Logique et algèbre

Damien Nouvel

Plan

De l'algèbre aux ensembles

- Quelques dates en l'algèbre
  - Mot de l'arabe al-jabr (par Al-Khwarizmi)
  - $\Rightarrow$ Construction à partir d'**éléments**
  - $\sim$ 1000 : utilisation des chiffres arabes
  - $\sim$ 1500 : apparition des symboles $+$, $-$, $=$
  - $\Rightarrow$ Chiffres et équations
- Vers la théorie des ensembles
  - Fin du XIX$^{\text{ème}}$ siècle
  - $\Rightarrow$ G. Cantor : “nous appelons *ensemble* tout réunion M d'objets de notre conception, déterminés et bien distincts, que nous dénommerons *éléments* de M”
  - $\Rightarrow$ Notion d'**élément** et d'**appartenance** $x \in E$

$\Rightarrow$ Liens entre la **logique** et l'**algèbre** ?

Ensembles, individus et catégories

- Relations ensemblistes
  - Relation partie-tout : **méronymie** / **holonomie**
    - La roue est partie d'une voiture
    - La tête est une partie du corps
    - ...

  ⇒ Relation entre individus
  - Relation hiérarchique : **subsomption**
    - La voiture est un véhicule
    - Le singe est un animal
    - ...

  ⇒ Relation entre catégories
- Pour les ensembles
  - Regroupement d'individus dans des catégories
  - Une catégorie peut-être un individu

Notations ensemblistes et principes généraux

- **Conventions** et **symboles**
  - Majuscules : ensembles (A, E, P, Q, R ...)
  - Minuscules : éléments (x, y, a, b ...)
  - Accolades { et } et barre verticale | : contenu d'un ensemble
  - $\varnothing$: ensemble vide (inclus dans tout ensemble)

  $\Rightarrow$ $P = \{x, y\}$, $P = \{x | \exists n, x = 2^n\}$
- Règles générales
  - Non-ordonnés : $\{x, y, z\} = \{z, x, y\}$
  - Sans répétitions : $\{x, y, y\} = \{x, y\}$
  - Peut-être de taille infinie (dénombrable ou non)
- Un ensemble peut être défini par
  - **Extension** (dénotation, liste exhaustive) : $P = \{x, y, z\}$
  - **Intention** ou **compréhension** : $P = \{x \textit{ est pair}\}$
  - **Récurrence** ou **induction** : $P = \{x = 1 \textit{ ou } x/3 \textit{ est dans } P\}$

Symboles et opérateurs

- Appartenance : $x \in P$ et $x \notin P \equiv \neg(x \in P)$
- Inclusion : $P \subseteq Q$ (si stricte : $P \subset Q$)
- Complémentaire : $\overline{P}$
- Union : $P \cup Q$
- Intersection : $P \cap Q$
- Différence (ensembliste) : $P \backslash Q$
- Différence symétrique : $P \Delta Q$

Ensembles et sous-ensembles

- Les **prédicats** définissent des ensembles
  - Cas unaire : l'ensemble des hommes $H = \{x | Homme(x) = V\}$
  - Cas n-aire : lien parent-enfant $P = \{(x, y) | Enfant(x, y) = V\}$
- L'**implication** donne les **sous-ensembles**
  - Sous-ensemble $P \subseteq Q$ si $\forall x(x \in P \rightarrow x \in Q)$
  - Sous-ensemble propre $P \subset Q$ si $\forall x(x \in P \rightarrow x \in Q) \wedge P \neq Q$
  - Si $P \subseteq Q$ et $Q \subseteq P$ alors $P = Q$ et $\forall x(x \in P \leftrightarrow x \in Q)$
- Ensembles **disjoints**
  - Deux ensembles P et Q sont disjoints s'ils n'ont aucun élément en commun
  - $\forall x \neg(x \in P \wedge x \in Q) \equiv \neg\exists x(x \in P \wedge x \in Q)$
  - $P \cap Q = \varnothing$

Opérateurs : intersection et union

- **Union** $\cup$ de P et Q
  - Éléments qui appartiennent soit à P **ou** à Q
  - $P \cup Q = \{x | x \in P \vee x \in Q\}$
  - ⇒ $\{x, y, z\} \cup \{x, z, t\} = \{x, y, z, t\}$
  - ⇒ $\varnothing$ n'affecte pas l'union : $P \cup \varnothing = P$
  - ⇒ Associative, commutative, $\varnothing$ neutre
- **Intersection** $\cap$ de P et Q
  - Éléments qui appartiennent à la fois à P **et** Q
  - $P \cap Q = \{x | x \in P \wedge x \in Q\}$
  - ⇒ $\{x, y, z\} \cap \{x, z, t\} = \{x, z\}$
  - ⇒ S'il n'y a aucun élément commun : $\varnothing$
  - ⇒ Associative, commutative, $\varnothing$ absorbant
- Union et intersection sont distributifs l'un pour l'autre :
  $P \cup (Q \cap R) = (P \cup Q) \cap (P \cup R)$

Opérateurs : complémentaire et différence

- **Complémentaire** de P et $\overline{P}$
  - Tout élément qui n'est **pas** dans P
  - $\overline{P} = \{x | \neg(x \in P)\} = \{x | x \notin P\}$
  - ⇒ Extension pas toujours possible à calculer
  - $\overline{\overline{P}} = P$
- **Différence** de P et Q
  - Tout élément qui est dans P mais **pas** dans Q
  - $P \backslash Q = \{x | x \in P \wedge x \notin Q\} = P \cap \overline{Q}$
  - ⇒ Non-associative, non-commutative, $\emptyset$ neutre
  - ⇒ Peu pratique, mais correspond à la soustraction
- **Différence symétrique** de P et Q
  - Tout élément qui est dans P **ou** Q mais **pas** dans P **et** Q
  - $P \Delta Q = \{x | (x \in P \vee x \in Q) \wedge \neg(x \in P \wedge x \in Q)\}$
  - ⇒ Associative, commutative, $\emptyset$ neutre
  - ⇒ La différence symétrique est distributive pour l'intersection

Parties d'un ensemble

- **Sous-parties** d'un ensemble
  - L'ensemble des sous-ensembles possibles
  - Pour un ensemble P, l'ensemble $\{Q|Q \subseteq P\}$
  - Exemple : si $P = \{x, y, z\}$ alors
    $Parties(P) = \{\{x, y, z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x\}, \{y\}, \{z\}, \varnothing\}$
- **Partition** d'un ensemble
  - Ensemble de sous-ensembles disjoints tels que leur union reforme l'ensemble et que leurs intersections soient vides
  - Exemple : si $P = \{x, y, z\}$ alors
    - $\{\{x, y\}, \{z\}\}$
    - $\{\{x\}, \{y\}, \{z\}\}$
    - ...

$\Rightarrow$ Combien de sous-parties ou de partitions possibles ?

Ensembles mathématiques

- $\mathbb{N}$: nombres entiers naturels (positifs)
- $\mathbb{Z}$: nombres entiers (positifs ou négatifs)
- $\mathbb{Q}$: nombres rationnels

$\Rightarrow$ $x \in \mathbb{Q} \leftrightarrow \exists y \in \mathbb{Z}, \exists z \in \mathbb{Z} \backslash \{0\} (x = y/z)$

- $\mathbb{R}$: nombres réels
- $\mathbb{P}$: nombres premiers
- $\mathbb{C}$: nombres complexes

$\Rightarrow$ $\mathbb{P} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

- Intervalles
  - $x \in [a, b] \leftrightarrow \{x \in \mathbb{R} \wedge x \geqslant a \wedge x \leqslant b\}$
  - $x \in [a, b[\leftrightarrow \{x \in \mathbb{R} \wedge x \geqslant a \wedge x < b\}$
  - $x \in]-\infty, b] \leftrightarrow \{x \in \mathbb{R} \wedge x \leqslant b\}$

Structures ordonnées, les n-uplets

- Importance de l'ordre des éléments
  - Coordonnées dans un plan : $(1, 2) \neq (2, 1)$
  - Relation parent-enfant : $(Pierre, Jean) \neq (Jean, Pierre)$
  - Attributs d'un objet dans une BDD
- Composition d'éléments : **n-uplets** (*triplets*, *quadruplets* ...)
  - **Produit cartésien** d'ensembles : $P \times Q$

  $\Rightarrow$ Associatif, non-commutatif
  - **Puissance** : $P^2 = P \times P$, $P^n = P \times P \times P \times \ldots P$ (n fois)
  - Exemples
    - $\Rightarrow$ Coordonnée en 3D $(x, y, z) \in \mathbb{R}^3$
    - $\Rightarrow$ Âge et taille de personnes $(x, y) \in \mathbb{N} \times \mathbb{R}$

$\Rightarrow$ Les éléments sont des **composantes** de l'objet

$\Rightarrow$ Répétitions d'éléments : $(1, 3, 1)$

$\Rightarrow$ Sur un domaine $\mathbb{D}$: prédicats n-aires dans $\mathbb{D}^n$

Exercices : extension et intension

- Soient $A = \{a, b, c, d\}$ et $B = \{a, d, e\}$, donnez l'extension de
  - $A \cup B$ et $A \cap B$
  - $A \times B$ et $(A \cap B)^3$
  - $(A \times B) \cap (B \times A)$
  - Les sous-parties possibles et deux partitions de A
- Donnez l'extension des ensembles suivants
  - $\{x | x \in \mathbb{N} \wedge x < 5\}$
  - $\{x | x \in \mathbb{Z} \wedge x^2 < 10\}$
  - $\{x | x \in \mathbb{Q} \wedge x < 2 \wedge 4 * x \in \mathbb{N}\}$
- Donnez des définitions en intension des ensembles suivants
  - $\{-2, -1, 0, 1, 2, 3, 4\}$
  - $\{1, 3, 5, 7, 9\}$

Exercices : démonstrations

- Soient A et B deux ensembles
  - Démontrez que $A \subseteq A \cup B$
  - Démontrez que $\overline{A \cap B} = \overline{A} \cup \overline{B}$
  - Reformulez $A \backslash B$ par intersection et complémentaire
  - Reformulez $A \Delta B$ par intersection, union et complémentaire
  - Démontrez que $(A \cap B) * C = (A * C) \cap (B * C)$
  - Démontrez que $(A * B) \cap (B * A) = (A \cap B)^2$

Plan

Cardinal d'un ensemble

- **Cardinal** : nombre d'éléments que contient un ensemble
  - Pour un ensemble P, noté $|P|$
  - Nombre entier positif : $|P| \in \mathbb{N}$
  - Exemples
    - $|\varnothing| = 0$
    - $|\{a, b, c\}| = 3$
    - $|\{a, a, b, c, b, c\}| = 3$
    - $|\{\{a, b\}, \{c\}\}| = 2$
- Quelques règles
  - Intersection : $|P \cap Q| \leqslant min(|P|, |Q|)$
  - Union : $|P \cup Q| = |P| + |Q| - |P \cap Q|$
  - Union : $|P \cup Q| \leqslant |P| + |Q|$
  - Si P et Q sont égaux : $|P \cap Q| = |P \cup Q| = |P| = |Q|$
  - Si P et Q sont disjoints : $|P \cap Q| = 0$ et $|P \cup Q| = |P| + |Q|$

Cardinal de n-uplet

- Contraintes sur l'ordre et possibilité de répétitions
  - $|P \times Q| = |P| * |Q|$
  - $|P^n| = |P|^n$
  - Par exemple, si $P = \{a, b\}$ alors
    - $P^3 = \{(a, a, a), (a, a, b), (a, b, a), (a, b, b),$
      $(b, a, a), (b, a, b), (b, b, a), (b, b, b)\}$
    - $|P^3| = |P|^3 = 2^3 = 8$
  - $\Rightarrow$ Ordre important $(b, a, a) \neq (a, b, a) \dots$

Algèbre et combinatoire

- **Produit cartésien** : n^k (n-uplets avec remise)
- **Permutations** : $n!$ (n-uplets sans remise)
  - Premier élément parmi n
  - Second élément parmi les $n-1$ restants
  - ...
- **Arrangements** : A_n^k
  - Sélection de k éléments ordonnés parmi n

  $\Rightarrow$ $A_n^k = n * (n-1) * (n-2) * \ldots (n-k+1) = \dfrac{n!}{(n-k)!}$
- **Combinaisons** : $\binom{n}{k}$ (ou C_n^k)
  - Regroupement des arrangements par ensembles
  - Une combinaison de k éléments donne $k!$ permutations

    $\Rightarrow$ $C_n^k * k! = A_n^k$

    $\Rightarrow$ $C_n^k = \dfrac{A_n^k}{k!} = \dfrac{n * (n-1) * (n-2) * \ldots (n-k)}{k * (k-1) * (k-2) * \ldots 1} = \dfrac{n!}{k! * (n-k)!}$

Cardinalités avec/sans ordre et remise

- Récapitulatif :

k parmi n	avec ordre	sans ordre
avec remise	n^k	$\frac{(n+k-1)!}{k!(n-1)!}$
sans remise	$\dfrac{n!}{(n-k)!}$	$\dfrac{n!}{k!(n-k)!}$

Cardinalités de parties d'ensembles

- Sous-ensembles possibles par **taille**
  - Pour un ensemble de taille n, sous-ensembles
    - Pour une taille k, combinaisons : $|\{Q \subset P \wedge |Q| = k\}| = C_n^k$
    - Pas d'intersection entre deux tailles :
      $\{Q \subset P \wedge |Q| = k\} \cap \{Q \subset P \wedge |Q| = l \wedge k \neq l\} = \varnothing$
    - Union des tailles : $|\{Q \subset P\}| = \sum_{k=0}^{n} |\{Q \subset P \wedge |Q| = k\}|$

$\Rightarrow$ $|\{Q \subset P\}| = \sum_{k=0}^{n} C_n^k$

- Sous-ensembles possibles par **présence d'éléments**
  - Présence ou absence d'un élément : 2 possibilités
  - Pour un ensemble de taille n : 2^n possibilités

$\Rightarrow$ En corollaire : $\sum_{k=0}^{n} C_n^k = 2^n$

Cardinalités de partitions d'ensembles

- Pour un ensemble de taille n, partitions de taille k : P_n^k
  - $P_n^1 = P_n^n = 1$
  - $P_n^{n-1} = \dfrac{n * (n-1)}{2}$
  - $P_n^2 = 2^{n-1} - 1$
  - Pour un k quelconque
    - Par récurrence : $P_n^k = P_{n-1}^{k-1} + k * P_{n-1}^k$
    - Calcul direct : $P_n^k = \dfrac{1}{k!} * \sum_{i=1}^{k} C_i^k (-1)^{k-i} i^n$

    $\Rightarrow$ Compliqué ...

Exercices : dénombrement

- Soient $P = \{a, b, c\}$ et $Q = \{a, d\}$, donnez
  - $|P|$, $|Q|$, $|P \cap Q|$, $|P \cup Q|$
  - $|\{(x, y) \in Q \times Q\}|$
  - $|P \times Q|$
  - $|P^3|$
  - $|(P \cup Q)^2|$
  - $|(P \cap Q)^7|$
  - $|\{E \subset P, |E| = 2\}|$
  - $|\{E \subset (P^2 \cup Q^2), |E| = 3\}|$
  - $|\{E \subset (P \cup Q)\}|$
- Alphabet : en tirant 4 lettres d'un sac de 26 (sans remise)
  - Combien de combinaisons de lettres sont possibles ?
  - Combien ne contiennent que des voyelles ou des consonnes ?
  - Pour chaque possibilité, combien de mots peut-on former ?
  - Combien de mots de 4 ou 3 lettres peut-on former ?

Plan

Notations

- **Application** (fonction) : relation entre deux ensembles
  - **Notation** $f : E \to F$
  - Ensemble de **départ** E
  - Ensemble d'**arrivée** (ou image) F
  - $\Rightarrow$ Application est définie par le produit $G \subset E \times F$
  - Fonction mathématique : $(x, y) \in G$ ssi $f(x) = y$
  - $\Rightarrow$ **Sémantique** portée par le nom de la fonction
- Une seule **image** possible
  - $\forall x \in E, \forall y_1 \in G, \forall y_2 \in G, ((x, y_1) \in G \wedge (x, y_2) \in G \to y_1 = y_2)$
  - $\Rightarrow$ Pour un élément x, on obtient qu'un seul $f(x)$
  - $\Rightarrow$ Pas de disjonction en sortie de la fonction
- Exemples
  - $f(x) = x^3 : G = (0, 0), (1, 1), (2, 8), (3, 27), (4, 64) \ldots$
  - $f(x, y) = x + 2y + 1 : G = ((0, 0), 1), ((0, 1), 3), ((1, 1), 5) \ldots$

Injection, surjection, bijection

- Caractérisation de G
- **Antécédent** : si $f(x) = y$ alors $x \in E$ est l'antécédent de y
- **Injection**
  - Chaque élément image a **au plus** un antécédent
  - $\forall x_1 \in E, \forall x_2 \in E, \forall y \in F, (f(x_1) = y \wedge f(x_2) = y \rightarrow x_1 = x_2)$
  - $\forall x_1 \in E, \forall x_2 \in E, (f(x_1) = f(x_2) \rightarrow x_1 = x_2)$
  - $\forall x_1 \in E, \forall x_2 \in E, (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))$
  - Contre-exemple : racine carrée sur $\mathbb{R}$
- **Surjection**
  - Chaque élément image a **au moins un** antécédent
  - $\forall y \in F, \exists x \in E, f(x) = y$
  - Exemple : valeur absolue sur $[0, +\infty[$

$\Rightarrow$ **Bijection** : application **injective et surjective**

Exercice

- Dites si ces fonctions sont injectives et/ou surjectives
  - $\mathbb{R} \rightarrow \mathbb{R} : f(x) = x + 3$
  - $\mathbb{N} \backslash \{0\} \rightarrow]0, 1] : g(x) = 1/x$
  - $\mathbb{R}^2 \rightarrow \mathbb{R} : f(x, y) = x + y$
  - $\mathbb{R}^+ \times \{-1, +1\} \rightarrow \mathbb{R} : f(x, y) = x * y$
  - $\mathbb{N} \rightarrow \mathbb{N} : f(n) = n^3$

Morphismes

- **Groupe** : ensemble et **loi de composition associative**
  - Loi de composition : application de $E \times E$ dans E
  - Notation par **opérateur** (infixe), par exemple : $E \bullet E$
  - Associativité : $\forall x, \forall y, \forall z, (x \bullet y) \bullet z = x \bullet (y \bullet z)$
  - Exemples : $(\mathbb{R}, +)$, $(\mathbb{R}, *)$, mais pas $(\mathbb{R}, -)$, $(\mathbb{R}, \div)$
- **Morphisme** : lien entre les groupes de départ et d'arrivée
  - Entre les opérateurs de chaque groupes
  - Notation : $f : (E, \bullet) \rightarrow (F, \diamond)$
  - $\forall x \in E, \forall y \in E, f(x \bullet y) = f(x) \diamond f(y)$
  - Exemples
    - Objets à attacher (O, att) et leur poids $(\mathbb{R}, +)$
    - Chaînes à concaténer $(\Sigma, .)$ et leur taille $(\mathbb{N}, +)$
    - Taille de chaîne $(\mathbb{N}, +)$ et chaînes possibles $(\mathbb{N}, *)$
  - Contre-exemple : tas de grains $(\mathbb{N}, +)$ et hauteur $(\mathbb{N}, +)$

Composition de morphismes

- Application h : appliquer f, puis g au résultat de f

$\Rightarrow$ Composition de fonctions $h(x) = g(f(x))$

- **Notation** $h = g \circ f$
- Exemples
  - Somme puis division par N
  - Compression puis taille d'un fichier
  - Résumé puis traduction d'un texte

Types de morphismes

- **Homomorphisme** : morphisme
- **Endomorphisme**
  - Mêmes groupes de départ et d'arrivée
  - Exemple : $f(x) = |x|$ (valeur absolue) dans $(\mathbb{R}, *)$
  - Possibilité de composition de morphismes $f \circ g$
- **Isomorphisme** (homéomorphisme, difféomorphisme)
  - Morphisme $f : E \to F$ qui admet un inverse $g : F \to E$
  - ⇒ Composition : $f \circ g = Id_E$ et $g \circ f = Id_F$
  - ⇒ Pour les ensembles : applications **bijectives**
  - Exemple : entiers
    $f : (\mathbb{N} \backslash \{0\} \times \{+1, -1\}, *) \to (\mathbb{Z} \backslash \{0\}, *), f(x, y) = x * y$
- **Automorphisme** : endomorphisme et isomorphisme
  - Exemple : exponentielle $f : (\mathbb{R}, *) \to (\mathbb{R}, +), f(x) = e^x$

Relations

- Relation $\mathcal{R}$ **binaire** sur un ensemble E
  - Sous-ensemble du produit cartésien : $\mathcal{R} \subset E \times E$
  - **Propriétés** possibles
    - **Réflexive** : $\forall x \in E, x\mathcal{R}x$
    - Irréflexive : $\forall x \in E, \neg x\mathcal{R}x$
    - **Symétrique** : $\forall (x, y) \in E^2, (x\mathcal{R}y \rightarrow y\mathcal{R}x)$
    - **Anti-symétrique** : $\forall (x, y) \in E^2, (x\mathcal{R}y \wedge y\mathcal{R}x \rightarrow x = y)$
    - **Transitive** : $\forall (x, y, z) \in E^3, (x\mathcal{R}y \wedge y\mathcal{R}z \rightarrow x\mathcal{R}z)$
    - Circulaire : $\forall (x, y, z) \in E^3, (x\mathcal{R}y \wedge y\mathcal{R}z \rightarrow z\mathcal{R}x)$
  - Exemples
    - $=$ sur $\mathbb{N}$: réflexive, symétrique, anti-symétrique, transitive
    - $\leqslant$ sur $\mathbb{N}$: réflexive, anti-symétrique, transitive
    - $<$ sur $\mathbb{N}$: irréflexive, transitive
    - *diviseur* sur $\mathbb{N}$: réflexive, anti-symétrique, transitive
    - *ancetre* sur personnes : irréflexive, transitive

Relations d'ordre

$\Rightarrow$ Les relations peuvent **ordonner** les éléments d'un ensemble

- Types d'ordres
  - **Pré-ordre** : relation **réflexive** et **transitive**
  - **Équivalence** : pré-ordre symétrique
  - **Ordre** : relation **réflexive**, **anti-symétrique** et **transitive**
    - Ordre **Total** : $\forall(x, y) \in E^2, x \neq y \rightarrow x\mathcal{R}y \vee y\mathcal{R}x$

    $\Rightarrow$ Les éléments deux-à-deux sont toujours en relation
    - Ordre **Partiel** (**treillis**) : $\exists(x, y) \neg x\mathcal{R}y \wedge \neg y\mathcal{R}x$

    $\Rightarrow$ Il existe des paires d'éléments sans relation
    - **Arbre** : $\forall(x, y, z) \in E^3, x\mathcal{R}y \wedge x\mathcal{R}z \wedge x \neq y \neq z \rightarrow y\mathcal{R}z \vee z\mathcal{R}y$
- Exemples
  - *diviseur* sur $\mathbb{N}$: pré-ordre
  - *dizaine*, *cousinade* : équivalence
  - *inclusion*, *sous-chaîne* : ordre partiel
  - $\leqslant$ sur $\mathbb{N}$: ordre total
  - Ordre alphabétique / lexicographique : ordre total

Exercices : morphismes et relations

- Morphisme par concaténation
  - Soit L un langage basé sur un alphabet Σ de 26 lettres (a ...z)
  - L'application de concaténation $c()$ (telle que $c(ab, cd) = abcd$) est-elle surjective ? Quelle contrainte faudrait-il ajouter pour qu'elle soit injective ?
  - L'application $t(\alpha)$ qui compte le nombre de caractères d'une chaîne est-elle injective, surjective ?
  - Nous transformons la concaténation comme opérateur "." (point, tel que $ab.cd = abcd$)
    - Est-il associatif ? Commutatif ?
    - Pour quels opérateurs t est un morphisme de L dans $\mathbb{N}$?
  - On définit la relation sub sur ce langage par le principe de sous-chaîne : $\alpha \; sub \; \beta \leftrightarrow \exists \gamma, \delta \in L^2, \alpha = \gamma.\beta.\delta$
    - Quelles sont les propriétés de l'ordre ainsi défini ?
    - Quelle est le type de cet ordre ?
    - Dessinez le treillis pour $\Sigma = \{a, b\}$ et $\{\alpha \in L, t(\alpha) \leqslant 3\}$