une seule classe d'équivalence.
- L'ensemble des classes d'équivalence forme une **partition** de E (i.e., leur union est égale à E, et leur intersection deux à deux est vide).

Relations d'ordre

On considère une relation $\mathcal{R}$ sur A.

Définition (Relation d'ordre)

Une relation d'ordre est une relation réflexive, antisymétrique et transitive.

Exemple (Relation d'ordre)

- La relation "inférieure ou égale".
- La relation "est un sous-ensemble de".

Définition (Relation d'ordre totale)

$\mathcal{R}$ est totale si $\forall x, y \in A : x\mathcal{R}y \vee y\mathcal{R}x$.

Exemple (Relation d'ordre totale)

$\leq$ sur $\mathbb{Z}$.

Définition (Relation d'ordre partielle)

$\mathcal{R}$ est partielle si $\exists x, y \in A, \neg(x\mathcal{R}y) \wedge \neg(y\mathcal{R}x)$.

Exemple (Relation d'ordre partielle)

$\subseteq$ sur $\mathcal{P}(A)$.

Plan Chap. 0 - rappels Mathématiques

Éléments remarquables

Soit X un ensemble muni d'une relation d'ordre.

Définition (Éléments remarquables)

- *majorant* de X tout élément $maj \in E$ tel que $\forall x \in X, x \preceq maj$.
- *minorant* de X tout élément $min \in E$ tel que $\forall x \in X, x \succeq min$.
- *élément maximal* de X le plus petit des majorants qui est dans X.
- *élément minimal* de X le plus grand des minorants qui est dans X.
- *maximum* de X tout majorant de X qui appartient à X.
- *minimum* de X tout minorant de X qui appartient à X.
- *borne supérieure* le plus petit des majorants de X.
- *borne inférieure* le plus grand des minorants de X.

Remarque : il n'existe pas forcément de majorant ou de minorant, mais il existe toujours au moins un élément maximal et au moins un élément minimal.

Plan Chap. 0 - rappels Mathématiques

Composition des relations

Définition (Composition de relation)

Soient $\mathcal{R} \subseteq A \times B$, et $\mathcal{R}' \subseteq B \times C$ deux relations.

$$\mathcal{R} \circ \mathcal{R}' = \{(a, c) \in A \times C \mid \exists b \in B.(a, b) \in \mathcal{R} \wedge (b, c) \in \mathcal{R}'\}$$

La composition de relation est également une relation ensembliste (entre les produits cartésiens d'ensembles).

Propriétés

- Associativité.
- Monotonie.
- $\cup -$ distributivité. Étant données trois relations $\mathcal{R}, \mathcal{R}_1, \mathcal{R}_2$,

$$(\mathcal{R}_1 \cup \mathcal{R}_2) \circ \mathcal{R} = (\mathcal{R}_1 \circ \mathcal{R}) \cup (\mathcal{R}_2 \circ \mathcal{R})$$
$$(\mathcal{R}_1 \cap \mathcal{R}_2) \circ \mathcal{R} = (\mathcal{R}_1 \circ \mathcal{R}) \cap (\mathcal{R}_2 \circ \mathcal{R})$$

Plan Chap. 0 - rappels Mathématiques

Fermeture de relation

Partant d'une relation quelconque, on peut "compléter" cette relation pour qu'elle vérifie une propriété. On parle alors de *fermeture*.

Soit A un ensemble, considérons une relation $\mathcal{R} \subseteq A \times A$.

Définition (Fermeture réflexive)

La **fermeture réflexive** de $\mathcal{R}$, est la plus petite relation $\mathcal{Q}$ sur A t.q. :

$$(\forall x, y \in A : x\mathcal{R}y \implies x\mathcal{Q}y) \wedge (\forall x \in A : x\mathcal{Q}x)\,.$$

Définition (Fermeture transitive)

La **fermeture transitive** de $\mathcal{R}$, notée $\mathcal{R}^+$, est la plus petite relation $\mathcal{Q}$ sur A t.q. :

$$(\forall x, y \in A : x\mathcal{R}y \implies x\mathcal{Q}y) \wedge (\forall x, y, z \in A : (x\mathcal{Q}y \wedge y\mathcal{Q}z) \implies x\mathcal{Q}z)\,.$$

Définition (Fermeture reflexive-transitive)

La *fermeture reflexive-transitive* de $\mathcal{R}$ est la plus petite relation $\mathcal{Q}$ sur A réflexive, transitive et qui contient $\mathcal{R}$. Elle est notée $\mathcal{R}^*$.

Plan Chap. 0 - rappels Mathématiques

Fonction et application

Définition

On ne donne pas les définitions formelles de fonctions et applications. On mentionne simplement l'idée de correspondance entre un ensemble de départ (le domaine) et un ensemble d'arrivée (l'ensemble image).

Définition (Fonction)

$f \subseteq A \times B$ est une *fonction*, lorsque pour tout a de A, il existe au plus un b de B tel que $a \mathcal{R} b$.

Nous utiliserons les raccourcis de notation suivantes :

- $f : A \to B$ pour $f \subseteq A \times B$,
- $f(a) = b$ pour $(a, b) \in f$,
- id_A pour l'identité sur A, i.e., $\{(a, a) \mid a \in A\}$.

Définition (Application)

Une fonction f est une *application*, lorsque pour tout a de A, il existe un b unique tel que $f(a) = b$.

Propriétés des fonctions et applications

Définition (Injectivité, surjectivité, bijectivité)

On dit qu'une fonction est :

- *injective*, si son inverse est une fonction, ou encore si tous les éléments de son domaine de définition ont une image distincte ;
- *surjective*, si son inverse est une fonction totale, ou encore si elle atteint tous les éléments de son ensemble image ;
- *bijective*, si son inverse est une application, ou encore si elle est injective et surjective.

Propriété

Soit $f : A \to B$ une application, il existe une application injective $g : B \to A$ telle que $g \circ f = id_A$ si et seulement si f est bijective.

Retour sur les propriétés des ensembles

Définition (Équipotence)

Soient A et B deux ensembles, on dit qu'ils sont *équipotents* si et seulement s'il existe une bijection de A vers B. On note $A \approx B$.

Notons que $A \approx B \equiv B \approx A$. En effet, s'il existe une bijection de A vers B, alors il en existe une de B vers A : sa fonction inverse.

Propriété

Soient A et B deux ensembles, $A \times B$ est équipotent à $B \times A$.

Définition (Ensemble dénombrable)

Un ensemble est dit *dénombrable* ssi :

- il est équipotent à $\mathbb{N}$, i.e., $A \approx \mathbb{N}$, ou
- cet ensemble est fini.

Exemple (Ensembles (non) dénombrables)

$\mathbb{N}^2$ est dénombrable. $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable.

Plan Chap. 0 - rappels Mathématiques

À propos de la rédaction de preuves

Principe d'une preuve

Application de règles de déduction permettant de relier ce que l'on sait (hypothèses) à ce que l'on veut prouver (théorème).

Rédiger les preuves correctement

La rédaction d'une preuve ne s'improvise pas.

- Principes utilisés dans les preuves.
- Techniques de preuves

Principe 1 : Règles de déduction

- Application des définitions.
- Substitution de termes égaux : si deux termes sont égaux alors on peut les changer, sans changer la validité de la conclusion.
- Modus ponens : si p_A et $p_A \implies p_B$ sont prouvés, alors on peut déduire p_B.
- Modus tollens : si $\neg p_B$ et $p_A \implies p_B$ sont prouvés, alors on peut déduire $\neg p_A$.
- Syllogisme (transitivité) : Si $p_A \implies p_B$ et $p_B \implies p_C$ sont prouvés, alors on peut déduire $p_A \implies p_C$.
- Dilemme : si $p_A \vee p_B$, $p_A \implies p_C$, $p_B \implies p_C$ sont prouvés alors on peut en déduire p_C
- ...

Principe 2 : Tiers Exclu

Étant donné une proposition p, plusieurs cas peuvent arriver :

1. soit p soit $\neg p$ est vraie,
2. p et $\neg p$ sont vraies
3. p et $\neg p$ ne sont pas vraies

2) est exclu par consistance de la logique propositionnelle ; 3) est exclu par le principe du tiers exclu.

Définition (Principe du tiers exclu)

La proposition $p \vee \neg p$ est toujours vraie (tautologie).

Utilisation du principe du tiers exclu

Pour prouver qu'une proposition p est vraie :

- la prouver sous une hypothèse h ; et
- la prouver sous l'hypothèse contraire $\neg h$.

Techniques de preuves

- Démonstration par l'absurde d'une proposition p : supposer $\neg p$, et démontrer qu'un fait mathématique connu est contredit.
- Démonstration par contraposition de $p \implies q$: montrer que $\neg q \implies \neg p$.
- Démonstration par récurrence : lorsque la propriété $p(n)$ dépend d'un paramètre $n \in \mathbb{N}$:
  - montrer $p(0)$
  - montrer que $\forall n \in \mathbb{N} : p(n) \implies p(n+1)$
- Démonstration par récurrence forte (ou complète) : lorsque la propriété $p(n)$ dépend d'un paramètre $n \in \mathbb{N}$:
  - montrer $p(0)$
  - montrer que $\forall n \in \mathbb{N}, (\forall m \leq n : p(n)) \implies p(n+1)$

Preuve utilisant le principe du tiers-exclu

Exemple (Preuve utilisant le principe du tiers-exclu)

Prouvons que

$$\forall a, b \in \mathbb{Z}, a \times b = 0 \implies a = 0 \vee b = 0$$

- Premier cas : $a = 0$. Alors $(a = 0) \vee (b = 0)$.
- Second cas : $\neg(a = 0)$. De $a \times b = 0$, on peut déduire $b = 0$.

Ici le principe du tiers exclu nous permet de déduire $a = 0 \vee \neg(a = 0)$.

Exemple (Preuve utilisant le principe du tiers-exclu)

Pour la preuve, nous supposons que $\sqrt{3}$ et $\sqrt{2}$ sont irrationnels.

- Supposons que $\sqrt{3}^{\sqrt{2}}$ soit rationnel. Comme $\sqrt{3}$ et $\sqrt{2}$ sont des nombres irrationnels, nous pouvons prendre $a = \sqrt{3}$ et $b = \sqrt{2}$
- Supposons que $\sqrt{3}^{\sqrt{2}}$ soit irrationnel. Comme $\sqrt{2}$ est irrationnel, nous prenons $a = \sqrt{3}^{\sqrt{2}}$ et $b = \sqrt{2}$. Nous avons $a^b = 3$.

Preuve par contradiction

Exemple (Preuve par contradiction)

Prouvons qu'il existe un nombre infini de nombre de premiers

- Supposons qu'il existe un nombre fini de nombres premiers, disons N.
- Soient $p_1, \ldots, p_N$ cette liste de nombre premiers.
- Considérons $p_1 \times \ldots \times p_N + 1$.
- Il y a deux cas :
  - Ce nombre est premier et comme $p_1 \times \ldots \times p_N + 1 > p_N$, il y a donc au moins $N + 1$ nombres premiers. Contradiction.
  - Ce nombre n'est pas premier. Comme ce nombre ne peut être divisé par aucun des p_i, $i = 1, \ldots, N$, il doit être divisible par un nombre premier plus grand que p_N. Contradiction.

Preuve par contradiction

Exemple (Preuve par contradiction)

Prouvons qu'il existe deux nombres irrationnels a et b tels que a^b soit rationnel

- Supposons que a^b soit irrationnel pour toute pair de nombres irrationnels a et b
- Nous savons que $\sqrt{2}$ est irationnel.
- En utilisant notre hypothèse $\sqrt{2}^{\sqrt{2}}$ est irationnel.
- Appliquons notre hypothèse à nouveau à $\sqrt{2}^{\sqrt{2}}$ et $\sqrt{2}$

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2$$

- 2 serait irrationnel. C'est une contradiction.

Preuve par contraposition

Exemple (Si $n \mod 3 = 2$, alors n n'est pas un carré)

- Prenons la contraposée : si n est un carré, alors $n \mod 3 \neq 2$.
- Reformulons. S'il existe k tel que $n = k^2$, alors $n \mod 3 = 0$ ou $n \mod 3 = 1$.
- Nous distinguons cas :
  - Cas $k \mod 3 = 0$. Nous avons $k = 3 \times m$ pour un m ce qui signifie que $k^2 = 9 \times m^2$. k^2 est aussi un multiple de 3.
  - Cas $k \mod 3 = 1$. Nous avons $k = 3 \times m + 1$ pour un m ce qui signifie que $k^2 = 9 \times m^2 + 6 \times m + 1 = 3 \times (3 \times m^2 + 2 \times m) + 1$. Donc $k^2 \mod 3 = 1$.
  - Cas $k \mod 3 = 2$. Nous avons $k = 3 \times m + 2$ pour un m ce qui signifie que $k^2 = 9 \times m^2 + 12 \times m + 4 = 3 \times (3 \times m^2 + 4 \times m + 1) + 1$. Donc $k^2 \mod 3 = 1$.

Plan Chap. 0 - rappels Mathématiques

Définitions inductives

Considérons :

- E un ensemble
- $f : E \times E \times \ldots \times E \to E$ une fonction partielle
- $A \subseteq E$ un sous-ensemble de E

Définition (Fermeture)

A est fermé par f ssi $f(A \times \ldots \times A) \subseteq A$

Définition (Definition inductive)

Une définition inductive de E est une famille de règle (fonctions partielles) définissant le plus petit ensemble de E qui est fermé par ces règles

Définitions inductives - bis

Définition (Definition inductive – en pratique)

Pour définir l'ensemble $A \subseteq U$ inductivement, on donne :

- une base, i.e., un ensemble $B \subseteq U$,
- des règles d'induction, de la forme si $e_1, \ldots, e_n \in A$, alors $f(e_1, \ldots, e_n) \in A$.

Exemple (Définition inductive)

On définit $Pair \subseteq \mathbb{N}$ inductivement de la manière suivante :

- Base : $0 \in Pair$,
- Induction : si $n \in Pair$, alors $2 * n \in Pair$ et $n + 2 \in Pair$.

Preuve par induction

Principe de preuve par induction

- On montre que la propriété est vraie pour chacun des éléments de la base.
- On montre que la propriété est préservée par application des règles d'induction. C'est-à-dire, si la propriété est satisfaite par certains éléments, en appliquant les règles sur ces éléments, l'ensemble obtenu satisfait la propriété.

Exemple (Preuve par induction)

$$Pair \subseteq \{2 * k \mid k \in \mathbb{N}\}$$

- Cas de base : $0 = 2 * 0 \in \{2 * k \mid k \in \mathbb{N}\}$.
- Pas d'induction : Considérons $n \in \mathbb{N}$ et supposons que $n \in \{2 * k \mid k \in \mathbb{N}\}$. On doit montrer que $n * 2 \in \{2 * k \mid k \in \mathbb{N}\}$ et $n + 2 \in\in \{2 * k \mid k \in \mathbb{N}\}$.
  - Pour $n * 2$, c'est trivial.
  - Pour $n + 2$, on sait qu'il existe $k \in \{2 * k \mid k \in \mathbb{N}\}$ tel que $n = 2 * k$. On a donc $n + 2 = 2 * k + 2 = 2 * (k + 1)$. Comme $k + 1 \in \mathbb{N}$, on a $n + 2 \in \{2 * k \mid k \in \mathbb{N}\}$.

Résumé - Plan Chap. 0 - rappels Mathématiques

Résumé

- Ensembles et opérations ensemblistes.
- Relations, relation d'ordre, d'équivalence.
- Fonctions et applications, et leur propriétés.
- Rédaction et techniques de preuves.
- Définitions inductives.

Pour le prochain cours

- Formaliser les conditions pour qu'une relation soit une fonction ou application.
- Formaliser les notions d'injectivité, surjectivité, bijectivité.
- Définir les entiers impairs et les entiers de la suite de Fibonacci de manière inductive.
- Formaliser les condtions à prouver lors d'une preuve par induction.