Cours de mathématiques discètes, première année IUT Informatique Sénart

Sabrina Ouazzani, sabrina.ouazzani@lacl.fr

Année scolaire 2017-2018

Première partie

Premier semestre

Table des matières

1 Théorie des ensembles : vocabulaire, relations, ensembles ordonnés

1.1 Vocabulaire et opérations ensemblistes

1.1.1 Notion d'ensemble

Introduction

Commençons par quelques exemples d'ensembles :

- Finis : l'ensemble des élèves de cette classe, l'ensemble des numéros de lignes du métro parisien …
- Infinis : l'ensemble des entiers naturels $\mathbb{N}$, l'ensemble des entiers relatifs $\mathbb{Z}$, l'ensemble des nombres réels $\mathbb{R}$, l'ensemble des nombres pairs, l'ensemble des points du plan …

Première introduction de la notion d'ensemble, par Georg Cantor au 19-ème siècle : « Par ensemble, nous entendons toute collection M d'objets m de notre intuition ou de notre pensée, définis et distincts, ces objets étant appelés les éléments de M ».

Un ensemble est intuitivement une collection d'objets satisfaisant tous une même propriété (par exemple, être un élève de cette classe, être un entier naturel).

L'ensemble est l'objet de base de la théorie des ensembles. Cette théorie se compose d'un certain nombre de "règles" élémentaires (axiomes) qui définissent comment construire et manipuler des ensembles.

Dans ce cours, nous étudierons quelques bases concernant les ensembles mais nous n'aborderons pas l'approche axiomatique de la théorie des en-

sembles [1].

Définitions d'ensembles

Un ensemble peut être défini de deux manières :

- en extension : il s'agit de lister tous ses éléments ;
- en compréhension : il s'agit de donner la propriété commune à tous ses éléments.

Exercice 1.

Dire si les ensembles suivants sont définis en extension ou en compréhension, puis associer les définitions en extension et en compréhension équivalentes :

1. les diviseurs de 14
2. $\{1, 2, 4, 8, 16, 32, 64\}$
3. $\{2, 4\}$
4. les deux plus petits nombres pairs non nuls
5. les puissances de 2 inférieures à 2^6
6. $\{1, 2, 7, 14\}$

Les éléments d'un ensemble *appartiennent* à cet ensemble. On peut aussi dire qu'ils sont *membres* de cet ensemble. L'élément x appartient à l'ensemble X se note $x \in X$. Au contraire, l'élément y n'appartient pas à l'ensemble Y se note $y \notin Y$.

[1] Pour plus d'informations sur cette dernière, l'ouvrage de Halmos "Naive set theory" constitue une bonne introduction (a été traduit en français).

Exercice 2.

Dire si les ensembles suivants sont définis en extension ou en compréhension, puis donner une définition équivalente des ensembles suivants. Si la définition de l'énoncé est en extension, donner une définition en compréhension, et vice-versa

1. $A = \{x \in \mathbb{R} | x(x+5) = 14\}$
2. $B = \{0, 2, 4, 6, 8, 10 \dots\}$
3. $C = \{x \in \mathbb{N} |$ pour tout $n \in \mathbb{N}, x^n = 1\}$
4. $D = \{0\}$
5. $E = \{x \in \mathbb{N} | x \times 0 = 42\}$

Un ensemble qui ne contient qu'un seul élément est appelé un *singleton*.

Quelques propriétés

Un ensemble ne peut pas contenir deux fois le même élément.

Si l'ensemble X contient les mêmes éléments que Y, alors $X = Y$. On dit alors que X et Y sont *égaux*.

Il existe un ensemble vide, noté $\emptyset$. Cet ensemble ne contient rien, bien que cela soit toujours un ensemble.

Exercice 3.

Est-ce que $A = \{\emptyset\}$ est égal à $B = \emptyset$?

Exercice 4.

Existe-t-il un ensemble de tous les ensembles ?

L'ensemble A est un *sous-ensemble* de B si tout élément de A est aussi un élément de B. On le note $A \subseteq B$. On dit aussi que A est *partie* de B ou que A est *inclus* dans B.

L'ensemble A est un *sous-ensemble propre* de B si tout élément de A est aussi un élément de B mais $A \neq B$. On le note $A \subset B$.

Exemple : $\{1, 2\}$ est un sous-ensemble et en particulier un sous-ensemble propre de $\{1, 2, 3\}$.

Attention : ne pas confondre l'appartenance d'un élément à un ensemble ($\in$) avec la propriété d'un ensemble d'être sous-ensemble d'un autre ($\subseteq$). En effet, un ensemble peut être vu comme étant un élément d'un autre ensemble (par exemple $\{4, 2\}$ est un élément de $\{\{4, 2\}, 3, 7\}$) mais cela est différent de l'inclusion ($\{4, 2\}$ n'est pas inclus dans $\{\{4, 2\}, 3, 7\}$ car ni 4 ni 2 ne sont des éléments de ce dernier).

Exercice 5.

L'ensemble vide est-il inclus dans tous les ensembles ?

L'ensemble de tous les sous-ensembles d'un ensemble A, noté $\mathcal{P}(A)$, est appelé l'*ensembles des parties* de A.

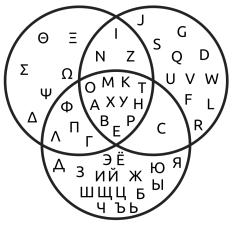
Exercice 6.

Donner l'ensemble des parties des ensembles suivants :

- $A = \{1, 2\}$
- $B = \emptyset$
- $C = \{\emptyset\}$
- $D = \mathcal{P}(\{3, 4\})$

Exercice 7.

1. Est-ce que $A \in \mathcal{P}(A)$? Est-ce que $A \subseteq \mathcal{P}(A)$?
2. Est-ce que $1 \in \mathcal{P}(\{1, 2\})$? Est-ce que $\{1\} \in \mathcal{P}(\{1, 2\})$?



Les ensembles peuvent être graphiquement représentés par des *diagrammes de Venn*.

Sur l'exemple ci-dessus, figurent les lettres communes aux ensembles de lettres latines, grecques, cyrilliques.

1.1.2 Opérations ensemblistes

Soient A et B deux ensembles.

Égalité

Nous avons déjà vu l'égalité de deux ensembles. Nous pouvons maintenant écrire cette propriété de la manière suivante $A = B$ si et seulement si $A \subseteq B$ et $B \subseteq A$.

Union et intersection

L'ensemble des éléments qui sont éléments de A ou éléments de B est appelé l'*union* (ou réunion) de A et de B. L'union de A et de B se note $A \cup B$.

L'ensemble des éléments qui sont des éléments de A et des éléments de B est appelé l'*intersection* de A et de B. L'intersection de A et de B se note $A \cap B$.

L'union et l'intersection sont deux opérations qui possèdent des propriétés particulières. Ici, la notation "$*$" représente l'union ou l'intersection :

- idempotence : $A * A = A$
- commutativité : $A * B = B * A$
- associativité : $A * (B * C) = (A * B) * C$
- élément neutre :
  - $A \cup \emptyset = A$
  - si l'on se place dans un ensemble E et que A est une partie de E, $A \cap E = A$

Exercice 8.

Si l'on se place dans un ensemble E et que A est une partie de E, que vaut $A \cup E$?

Ces deux opérations sont également distributives entre elles :

- distribution de $\cup$ sur $\cap$: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- distribution de $\cap$ sur $\cup$: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Exercice 9.

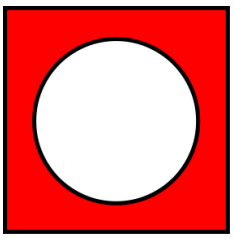
On se donne trois ensembles A, B, C tels que $A \cap B \cap C = \emptyset$. Sont-ils nécessairement disjoints deux à deux ? Donner des exemples.

Exercice 10.

1. Montrer que $A \cap (A \cup B) = A \cup (A \cap B)$.
2. Est-il possible de simplifier cet énoncé ?

Complémentation et différence ensembliste

Soit $A \subset E$. L'ensemble des éléments de E qui ne sont pas des éléments de A est appelé le *complémentaire* de A par rapport à E. Les complémentaire de A par rapport à E se note A^C ou $\overline{A}$.

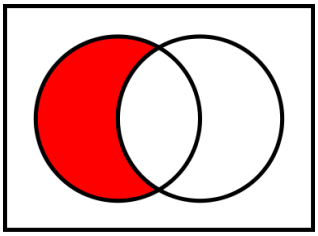


La complémentation possède les propriétés suivantes :

- $A \cap A^C = \emptyset$
- $A \cup A^C = E$
- involution : $(A^C)^C = A$
- lois de De Morgan :
  1. $(A \cup B)^C = A^C \cap B^C$

2. $(A \cap B)^C = A^C \cup B^C$

Soient A et B deux ensembles. L'ensemble des éléments de A qui n'appartiennent pas à B est appelé la *différence ensembliste* de A et de B. La différence ensembliste de A et de B se note $A \setminus B$ et se lit A moins B ou A privé de B.



La différence ensembliste possède les propriétés suivantes :

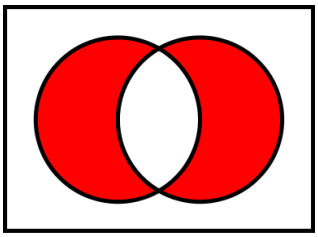
- $(A \cap B) \setminus C = A \cap (B \setminus C) = (A \setminus C) \cap (B \setminus C)$
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

De plus $A \setminus B = \emptyset$ si et seulement si $A \subseteq B$.

Différence symétrique

L'ensemble des éléments qui appartiennent soit à A, soit à B, mais pas aux deux à la fois, est appelé la *différence symétrique* de A et de B. La différence symétrique de A et de B se note $A \Delta B$.

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$



Exercice 11.

Soit $A = \{1, 2, 3, 4, 5, 6\}$ et $B = \{1, 3, 5, 7, 9\}$. Calculer $A \Delta B$.

La différence symétrique possède les propriétés suivantes :

- commutativité : $A\Delta B = B\Delta A$
- associativité : $(A\Delta B)\Delta C = A\Delta(B\Delta C)$
- élément neutre : $A\Delta\emptyset = A$
- $A\Delta A = \emptyset$

La propriété suivante est également vérifiée : $A\Delta B = \emptyset$ si et seulement si $A = B$.

Produit cartésien

L'ensemble des couples (a, b) où $a \in A$ et $b \in B$ est appelé le *produit cartésien* de A et de B. Le produit cartésien de A et de B se note $A \times B$.

Attention, le produit cartésien n'est pas une opération commutative : $A \times B \neq B \times A$.

Les couples (a, b) sont des éléments, pas des ensembles. De plus, le couple (a, b) est distinct du couple (b, a).

Exercice 12.

Procéder à l'union, l'intersection, la complémentation (par rapport à $\{1, 2, 3\}$) et le produit cartésien des couples d'ensembles A et B suivants, illustrer les réponses par des diagrammes de Venn :

- $A = \{1, 2\}$, $B = \{1, 3\}$
- $A = \emptyset$, $B = \{1, 3\}$

1.2 Relations

1.2.1 Relations et fonctions

Relations

Un sous-ensemble G du produit cartésien $A \times B$ définit une *relation binaire* entre A et B. L'ensemble A est alors l'*ensemble de départ*, l'ensemble B est l'*ensemble d'arrivée* et le sous-ensemble G de $A \times B$ considéré est appelé le *graphe* de la relation. On note en général $\mathcal{R}$ une relation.

Si (x, y) est un couple du graphe, on le note $x\mathcal{R}y$ ou $\mathcal{R}(x, y)$, ce qui se lit x est en relation avec y.

Un sous-ensemble du produit cartésien $A \times B \times C \cdots$ définit une *relation n-aire* entre $A, B, C \cdots$.

Exemples :

- soit A l'ensemble des aéroports de France. On peut considérer la relation binaire *volDirect* qui est un sous-ensemble de $A \times A$ tel que $volDirect(a_1, a_2)$ est vraie si et seulement s'il existe une liaison commerciale directe entre l'aéroport a_1 et l'aéroport a_2.
- soit E l'ensemble des étudiants de cette classe. On peut considérer la relation binaire *estVoisinDe* qui est un sous-ensemble de $E \times E$ tel que $estVoisinDe(e_1, e_2)$ est vraie si et seulement si l'étudiant e_1 est assis à côté de l'étudiant e_2.

Remarquons que les relations sont des ensembles et que les opérations que nous avons définies sur les ensembles s'y appliquent.

Une relation binaire $\mathcal{R}$ sur $A \times A$ est :

- *symétrique* si $a\mathcal{R}b$ alors $b\mathcal{R}a$
- *antisymétrique* si $\forall a, b$ si $a\mathcal{R}b$ et $b\mathcal{R}a$ alors $a = b$
- *réflexive* si $\forall a$ alors $a\mathcal{R}a$
- *transitive* si $\forall a, b, c$ si $a\mathcal{R}b$ et $b\mathcal{R}c$ alors $a\mathcal{R}c$

Si une relation est à la fois symétrique, réflexive et transitive, on dit que cette relation est une *relation d'équivalence*.

Exercice 13.

Dire si les relations sur les ensembles A, E, définis comme exemples plus haut, respectent les propriétés de symétrie, d'anti-symétrie, de réflexivité et de transitivié. Préciser également si ces relations sont des relations d'équivalence.

Applications

Une *application* de A dans B est une relation binaire $\mathcal{R}$ dont le graphe G est muni des propriétés suivantes :

- pour tout élément x de A, il doit exister un élément y de B tel que (x, y) est un élément de G

- cet élément y est unique

Dans ce cas, y est appelé l'*image* de x par $\mathcal{R}$, et x est appelé l'*antécédent* de y par $\mathcal{R}$.

Cela peut aussi s'écrire formellement par $y = \mathcal{R}(x)$.

Soit f une application. On note :

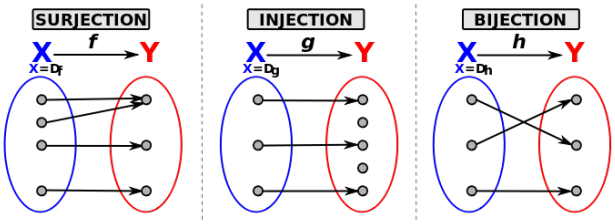
- $f : E \to F$ la proposition "f est une application de E dans F"
- $f : x \mapsto y$ la proposition "y est l'image de x par f"

Une *relation fonctionnelle*, ou *fonction* est une application pour laquelle, dans la définition précédente, y peut ne pas être défini (x est en relation avec 0 ou 1 élément de B).

Soit f une application dans laquelle on note y l'image de x :

- Une application est *surjective* (on dit aussi que c'est une *surjection*) si tout élément y admet un antécédent.
- Une application est *injective* (on dit aussi que c'est une *injection*) si y admet au plus un antécédent.
- Une application est *bijective* (on dit aussi que c'est une *bijection*) si elle est injective et surjective.

Tout élément de l'ensemble d'arrivée d'une application bijective a donc *exactement un* antécédent.



Exercice 14.

Soit f une application des étudiants de cette classe vers les plateaux (remplis) du RU qui définit la répartition des plateaux entre les étudiants.

- A priori, vous souhaitez que f soit plutôt injective ou surjective ?
- A priori, vous pensez que le personnel souhaite que f soit plutôt injective ou surjective ?
- Est-ce que tout le monde peut se mettre d'accord sur la propriété de f ?

Remarquons dans l'exercice précédent que, parce que f est une application, vous ne pouvez pas manger plusieurs plateaux (le y est unique) et que chacun mangera (pour chaque étudiant x, le y existe) ! Si f était une fonction, il se pourrait que certains ne mangent pas de plateaux.

Méthodologie : soit $f : A \to B$.

- Pour montrer que f est injective, montrer que si $f(x) = f(y)$ alors $x = y$.
- Pour montrer que f n'est pas injective, exhiber deux éléments x et y de A tels que $x \neq y$ et $f(x) = f(y)$.
- Pour montrer que f est surjective, montrer que pour tout élément y de B, il existe au moins un élément x de A tel que $f(x) = y$.
- Pour montrer que f n'est pas surjective, exhiber un élément y de B tel que, pour tout élément x de A, $f(x) \neq y$.

Soit $f : A \to B$ une application bijective. La fonction *inverse* (ou *réciproque*) de f est la fonction $f^{-1} : B \to A$ telle que $f^{-1}(b) = a$ si et seulement si $f(a) = b$.

Une fonction qui n'est pas bijective n'a pas d'inverse.

Soit $g : A \to B$ et $f : B \to C$. La fonction $f \circ g : A \to C$ est la *composition* de f et de g et est définie par $(f \circ g)(a) = f(g(a))$.

La composition $f \circ g$ est définie quand l'image de g est un sous-ensemble de l'image de f. Elle n'est pas définie sinon.

1.2.2 Cardinalité

Soient A et B deux ensembles. On dit que A et B ont la même *cardinalité* si et seulement s'il existe une bijection entre A et B. Cela se note $|A| = |B|$.

On a que :

- $|A| \leq |B|$ si et seulement s'il existe une injection de A vers B.
- $|A| \geq |B|$ si et seulement s'il existe une surjection de A vers B.

Un ensemble est *fini* s'il contient exactement m éléments distincts où m est un entier naturel. Dans ce cas, m est la cardinalité de l'ensemble.

L'ensemble vide a pour cardinalité 0.

Exercice 15.

Dire si les ensembles suivants sont finis :

- $\emptyset$
- $\mathbb{N}$
- $\{1, 42, 3000000, 12, 5^{23}\}$

Un ensemble est *dénombrable* s'il :

- est fini ;
- ou est infini et a la même cardinalité que $\mathbb{N}$.

On peut voir les éléments d'un ensemble dénombrable comme étant indexés par des entiers naturels.

Exercice 16.

Dire si les ensembles suivants sont dénombrables :

- $\emptyset$
- $\mathbb{N}$
- $\{1, 42, 3000000, 12, 5^{23}\}$
- l'ensemble des nombres pairs
- $\mathbb{R}$

1.3 Ensembles ordonnés

Un *ordre* sur un ensemble E, est une relation binaire sur E qui est réflexive, transitive et antisymétrique.

Un *ordre total* sur un ensemble E, est un odre muni de la propriété de totalité : $\forall a, b$ $a\mathcal{R}b$ ou $b\mathcal{R}a$.

Une relation d'ordre peut ne pas respecter la totalité. On parle alors de relation d'ordre *partiel*.

La relation $\leq$ (au sens usuel) sur $\mathbb{R}$ est un exemple de relation d'ordre total.

Exercice 17.

Est-ce que la relation $\subseteq$ sur $\mathcal{P}(E)$ est une relation d'ordre ?

On appelle *ensemble ordonné* un ensemble non vide muni d'une relation d'ordre. Un *ensemble partiellement ordonné* est un ensemble non vide muni d'une relation d'ordre partiel. Un *ensemble totalement ordonné* est un ensemble non vide muni d'une relation d'ordre total.

Précisons que, par la suite, nous désignerons par *ordre* un ensemble ordonné.

Un *plus petit élément* (ou *minorant*) m de l'ensemble E muni de la relation d'ordre $\mathcal{R}$ est un élément m tel que $m\mathcal{R}e$ pour tout élément de e de E.

Un *plus grand élément* (ou *majorant*) M de l'ensemble E muni de la relation d'ordre $\mathcal{R}$ est un élément M tel que $e\mathcal{R}M$ pour tout élément de e de E.

Un *bon ordre* sur un ensemble E est un ordre sur E, muni de la propriété que tout sous-ensemble non-vide de E contient un plus petit élément.

Exercice 18.

Est-ce que les ensembles bien ordonnés sont aussi totalement ordonnés ?

2 Logique : calcul propositionnel et calcul des prédicats

2.1 Calcul propositionnel

2.1.1 Proposition

Une *proposition* est un énoncé auquel on peut attribuer une valeur de vérité : vrai ou faux.

Exemples : “Il y a des élèves dans cette classe” (proposition vraie), “Il n’y a pas d’élèves dans cette classe” (proposition fausse), “ 6 * 7 = 42” (proposition vraie), “6 * 7 = 49” (proposition fausse).

Les énoncés interrogatifs, impératifs, hypothétiques et paradoxes du menteur (“Je mens”) ne sont pas des propositions car on ne peut pas leur attribuer de valeur de vérité.

Une proposition est soit vraie, soit fausse (et rien d’autre, on appelle cela le principe *tiers-exclu*). Elle ne peut pas être à la fois vraie et fausse (principe de *non-contradiction*).

Nous étudierons ici des formules décrivant des relations entre objets et qui, après que chaque objet ait reçu une valeur de vérité, prennent une valeur de vérité globale (et sont donc des propositions).

2.1.2 Langage

Nous manipulerons le *langage* suivant, qui décrit les éléments qui composent les formules :

- un ensemble dénombrable de *variables propositionnelles* ou *propositions atomiques*, en général notées $p, q, r \ldots$;
- un ensemble fini d’*opérateurs* ou *connecteurs* ;

- les constantes “vrai” ($\top$ ou t ou 1) et “faux” ($\bot$ ou f ou 0) ;
- des parenthèses (on peut les omettre si on définit un ordre de priorité des connecteurs).

Les connecteurs considérés sont, dans l'ordre de priorité :

- $\neg$, lu ”non” ($\neg A$ peut aussi être noté $\overline{A}$) ;
- $\wedge$, lu ”et” ; $\vee$, lu ”ou” ;
- $\rightarrow$, lu ”quand”, ”si... alors” ; $\leftrightarrow$, lu ”équivalent à”.

Ainsi, une formule de la logique des propositions se définit de la manière suivante :

- ce peut être une proposition atomique ou une constante ;
- ce peut être une formule composée par les opérateurs présentés.

Exemples : p, $p \wedge q$, $p \vee \neg q$ ...

Exercice 19.

Soient : p = “il fait froid”, q = “il pleut”, a = “Jean fait des des maths”, b = “Jean fait de la danse”, c = “Jean fait de la biologie”.

1. Enoncer en français les formules logiques : $\neg p$, $p \wedge q$, $p \vee q$, $p \vee \neg q$, $q \rightarrow p$, $p \rightarrow q$, $\neg p \rightarrow \neg q$.
2. Formaliser ces énoncés français en logique propositionnelle :
   - “Jean fait des maths mais pas de biologie.”
   - “Jean ne fait ni maths ni danse.”
   - “Jean étudie exactement une matière.”
   - “Jean n'étudie pas plus d'une matière.”
   - “Si Jean fait des maths ou de la biologie alors il n'étudie pas la danse.”

2.1.3 Sémantique

Exercice 20.

Considérons les formules :

- ”3 est impair” $\wedge$ ”Paris est la capitale de la France”
- ”2 est impair” $\vee$ $\neg$”Paris est la capitale de la France”

Sont-elles vraies ?

Nous pouvons attribuer une valeur de vérité aux expressions composées.

Pour cela, nous définissons une fonction totale d'*interprétation*, ou *valuation*, v qui, à chaque atome, associe la constante 0 ou 1.

La valuation d'une formule se calcule ensuite de la manière suivante :

- $v(0) = 0$
- $v(1) = 1$
- $v(\neg A) = 1$ ssi $v(A) = 0$
- $v(A \wedge B) = 1$ ssi $v(A) = 1$ ET $v(B) = 1$
- $v(A \vee B) = 1$ ssi $v(A) = 1$ OU $v(B) = 1$
- $v(A \rightarrow B) = 1$ ssi $v(\neg A \vee B)$ ssi $(v(A) = 0)$ OU $v(B) = 1$
- $v(Ap \leftrightarrow B) = 1$ ssi $v(A) = v(B)$ ssi $v(A \rightarrow B)$ ET $v(B \rightarrow A)$

Nous notons $v(A)$ la valeur de vérité d'une formule A dans une valuation v.

La *table de vérité* d'une formule est une présentation exhaustive des valeurs de vérité possibles de ses composantes, associées aux valeurs de vérité correspondantes de la formule.

Nous présentons respectivement ci-dessous les tables de vérité de la négation, de la conjonction, de la disjonction, de l'implication et de l'équivalence.

p	NON p
1	0
0	1

p	q	p ET q
1	1	1
1	0	0
0	1	0
0	0	0

p	q	p OU q
1	1	1
1	0	1
0	1	1
0	0	0

p	q	$p \rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Notons que $(p \vee q)$ est vraie, soit si p est vraie, soit si q est vraie, soit si les deux sont vraies. C'est un OU non-exclusif. Ce n'est pas toujours le cas en langage naturel.

- Une interprétation v est appelée un *modèle* de A si et seulement si $v(A) = 1$.
- Une formule A est *satisfiable* si et seulement si elle possède un modèle.
- Une formule A est *valide* si et seulement si toutes ses interprétations sont des modèles.
- Une formule A est une *contradiction* si et seulement si elle ne possède pas de modèle.
- Deux formules A et B sont *logiquement équivalentes* si et seulement si A et B sont vraies dans exactement les mêmes interprétations : A et B ont exactement les mêmes modèles. Cela se note $A \equiv B$.
- Une formule B est une *conséquence logique* des formules $A_1 \cdots A_k$ si toute interprétation qui est un modèle de toutes les formules $A_1 \cdots A_k$ est aussi un modèle de B. Cela se note $A_1 \cdots A_k \models B$.

Exercice 21.

Montrer la conséquence logique suivante : $A, A \rightarrow B \models B$.

Les opérateurs $\vee$ et $\wedge$ sont associatifs :

- $(A \vee B) \vee C = A \vee (B \vee C) = A \vee B \vee C$

- $(A \wedge B) \wedge C = A \wedge (B \wedge C) = A \wedge B \wedge C$

Exercice 22.

Montrer que les propositions $A \vee (B \wedge C)$ et $(A \vee B) \wedge C$ ne sont pas équivalentes.

Les opérateurs $\vee$ et $\wedge$ sont distributifs :

- $A \vee (B_1 \wedge \cdots \wedge B_k) \equiv (A \vee B_1) \wedge \cdots \wedge (A \vee B_k)$
- $A \wedge (B_1 \vee \cdots \vee B_k) \equiv (A \wedge B_1) \vee \cdots \vee (A \wedge B_k)$

Les lois de De Morgan s'appliquent :

- $\neg(A_1 \wedge \cdots \wedge A_k) \equiv (\neg A_1 \vee \cdots \vee \neg A_k)$
- $\neg(A_1 \vee \cdots \vee A_k) \equiv (\neg A_1 \wedge \cdots \wedge \neg A_k)$

Exercice 23.

Montrer avec une table de vérité que :

- $(p \to q)$ est une proposition équivalente à $((\neg p) \vee q)$. En particulier, $(p \to q)$ est vraie quand p est fausse. Ceci est la définition de l'implication.
- $(p \to q)$ est une proposition équivalente à $\neg q \to \neg p$. Ceci est la *contraposée*.
- $((p \to q) \to r)$ et $(p \to (q \to r))$ ne sont pas équivalentes.
- $(\neg(p \to q))$ est une proposition équivalente à $(p \wedge (\neg q))$.
- $p \to (q \to r)$ est une proposition équivalente à $(p \wedge q) \to r$. Ceci est la *curryfication*.

2.1.4 Déduction naturelle

Les tables représentent parfois trop de travail pour montrer une équivalence ou une conséquence logique. Souvent, on parvient à les prouver avec un raisonnement plus naturel. Voyons[1] cet argument en français :

"Des poils de chat ou des poils de chien on été trouvés sur la scène du crime. Si des poils de chien ont été trouvés, l'officier Thomas a eu une crise d'allergie. Si des poils de chat ont été trouvés, alors Maubert est responsable du crime. Mais l'officier Thomas n'a pas eu de crise d'allergie, et donc Maubert doit être responsable du crime."

La validité de l'argument peut être rendue évidente en représentant la chaîne de raisonnement qui conduit des *prémisses* (les données du problème) aux *conclusions* :

1. Des poils de chat ou des poils de chien on été trouvés sur la scène du crime. (Prémisse)
2. Si des poils de chien ont été trouvé, l'officier Thomas a eu une crise d'allergie. (Prémisse)
3. Si des poils de chat ont été trouvés, alors Maubert est responsable du crime. (Prémisse)
4. L'officier Thomas n'a pas eu de crise d'allergie. (Prémisse)
5. Des poils de chien n'ont pas été trouvés sur la scène du crime. [suivant 2, 4]
6. Des poils de chat ont été trouvés sur la scène du crime. [suivant 1, 5]
7. Maubert est responsable du crime. [suivant 3, 6] (Conclusion)

On va utiliser :

- la notion de conséquence logique pour faire des déductions ;
- la notion d'équivalence logique pour définir une règle de réécriture qui permet de transformer une formule en formules de forme différente mais logiquement équivalentes.

L'ensemble des *sous-formules* d'une formule A est le plus petit ensemble tel que :

[1] `http://www.iep.utm.edu/prop-log/`

- A est une sous-formule de A.
- Si $\neg B$ est une sous-formule de A alors B est une sous-formule de A.
- Si $B \wedge C$ est une sous-formule de A alors B et C sont des sous-formules de A.
- Si $B \vee C$ est une sous-formule de A alors B et C sont des sous-formules de A.
- Si $B \to C$ est une sous-formule de A alors B et C sont des sous-formules de A.

L'endroit où une sous-formule apparaît est son *occurrence*.
Exemples :
Considérons la formule $((p \vee q) \wedge \neg p)$. p en est une sous-formule, ainsi que $(p \vee q)$ et $(\neg p)$, tandis que $(q \wedge \neg p)$ ne l'est pas. On dit que p a deux occurrences dans $((p \vee q) \wedge \neg p)$, et $(p \vee q)$ une.

Exercice 24.

Quel est l'ensemble des sous-formules de $(((p \vee q) \wedge \neg p) \to \bot)$?

Si $A \equiv B$ et A est une sous-formule de C :

- on peut remplacer A par B dans C pour obtenir C'
- on a $C \equiv C'$

Les équivalences logiques couramment utilisées sont celles du tableau figurant ci-dessous.

Équivalence logique	Nom
$X \vee \neg X \equiv t$	Tautologie (Tau)
$X \wedge \neg X \equiv f$	Contradiction (Cont)
$X \vee t \equiv t$	Dominance (Dom$\vee$)
$X \vee f \equiv X$	Dominance (Dom$\vee$)
$X \wedge f \equiv f$	Dominance (Dom$\wedge$)
$X \wedge t \equiv X$	Dominance (Dom$\wedge$)
$\neg(\neg X) \equiv X$	Double négation (DN)
$X \vee Y \equiv Y \vee X$	Commutativité (Com$\vee$)
$X \wedge Y \equiv Y \wedge X$	Commutativité (Com$\wedge$)
$(X \vee Y) \vee Z \equiv X \vee (Y \vee Z)$	Associativité (Assoc$\vee$)
$(X \wedge Y) \wedge Z \equiv X \wedge (Y \wedge Z)$	Associativité (Assoc$\wedge$)
$X \vee X \equiv X$	Idempotence (Id$\vee$)
$X \wedge X \equiv X$	Idempotence (Id$\wedge$)
$\neg(X \wedge Y) \equiv \neg X \vee \neg Y$	De Morgan (DM$\wedge$)
$\neg(X \vee Y) \equiv \neg X \wedge \neg Y$	De Morgan (DM$\vee$)
$X \to Y \equiv \neg Y \to \neg X$	Contraposée (C)
$X \to Y \equiv \neg X \vee Y$	Implication (Impl)
$X \to (Y \to Z) \equiv (X \wedge Y) \to Z$	Curryfication (Cu)
$X \vee (X \wedge Y) \equiv X$	Absorption (Abs$\vee$)
$X \wedge (X \vee Y) \equiv X$	Absorption (Abs$\wedge$)
$X \vee (Y \wedge Z) \equiv (X \vee Y) \wedge (X \vee Z)$	Distributivité (Dis$\vee$)
$X \wedge (Y \vee Z) \equiv (X \wedge Y) \vee (X \wedge Z)$	Distributivité (Dis$\wedge$)
$X \leftrightarrow Y \equiv (X \to Y) \wedge (Y \to X)$	Equivalence (Eq1)
$X \leftrightarrow Y \equiv (X \wedge Y) \vee (\neg Y \wedge \neg X)$	Equivalence (Eq2)

TAB. 2.1 : Équivalences logiques courantes.

Exemple 1. *Supposons que $A \equiv B$. Alors :*

- *$(A \vee C) \to D$ peut être réécrite $(B \vee C) \to D$.*
- *$(A \vee C) \to D \equiv (B \vee C) \to D$*

Exemple 2. *On montre que $\neg(A \to B) \equiv A \wedge \neg B$.*

1. *$\neg(A \to B)$*
2. *$\neg(\neg A \vee B)$ [1, Impl]*
3. *$\neg\neg A \wedge \neg B$ [2, DM$\vee$]*

4. $A \wedge \neg B$ *[3, DN]*

Exercice 25.

Montrer que $(A \wedge B) \vee (\neg A \wedge C) \vee (B \wedge C) \equiv (A \wedge B) \vee (\neg A \wedge C)$.
A chaque étape, indiquer quelle règle a été appliquée.

Exercice 26.

Prouver par le calcul :

1. $A \vee (A \wedge B) \equiv A$ [sans utiliser Abs$\vee$]
2. $A \wedge t \equiv A$ [sans utiliser Dom$\wedge$]

Preuves directes : Des prémisses à la conclusion

Ce sont des équivalences logiques, donc elles "marchent" dans les deux sens.

Nous avons la propriété que $A \equiv B$ ssi $A \models B$ et $B \models A$.

Ainsi, pour prouver l'équivalence logique, on fera souvent deux preuves de conséquence logique.

Une *preuve directe* de $A_1, \ldots, A_k \models B$ est une séquence de formules telle que chaque étape est soit :

- une prémisse A_i ;
- la conlusion d'une conséquence logique en partant de formules précédentes dans la séquence.

La conclusion de la preuve est la dernière ligne de la preuve.

Pour montrer une conséquence logique, on utilise aussi des *règles d'inférence* qui "marchent" dans un seul sens, comme dans la Table 2.2.

Conséquence logique	Nom
$X \to Y, X \models Y$	Modus Ponens (MP)
$X \to Y, \neg Y \models X$	Modus Tolens (MT)
$X \vee Y, \neg X \models Y$	Syllogisme Disjonctif (SD1)
$X \vee Y, \neg Y \models X$	Syllogisme Disjonctif (SD2)
$X \models X \vee Y$	Addition (Add1)
$Y \models X \vee Y$	Addition (Add2)
$X \wedge Y \models X$	Simplification (Simp1)
$X \wedge Y \models Y$	Simplification (Simp2)
$X, Y \models X \wedge Y$	Conjonction (Conj)
$X \to Y, Y \to Z \models X \to Z$	Syllogisme Hypothétique (SH)
$(X \to Z), (Y \to U), X \vee Y \models Z \vee U$	Dilemme Constructif (DC)
$X \to Y \models X \to (X \vee Y)$	Absorption (Abs$\to$)

Tab. 2.2 : Règles d'inférence de la déduction naturelle.

Exercice 27.

Des poils de chat ou des poils de chien on été trouvés sur la scène du crime. Si des poils de chien ont été trouvé, l'officier Thomas a eu une crise d'allergie. Si des poils de chat ont été trouvés, alors Maubert est responsable du crime. Mais l'officier Thomas n'a pas eu de crise d'allergie, et donc Maubert doit être responsable du crime.

1. Trouver et formaliser les prémisses de l'énoncé. On pourra utiliser les variables $Chien$, $Chat$, Off, $Maub$
2. Identifier et formaliser les conclusions de l'énoncé.
3. Exprimer l'énoncé sous forme de conséquence logique.
4. Prouver la conséquence logique $[Chat \vee Chien, Chien \to Off, Chat \to Maub, \neg Off \models Maub]$ par le calcul.

Exercice 28.

Prouver par le calcul :

1. $P \vee Q, P \to R, Q \to S \models R \vee S$
2. $A, B \models A$
3. $A, B \models (A \wedge B) \vee C$
4. $\neg(P \wedge Q), P \models \neg Q$

Plus tard on pourra se passer d'indiquer les étapes de commutativité.

2.1.5 Formes normales

En utilisant les équivalences logiques, on peut réécrire une formule A de manière à obtenir une formule B logiquement équivalente ($A \equiv B$) qui sera plus facile à lire ou plus adaptée aux calculs.

Certaines formes de formules sont tellement importantes qu'elles sont même dites *normales*.

Définition de la *syntaxe additionnelle* :

- littéraux (un atome ou la négation d'un atome)
- $\vee$-clauses ("une somme de littéraux")
- $\wedge$-clauses ("un produit de littéraux"), aussi appelé *monôme*
- DNF (Disjunctive Normal Form) : une disjonction de $\wedge$-clauses ("une somme de produits")
- CNF (Conjonctive Normal Form) : une conjonction de $\vee$-clauses ("un produit de sommes")

On peut trouver une DNF d'une formule à partir de sa table de vérité.

Exemple 3. *On se donne la table de vérité :*

p	q	r	$A = (p \vee \neg q \vee r) \rightarrow (p \wedge r))$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

La formule A est vraie exactement quand :

- $\neg p \wedge q \wedge \neg r$ *ou*
- $p \wedge \neg q \wedge \neg r$ *ou*
- $p \wedge q \wedge r$

Donc, une DNF équivalente à A est simplement :

$$(\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r)$$

On peut aussi trouver une CNF d'une formule F à partir de sa table de vérité. On commence par trouver la table de vérité de $\neg F$ puis on simplifie $\neg\neg F$ en appliquant des règles de De Morgan et des double négation.

En général, on peut suivre l'algorithme suivant pour convertir n'importe quelle formule dans une CNF.

Algorithme 1. *Une formule peut être mise sous forme normale conjonctive en suivant l'algorithme suivant :*

1. *tant que possible, appliquer l'équivalence logique (en remplaçant l'équivalence matérielle par sa définition en terme d'implications logiques)* $A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$
2. *tant que possible, appliquer l'équivalence logique (en remplaçant l'implication matérielle par sa définition en terme de disjonction)* $A \rightarrow B \equiv \neg A \vee B$
3. *tant que possible, appliquer les équivalences logiques suivantes (en remplaçant un membre gauche par le membre droit équivalent) :*
   (a) $\neg\neg A \equiv A$
   (b) $\neg(A_1 \wedge \ldots \wedge A_k) \equiv (\neg A_1 \vee \ldots \vee \neg A_k)$

(c) $\neg(A_1 \vee \ldots \vee A_k) \equiv (\neg A_1 \wedge \ldots \wedge \neg A_k)$

(d) $A \vee (B_1 \wedge \ldots \wedge B_k) \equiv (A \vee B_1) \wedge \ldots \wedge (A \vee B_k)$

Exemple 4. *On a la formule* $F = (a \to b) \vee (\neg c \wedge a)$.
On obtient cette suite d'équivalences logiques :

1. $(a \to b) \vee (\neg c \wedge a)$
2. $(\neg a \vee b) \vee (\neg c \wedge a)$
3. $((\neg a \vee b) \vee \neg c) \wedge ((\neg a \vee b) \vee a)$
4. $(\neg a \vee b \vee \neg c) \wedge (\neg a \vee b \vee a)$

On obtient une CNF.
Elle peut être simplifiée !

1. $(\neg a \vee b \vee \neg c) \wedge (\neg a \vee b \vee a)$
2. $(\neg a \vee b \vee \neg c) \wedge (b \vee \neg a \vee a)$
3. $(\neg a \vee b \vee \neg c) \wedge (b \vee \neg a \vee a)$
4. $(\neg a \vee b \vee \neg c) \wedge (b \vee t)$
5. $(\neg a \vee b \vee \neg c) \wedge t$
6. $\neg a \vee b \vee \neg c$

a	b	c	$(a \to b)$	$(\neg c \wedge a)$	$F = (a \to b) \vee (\neg c \wedge a)$	$\neg a \vee b \vee \neg c$
0	0	0	1	0	1	1
0	0	1	1	0	1	1
0	1	0	1	0	1	1
0	1	1	1	0	1	1
1	0	0	0	1	1	1
1	0	1	0	0	0	0
1	1	0	1	1	1	1
1	1	1	1	0	1	1

A partir de là, il est aussi très facile de trouver une CNF d'une formule à partir de sa table de vérité.

Exemple 5. *On se donne la table de vérité :*

p	q	r	A	$\neg A$
0	0	0	0	1
0	0	1	0	1
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	0

La formule $\neg A$ est vraie exactement quand :

- $\neg p \wedge \neg q \wedge \neg r$ *ou*
- $\neg p \wedge \neg q \wedge r$ *ou*
- $\neg p \wedge q \wedge r$ *ou*
- $p \wedge \neg q \wedge r$ *ou*
- $p \wedge q \wedge \neg r$

Donc, une DNF équivalente à $\neg A$ est simplement :

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r)$$

On a $A \equiv \neg\neg A$. Donc A est logiquement équivalente à :

$$\neg((\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r))$$

On obtient une CNF en appliquant l'algorithme. En fait, il suffit d'appliquer la dernière étape :

$$(p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$$

2.1.6 Simplifications

Commes les tests dans un programme, les circuits électroniques correspondent à des formules logiques. Simplifier un circuit électrique revient à simplifier sa représentation en logique. Cela permet de faire des designs plus simples, moins chers, de consommation moindre, …

Par exemple, plutôt que d'implanter un circuit $(C \wedge A) \vee (C \wedge B) \vee (\neg C \wedge A) \vee (\neg C \wedge B)$ qui comporte 4 portes logiques AND, 3 portes OR, et 2 portes NOT, il vaudra mieux implanter un circuit $A \vee B$.

Exercice 29.

Montrer en utilisant des équivalences logiques que $(C \wedge A) \vee (C \wedge B) \vee (\neg C \wedge A) \vee (\neg C \wedge B) \equiv A \vee B$.
(Indication 1 : Une équivalence logique peut se montrer dans un sens et dans un autre. Indication 2 : $t \equiv (C \vee \neg C)$.)

Mais avec la méthode des équivalences logiques, le calcul peut devenir laborieux pour simplifier les formes propositionelles à plus de deux variables.

Une méthode sémantique consiste à présenter les tables de vérité de manière à utiliser la capacité naturelle de la cognition humaine à trouver des motifs.

Il faut d'abord savoir énumérer des ensembles de valuations selon le *code de Gray* où deux valuations successives ne diffèrent que de un bit.

- pour une variable : 0 1
- pour deux variables : 00 01 | 11 10
- pour trois variables : 000 001 011 010 | 110 111 101 100
- pour quatres variables : 0000 0001 0011 0010 0110 0111 0101 0100 | 1100 1101 1111 1110 1010 1011 1001 1000

Un *tableau de Karnaugh* pour deux variables x et y est de la forme :

x \ y	$\bar{y}$	y
$\bar{x}$	$\bar{x}\bar{y}$	$\bar{x}y$
x	$x\bar{y}$	xy

ou

x \ y	0	1
0	00	01
1	10	11

Un tableau de Karnaugh pour trois variables x, y, et z est de la forme :

x \ yz	00	01	11	10
0	000	001	011	010
1	100	101	111	110

Un tableau de Karnaugh pour quatre variables w, x, y, et z est de la forme :

wx \ yz	00	01	11	10
00	0000	0001	0011	0010
01	0100	0101	0111	0110
11	1100	1101	1111	1110
10	1000	1001	1011	1010

Les tableaux de Karnaugh sont construits de manière à ce qu'on puisse les parcourir d'une case à une autre en changeant exactement un littéral. Par exemple, avec 3 variables, on peut passer de la case $x \wedge \neg y \wedge z$ vers la case $x \wedge \neg y \wedge \neg z$. Sur une ligne l, on peut aussi passer de la case la plus à droite à la case la plus à gauche, et inversément. Sur une colonne c, on peut aussi passer de la case la plus haute à la case la plus basse, et inversément.

Un *1groupe* G est un ensemble de cases d'un tableau de Karnaugh tel que :

- toute case de G contient un 1 ;
- G est un rectangle (possiblement carré, possiblement à cheval sur les bords), et contient 2^j cases, avec j entre 0 et le nombre de variables.

Méthodologie :

La *technique de Karnaugh* consiste à examiner les tableaux de Karnauh et trouver les 1groupes de 1. On construit les plus grands 1groupes possibles en assurant tous les 1 de la tables sont dans au moins un groupe, possiblement plusieurs !

C'est-à-dire, pour une formule F, on cherche un ensemble M de monômes, $\wedge$-clauses, tel que :

- si $A \in M$ alors $A \models F$
- $F \models \bigwedge_{A \in M} M$

On peut aussi chercher les 0groupes pour déterminer une forme simple de la négation $\neg F$ d'une formule F. En appliquant la règle de De Morgan et la règle de double négation, on trouve une forme simple de la formule F.

Exemple 6. *Avec trois variables p, q et r, des tables de vérité, leur tableau de Karnaugh correspondant, et une forme propositionnelle :*

p	q	r	F_1
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

p \ qr	00	01	11	10
0	0	1	1	0
1	0	1	1	0

$F_1 \equiv r$

p	q	r	F_2
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

p \ qr	00	01	11	10
0	1	1	0	0
1	0	0	1	1

$F_2 \equiv (\neg p \wedge \neg q) \vee (p \wedge q)$

p	q	r	F_3
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

p \ qr	00	01	11	10
0	1	1	1	1
1	0	0	1	1

$F_3 \equiv \neg p \vee q; \neg F_3 \equiv p \wedge \neg q; F_3 \equiv \neg\neg F_3 \equiv \neg p \vee q$

Exercice 30.

Déterminer une forme propositionelle simple correspondant à ces tableaux de Karnaugh :

(1)

wx \ yz	00	01	11	10
00	1	0	0	1
01	0	1	1	0
11	0	1	1	0
10	1	0	0	1

(2)

wx \ yz	00	01	11	10
00	1	1	1	1
01	1	1	1	1
11	1	1	1	1
10	0	0	0	0

Exercice 31.

Utiliser les tableaux de Karnaugh pour simplifier :

1. $(x \wedge y) \vee (\neg x \wedge y)$
2. $(x \wedge \neg y) \vee (\neg x \wedge y)$
3. $(x \wedge \neg y) \vee (\neg x \wedge y) \vee (\neg x \wedge \neg y)$

2.2 Calcul des prédicats

La logique propositionnelle ne suffit pas à exprimer des détails importants dans des énoncés dans le language naturel (français...) ou en mathématique.[2]

Entrer dans la structure d'une proposition On a vu dans l'introduction que certains énoncés utilisent des variables qui ne sont pas des propositions elle-mêmes.

$5+5=10$ est une proposition vraie. $5+2=8$ est une proposition fausse. En revanche, $5+2=x$ n'est pas une proposition. Elle le devient quand x a une valeur, mais x n'est pas elle-même une variable propositionnelle.

[2]On suit la présentation de "Discrete Mathematics and Its Applications" (7ième édition) de K. Rosen.

Déduire des spécialisations et généralisations En logique propositionnelle on ne peut pas non plus faire des raisonnements permettant de spécialiser ou généraliser des énoncés.

De “Tous les serveurs de l'IUT fonctionnent correctement” on ne peut pas en conclure que “SERVEUR3 fonctionne correctement”, même lorsque l'on sait que SERVEUR3 est un serveur de l'IUT.

De “SERVEUR3 est attaqué par un intrus” on ne peut pas conclure qu'“il existe un serveur de l'IUT qui est attaqué par un intrus”, même lorsque l'on sait que SERVEUR3 est un serveur de l'IUT.

2.2.1 Prédicats

On retrouve partout en mathématique, informatique, ou le language courant des énoncés qui comportent des variables non propositionnelles tels que $x > 3$, $x = y + 3$, $x + y = z$, “serveur x est attaqué par un intrus”, “serveur x fonctionne correctement”.

L'énoncé “x est plus grand que 3” comporte :

- la variable x qui est le sujet de l'énoncé.
- la propriété “est plus grand que 3”, qui est une propriété que le sujet de l'énoncé peut avoir.

On peut formaliser “x est plus grand que 3” par $P(x)$ où P dénote “est plus grand que 3”. C'est un *prédicat*. Quand une valeur est attribuée à x, $P(x)$ a une valeur de vérité et devient une proposition.

Un prédicat peut attendre plusieurs variables.

Exercice 32.

- Soit $P(x)$ = “x est plus grand que 3”. Quelles sont les valeurs de vérité de $P(4)$ et $P(2)$?
- Soit $Q(x, y)$ = “x = y + 3”. Quelles sont les valeurs de vérité de $Q(1, 2)$ et $Q(3, 0)$?

Quand un prédicat est *instancié*, c'est-à-dire quand chaque variable a une valeur attribuée, on obtient une proposition avec une valeur de vérité.

Exemple 7. *Une classe d'objets en bases de données peut être capturée par des prédicats, e.g.,* $Personne(insee, nom, prenom)$. *Un objet en particulier est donc un prédicat instancié, e.g.,* $Personne(11992848, Durand, Marie)$

ou $Personne(20194888, Dujol, Oscar)$ *qui sont vrais si l'information correspondante est dans la BD.*

Une classe-association peut être un prédicat, e.g., $Epouse(x, y)$*. Un instantiation donne une relation entre* x *et* y *comme dans* $Epouse(11992848, 20194888)$ *qui est vrai si l'information correspondante est dans la BD.*

Les opérateur propositionnels $\wedge$, $\vee$, $\neg$, ... peuvent donc servir à construire des énoncés complexes.

Exercice 33.

On pose $R(x, y, z) =$ ‘‘$x + y = z''$ et $S(u, v) =$ ‘‘$u < v''$. Quelles sont les valeurs de vérité de :

1. $R(0, 0, 1)$
2. $R(1, 2, 3)$
3. $R(2, 1, 3) \wedge S(2, 6)$
4. $R(0, 0, 1) \vee \neg S(3, 2)$

Exercice 34.

Sur le domaine des humains, on pose $H(x) =$ “x est un homme”, $F(x) =$ “x est une femme”, $R(x) =$ “L'humain x est roux”.
Définir les formes prédicatives de :

1. “x est un homme roux”
2. “x est une femme mais elle n'est pas rousse”

2.2.2 Quantification

Le *domaine* est l'ensemble des valeurs que peuvent prendre les variables de prédicats.

La *quantification universelle* de $P(x)$ est l'énoncé “$P(x)$ pour toute valeur du domaine donnée à x”.

On note $\forall x P(x)$.

On peut lire $\forall x P(x)$ comme “pour tout x $P(x)$ (est vrai)”.

Une valeur de x du domaine pour laquelle $P(x)$ est faux est un *contre-exemple* de $\forall x P(x)$.

Exemple 8. *Soit $P(x) =$ "$x^2 < 10$". Quelle est la valeur de vérité de $\forall x P(x)$ quand le domaine est l'ensemble des entiers positifs inférieurs ou égaux à 5 ?*

$\forall x P(x)$ est la même chose que $P(1) \wedge P(2) \wedge P(3) \wedge P(4) \wedge P(5)$. Donc c'est faux. 4 et 5 sont des contre-exemples.

Exercice 35.

- Soit $P(x) =$ "$x + 8 > x$". Quelle est la valeur de vérité de $\forall x P(x)$ quand le domaine est l'ensemble des nombres réels ?
- Soit $Q(x) =$ "$x < 3$". Quelle est la valeur de vérité de $\forall x Q(x)$ quand le domaine est l'ensemble des nombres réels ? Clairement $Q(3)$ est faux. Tout nombre supérieur ou égal à 3 est un contre exemple de $\forall x Q(x)$.
- Soit $P(x) =$ "$x^2 < 10$". Quelle est la valeur de vérité de $\forall x P(x)$ quand le domaine est l'ensemble des entiers positifs strictement inférieurs à 4 ?

  $\forall x P(x)$ est la même chose que $P(1) \wedge P(2) \wedge P(3)$. Donc c'est vrai.

La *quantification existentielle* de $P(x)$ est l'énoncé "il existe une valeur du domaine qui, lorsque attribuée à x, on a $P(x)$".

On note $\exists x P(x)$.

On peut lire $\exists x P(x)$ comme "il y a (au moins) un x tel que $P(x)$ (est vrai)" ; "pour quelque x, $P(x)$ (est vrai)".

Une valeur de x du domaine pour laquelle $P(x)$ est vrai est un *témoin* de $\exists x P(x)$.

Exemple 9. *Soit $P(x) =$ "$x > 3$". Quelle est la valeur de vérité de $\exists x P(x)$ quand le domaine est l'ensemble des nombres réels ? Le nombre π est un témoin, donc c'est vrai.*

Exercice 36.

- Soit $Q(x) =$ ‘‘$x = x + 1$’’. Quelle est la valeur de vérité de $\exists x P(x)$ quand le domaine est l'ensemble des nombres réels ?
- Soit $P(x) =$ ‘‘$x^2 > 10$’’. Quelle est la valeur de vérité de $\exists x P(x)$ quand le domaine est l'ensemble des entiers positifs strictement inférieurs à 4 ?
- Soit $P(x) =$ ‘‘$x^2 > 10$’’. Quelle est la valeur de vérité de $\exists x P(x)$ quand le domaine est l'ensemble des entiers positifs inférieurs ou égaux à 5 ?

Exercice 37.

On pose $P(x) =$ ‘‘$x < x + 1$’’, et $Z(a) =$ ‘‘$a^2 > 0$’’ : Quelles sont les valeurs de vérité de :

1. $\forall x P(x)$
2. $\forall x (P(x) \wedge Z(x))$
3. $\exists x Z(x)$
4. $\exists x (P(x) \wedge Z(x))$

On peut utiliser le langage ainsi étendu pour définir des prédicats complexes.

Exercice 38.

Sur le domaine des humain. On a $Mariea(x, y) =$ “x est marié(e) à y”. Définir la forme prédicative de “x est célibataire”.

2.2.3 Domaine restraint

Les propriétés dépendent fortement du domaine. Il y a souvent des choses utiles à dire pour une partie du domaine. Par exemple :

- “pour tout x, $x^2 > 0$” n'est pas vrai pour tout entier.

- "pour tout x différent de 0, $x^2 > 0$ est vrai pour tout entier.

Comment faire pour quantifier universellement sur seulement une partie du domaine ? On utilise l' *implication matérielle*.

- "pour tout x, si $x \neq 0$ alors $x^2 > 0$" est vrai pour tout entier.
- $\forall x(x \neq 0 \rightarrow x^2 > 0)$

L'implication matérielle permet donc de spécifier une condition supplémentaire sur le domaine sur lequel on quantifie universellement.

Comment faire pour quantifier existentiellement sur seulement une partie du domaine ? On utilise la conjonction.

- "il y a un entier x inférieur à 0 tel que $x^2 = 4$"
- "il y a un entier x tel que ($x < 0$ et $x^2 = 4$)"
- $\exists x(x < 0 \wedge x^2 = 4)$

La conjonction permet donc de spécifier une condition supplémentaire sur le domaine sur lequel on quantifie existentiellement.

2.2.4 Nier des énoncés quantifiés

L'énoncé "Tout étudiant de cette classe a étudié la logique au lycée" est formalisé par $\forall x L(x)$ où :

- le domaine est l'ensemble des étudiants de cette classe.
- $L(x)$ signifie que l'étudiant x a étudié la logique au lycée.

Si $\forall x L(x)$ n'est pas vrai, alors sa négation doit être vraie. C'est à dire :

- "il n'est pas vrai que tout étudiant de cette classe a étudié la logique au lycée". $\neg\forall x L(x)$
- "il y a un étudiant dans cette classe qui n'a pas étudié la logique au lycée". $\exists x \neg L(x)$

Ca marche dans l'autre sens. L'énoncé "Il existe un étudiant dans cette classe qui a trois yeux" est formalisé par $\exists x Y(x)$. Sa négation est :

- "il n'est pas vrai qu'il existe un étudiant dans cette classe qui a trois yeux". $\neg\exists x Y(x)$

- "pour tout étudiant dans cette classe, il n'est pas vrai qu'il/elle a trois yeux". $\forall x \neg Y(x)$

En général on a pour tout prédicat P à une variable (règles de De Morgan pour les quantificateurs) :

$$\neg \forall x P(x) \equiv \exists x \neg P(x)$$

et

$$\neg \exists x P(x) \equiv \forall x \neg P(x)$$

2.2.5 Quantifications imbriquées

Les formules $\forall x P(x, y)$ et $\exists x P(x, y)$ sont des formes prédicatives avec variable libre x. C.f. Exo 38. Comme telles, ce ne sont pas propositions. On pourrait quantifier sur x.

Exercice 39.

On prend le domaine des humains. Soit le prédicat binaire $A(x, y) =$ "x aime y". Formaliser les énoncés suivants :

1. Tout le monde aime quelqu'un.
2. Tout le monde aime tout le monde.
3. Il y a quelqu'un qui aime tout le monde.
4. Il y a quelqu'un qui n'aime personne.
5. Tout le monde s'aime soit-même.
6. Tout le monde est aimé par quelqu'un.
7. Il n'y a personne qui soit aimé par tout le monde.

La négation d'énoncés se fait avec des quantificateurs imbriqués en appliquant les règles de De Morgan. Comme avant, le résultat peut être rendu plus intuitif en appliquant quelques règles de la logique propositionnelle.

Equivalence logique	Nom
$\neg\forall x P(x) \equiv \exists x \neg P(x)$	De Morgan (DM$\forall$)
$\neg\exists x P(x) \equiv \forall x \neg P(x)$	De Morgan (DM$\exists$)
$\forall x \, \forall y \, P(x,y) \equiv \forall y \, \forall x \, P(x,y)$	Com($\forall$)
$\exists x \, \exists y \, P(x,y) \equiv \exists y \, \exists x \, P(x,y)$	Com($\exists$)
$\forall x \, P(x) \wedge \forall x \, Q(x) \equiv \forall x \, (P(x) \wedge Q(x))$	Dis($\forall - \wedge$)
$\exists x \, P(x) \vee \exists x \, Q(x) \equiv \exists x \, (P(x) \vee Q(x))$	Dis($\exists - \vee$)

Tab. 2.3 : Quelques équivalences logiques.

Exercice 40.

Considérer l'énoncé "Il y a une femme qui a pris un vol de toutes les compagnies aériennes."
On prend le domaine constitué de toutes les femmes, toutes les compagnies aériennes et tous les vols. On pose $Vol(x,y)$ = "x est un vol de la compagnie y" et $Pris(x,y)$ = "la femme x a pris le vol y".

1. Donner une formulation en logique des prédicats.
2. Donner la négation.

2.2.6 Équivalences logiques

Quelques équivalences logiques de la logique des prédicats sont présentées dans la Table 2.3.

2.3 Schémas de raisonnement

2.3.1 Preuves informelles

Généralement en mathématique, les preuves sont destinée à être lues par des humains. On utilise alors des preuves informelles. Dans les preuves informelles, on se permet parfois et souvent d'appliquer plusieurs règles d'inférences à la fois et de ne pas toujours nommer les règles que l'on utilise.

2.3.2 Preuves directes

Une preuve directe qu'un énoncé $A \to B$ est un théorème est identique à prouver que $A \models B$. La preuve informelle est contruite quand :

- on fait l'hypothèse que la proposition A est vraie.
- on utilise des axiomes, définitions et règles d'inférences.
- on arrive au fait que la proposition B est vraie.

Exercice 41.

Définition : Un entier n est *impair* si il existe un entier a tel que $n = 2a + 1$.
Donner une preuve directe de "si n est un entier impair alors n^2 est impair".

Preuve 1. *C'est* $\forall n(P(n) \to Q(n))$ *avec* $P(n)$ = *"n est un entier impair" et* $Q(n)$ = *"n^2 est impair".*
On prend un entier n ***arbitraire*** *et on fait l'hypothèse que* $P(n)$ *est vraie.*
Par définition il existe un entier k tel que $n = 2k+1$. *On veut montrer que* $Q(n)$ *est vraie.*
On a $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$.
On factorise $n^2 = 2(2k^2 + 2k) + 1$.
On pose $K = (2k^2 + 2k)$. *C'est un entier.*
Donc il existe un entier K *tel que* $n^2 = 2K + 1$.
Donc par définition, $Q(x)$.

2.3.3 Preuves par contraposée

Une preuve par contraposée qu'un énoncé $A \to B$ est un théorème utilise l'équivalence logique $A \to B \equiv \neg B \to \neg A$. On peut alors faire une preuve directe de $\neg B \to \neg A$. La preuve informelle est contruite quand :

- on fait l'hypothèse que la proposition B est fausse.
- on utilise des axiomes, définitions et règles d'inférences.
- on arrive au fait que la proposition A est fausse.

Exercice 42.

Définition : Un entier n est un *pair* si il existe un entier a tel que $n = 2a$.
Donner une preuve par contraposée de "si n est un entier et $3n + 2$ est impair, alors n est impair".

Preuve 2. *On prend un entier n* ***arbitraire****. On fait l'hypothèse que n n'est pas impair. C'est à dire que n est pair. Donc, il existe un entier a tel que $n = 2a$.*
On a $3n + 2 = 3(2a) + 2 = 6a + 2 = 2(3a + 1)$.
On pose $A = 3a + 1$. C'est un entier.
Donc il existe un entier A tel que $3n + 2 = 2A$. Donc $3n + 2$ est pair.
Donc il n'est pas impair.

Exercice 43.

Prouver que "si n^2 est impair alors n est impair.".

Preuve 3. *On procède par contraposée. C'est à dire, on prouve "si n est pair alors n^2 est pair".*
On fait l'hypothèse que n est pair. Donc il existe un entier a tel que $n = 2a$. En élevant au carré on a $n^2 = 4a^2 = 2(2a^2)$.
On pose $A = 2a^2$. C'est un entier.
Donc il y a un entier A tel que $n^2 = 2A$. Donc n^2 est pair.

2.3.4 Preuves par contradiction

Un énoncé A est un théorème ssi $t \to A$. En effet, on a la séquence d'équivalences logiques suivante.

1. A
2. $f \vee A$
3. $\neg t \vee A$
4. $t \to A$

Une preuve par contradiction de A est en fait une preuve par contraposée de $t \to A$. Autrement dit, une preuve directe de $\neg A \to f$.

Pour prouver A par contradiction :

- on commence par nier A
- on utilise ensuite des axiomes, définitions et règles d'inférences pour arriver à la contradiction $Q \wedge \neg Q \equiv f$ pour une certaine proposition Q.

Exercice 44.

Définition : un nombre réel n est rationnel si il existe deux entiers a et b avec $b \neq 0$ tels que $n = a/b$. Un nombre réel est irrationnel, sinon.
Prouver que $\sqrt{2}$ est irrationel.

Preuve 4. *Supposons pour contradiction, que y est rationnel. Donc il existe deux entier A et $B \neq 0$ tels que $\sqrt{2} = A/B$. Prenons $a/b = A/B$ la forme réduite, c'est-à-dire que a* ***et*** *b* ***n'ont pas de facteurs communs****. Appelons cette proposition Q.*
Donc $\sqrt{2} = a/b$. On élève au carré : $2 = a^2/b^2$.
On a

$$2b^2 = a^2 \tag{2.1}$$

Donc par définition, a^2 est pair.
Donc, a est pair. (cf. Ex.43) Donc il y a un nombre entier c tel que $a = 2c$.
On substitue dans Eq. 2.1 : $2b^2 = (2c)^2 = 4c^2$.
On a donc $b^2 = 2c^2$. Donc par définition, b^2 est pair.
Donc b est pair. (cf. Ex.43)
Donc $\neg Q$.
On avait déjà Q. Donc on a $Q \wedge \neg Q \equiv f$.

On a prouvé que "si $\sqrt{2}$ est rationnel alors f".
Donc $\sqrt{2}$ est irrationnel.

2.3.5 Preuves d'équivalences

Les preuves d'équivalences permettent de prouver qu'une proposition de la forme $A \leftrightarrow B$ est un théorème. On peut :

- Faire une preuve directe en partant de A et en arrivant à B en utilisant seulement des équivalence logiques.
- ou faire deux preuves (directes, par contraposée, par contradiction, ...) de $A \rightarrow B$ puis de $B \rightarrow A$. Cela repose sur l'équivalence logique $A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$.

C'est aussi comme prouver $A \equiv B$, que l'on peut faire en prouvant $A \models B$ puis $B \models A$.

Exercice 45.

Prouver que "avec n un entier, n est impair ssi n^2 est impair".

Preuve 5. *On a déjà montré gauche-droite par une preuve directe (Ex. 41). On a déjà montré droite-gauche par contraposée (Ex.43).*

2.3.6 Preuves par induction

Le principe d'induction repose sur la formule prédicative évaluée sur le domaine des entiers non négatifs :

$$(P(0) \wedge \forall k(P(k) \rightarrow P(k+1))) \rightarrow (\forall x P(x))$$

De manière équivalente, sur le domaine des entiers $k \geq b$ avec $b \geq 0$:

$$(P(b) \wedge \forall k(P(k) \rightarrow P(k+1))) \rightarrow (\forall x P(x))$$

Pour prouver qu'une proposition $P(x)$ est vraie pour tout x du domaine, il suffit donc d'établir un cas de base $P(b)$ et le pas général d'induction $\forall k(P(k) \rightarrow P(k+1))$.

On peut illustrer le principe d'induction comme une ascension arbitrairement haute sur une échelle. Pour savoir si l'on peut monter arbitrairement haut sur une échelle, c'est-à-dire sur tous les barreaux d'une échelle, il suffit de savoir :

1. que l'on peut monter sur le premier barreau : $P(1)$

2. que en supposant que l'on peut monter sur un barreau arbitrairement haut $P(k)$, on pourrait monter sur l'échelon suivant $P(k+1)$.

Exercice 46.

La somme des n premiers entiers positifs est égale à $n(n+1)/2$.

Preuve 6. *Soit le prédicat $P(x)$ = "la somme des x premiers entiers positifs est égale à $x(x+1)/2$.*
Cas de base : $P(0) = 0 = 0(0+1)/2$
*Hypothèse d'induction : Pour un **arbitraire** $k \geq 0$, supposons que $P(k)$.*
Pas d'induction : On veut prouver $P(k+1)$.
Par H.I., $P(k)$ est vrai. Donc $\Sigma_{i=0}^{k} i = k(k+1)/2$.
La somme des $k+1$ premiers entiers positifs est $\Sigma_{i=0}^{k+1} i = (k+1) + \Sigma_{i=0}^{k} i = (k+1) + \frac{k(k+1)}{2}$.
C'est $(k+1)(1+\frac{k}{2}) = (k+1)\frac{2+k}{2} = (k+1)\frac{(k+1)+1}{2} = \frac{(k+1)((k+1)+1)}{2}$.
Ce qui établit $P(k+1)$ et que $\forall x(P(x) \rightarrow P(x+1))$.

On a donc $P(0) \wedge \forall x(P(x) \rightarrow P(x+1))$. Donc pour tout entier positif n, la proposition $P(n)$ est vraie.

3 Arithmétique : nombres premiers, division euclidienne, congruences

Sur l'arithmétique[1] repose la sécurité de nos communications digitales. L'arithmétique est le fondement théorique et pratique des techniques de chiffrement. (Nombres premiers, clés secrètes, clé publique calculée, algorithme d'Euclide et coefficients de Bézout, cryptage et décodage par l'exponentiation rapide dans l'arithmétique modulaire...)

3.1 Division euclidienne

Soient $a, b \in \mathbb{Z}$. On dit que b *divise* a s'il existe $q \in \mathbb{Z}$ tel que

$$a = bq$$

Si c'est le cas, on écrit :

$$b|a$$

Exemple : Montrons que si $c|b$ et $b|a$ alors $c|a$.

- $c|b$ alors il existe q tel que $b = cq$
- $b|a$ alors il existe k tel que $a = bk$
- donc $a = cqk = cq'$ où $q' = qk$ donc $c|a$.

[1] On emprunte largement du chapitre Arithmétique de Exo7. `http://exo7.emath.fr/cours/ch_arithmetique.pdf`

Exercice 47.

Montrer :

1. si $a|b$ et $a|c$ alors $a|b+c$.
2. si $d|b$ alors $d|bq$.
3. si $d|b+c$ et $d|b$ alors $d|c$.

Théorème 1 (Division Euclidienne)**.** *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$. Il existe des entiers $q, r \in \mathbb{Z}$ tels que*

$$a = bq + r \text{ et } 0 \leq r < b$$

De plus, q et r sont uniques.

Soient $a, b \in \mathbb{Z}$ avec au moins l'un des deux non nul. Le plus grand entier qui divise a et b s'appelle le *plus grand commun diviseur* de a et b. Il se note

$$\mathsf{pgcd}(a, b)$$

Exercice 48.

Montrer que si $a = bq + r$ alors alors $\mathsf{pgcd}(a, b) = \mathsf{pgcd}(b, r)$.

Algorithme d'Euclide. On veut une méthode algorithmique pour calculer $\mathsf{pgcd}(a, b)$. On peut supposer $a \geq b$. On fait des divisions euclidiennes successives, et le pgcd sera le dernier reste non nul.

- division de a par b : $a = bq_1 + r_1$. $\mathsf{pgcd}(a, b) = \mathsf{pgcd}(b, r_1)$. Si $r_1 = 0$, alors $\mathsf{pgcd}(a, b) = b$. Sinon, on continue :
- $b = r_1 q_2 + r_2$. $\mathsf{pgcd}(b, r_1) = \mathsf{pgcd}(r_1, r_2)$.
- ...
- $r_{k-2} = r_{k-1} q_k + r_k$. $\mathsf{pgcd}(r_{k-2}, r_{k-1}) = \mathsf{pgcd}(r_{k-1}, r_k)$.
- $r_{k-1} = r_k q + 0$. $\mathsf{pgcd}(r_{k-1}, r_k) = \mathsf{pgcd}(r_k, 0) = r_k$.

L'algorithme terminera. En effet, à chaque étape, le reste est plus petit que le quotient, donc les restes forment une suite d'entiers positifs décroissante $b > r_1 > r_2 > \ldots \leq 0$.

Exercice 49.

Pour les couples (m, n) suivants déterminer $\mathsf{pgcd}(m, n)$. (Appliquer l'algorithme d'Euclide si besoin.)

1. (18, 6)
2. (14, 6)
3. (121, 11)
4. (600, 124)

Une conséquence de l'algorithme d'Euclide :

Théorème 2 (Théorème de Bézout)**.** *Soit a et b deux entiers. Il existe $u, v \in \mathbb{Z}$ tels que :*

$$au + bv = \mathsf{pgcd}(a, b)$$

Les variables u et v dans le théorème sont appelées des *coefficients de Bézout*. Ces coefficients ne sont pas uniques.

Exercice 50 (Lemme de Gauss)**.**

Prouver le Lemme de Gauss : soit $a, b, c \in \mathbb{Z}$. Si $a|bc$ et $\mathsf{pgcd}(a, b) = 1$ alors $a|c$.

Soient $a, b \in \mathbb{Z}$. Le plus petit entier qui divise a et b s'appelle le *plus petit commun multiple* de a et b. Il se note

$$\mathsf{ppcm}(a, b)$$

Propriété 1. *Soient $a, b \in \mathbb{Z}$ avec au moins l'un des deux non nul.*

$$\mathsf{pgcd}(a, b) \times \mathsf{ppcm}(a, b) = |ab|$$

3.2 Nombres premiers

Un nombre $n \in \mathbb{N}$ est dit *premier* s'il a exactement deux diviseurs positifs distincts, 1 et n.

Exemple 10. 0, 1, 4, 100 *ne sont pas premiers.*
2, 3, 5, 7, 11, 13, ... *sont premiers.*

Exercice 51.

Théorème fondamental de l'arithmétique (Existence). Montrer que tout $n \in \mathbb{N}$ tel que $n \geq 2$ est un produit de nombres premiers.

Exercice 52.

Décomposer en produit de facteurs premiers :

1. 8
2. 64
3. 68

Exercice 53.

Montrer qu'il existe une infinité de nombres premiers. [Indication : pour l'absurde, supposer qu'il existe un nombre premier plus grand que tous les autres.]

Théorème 3. Théorème fondamental de l'arithmétique (Existence et Unicité). *Tout $n \in \mathbb{N}$ tel que $n \geq 2$ admet une décomposition unique en facteurs de nombres premiers.*

3.3 Congruences

Soit $n \geq 1$. On dit que a est *congru* à b *modulo* n, si n divise $b - a$. On note

$$a \equiv b \ (mod\ n)$$

ou

$$a \equiv b[n]$$

Propriété 2. *$n|a$ ssi $a \equiv 0[n]$.*

La valeur de $a[n]$ est l'unique valeur $0 \leq r < n$ telle que $a \equiv b \ (mod\ n)$. C'est-à-dire, le reste de la division Euclidienne de a par n : $a = bq + r$.

Exercice 54.

Montrer :

1. si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a + c \equiv b + d[n]$
2. si $a \equiv b[n]$ et $c \equiv d[n]$ alors $ac \equiv bd[n]$
3. si $a \equiv b[n]$ alors pour $k \geq 0$, $a^k \equiv b^k[n]$
4. $ab[n] \equiv (a[n] \times b[n]) \ (mod\ n)$

Exponentiation rapide. Comment trouver le résultat de $17^{154}[100]$?

Une méthode naïve : on peut laborieusement calculer 17^{154} (le résultat a 190 chiffres !), et trouver le reste de la division Euclidienne par 100.

Sinon, une technique efficace consiste—très schématiquement—à écrire l'exposant en binaire, et décomposer la puissance grâce à elle. Ensuite on calcul chaque puissance composante modulo 100, on les multiplie, en simplifiant au fur et à mesure. On présente la méthode par l'exemple.

Exemple 11. *On calcule $17^{154}[100]$ par exponentiation rapide.*

Ici $154 = 128 + 16 + 8 + 2 = (10011010)_2$.

On va calculer successivement 17^1, 17^2, 17^4, 17^8, 17^{16}, 17^{32}, 17^{64}, 17^{128} *modulo* 100.

- $17^1[100] = 17[100]$
- $17^2[100] = 289[100] = 89[100]$
- $17^4[100] = 17^2 \times 17^2[100] = 89 \times 89[100] = 7921[100] = 21[100]$
- $17^8[100] = 17^4 \times 17^4[100] = 21 \times 21[100] = 441[100] = 41[100]$
- $17^{16}[100] = 17^8 \times 17^8[100] = 44 \times 44[100] = 1681[100] = 81[100]$
- $17^{32}[100] = 17^{16} \times 17^{16}[100] = 81 \times 81[100] = 6561[100] = 61[100]$

- $17^{64}[100] = 17^{32} \times 17^{32}[100] = 61 \times 61[100] = 3721[100] = 21[100]$
- $17^{128}[100] = 17^{64} \times 17^{64}[100] = 21 \times 21[100] = 441[100] = 41[100]$

Maintenant : $17^{154}[100] = 17^{128} \times 17^{16} \times 17^{8} \times 17^{2}[100] = (17^{128}[100] \times 17^{16}[100] \times 17^{8}[100] \times 17^{2}[100])[100] = 41 \times 81 \times 41 \times 89[100] = 3321 \times 3649[100] = 21 \times 49[100] = 1029[100] = 29$.

Exercice 55.

Calculer :

1. $5^{11}[14]$
2. $10^{5}[85]$