MATHEMATICS MEMORY JOGGER

DIDIER WILLAME AND HADRIEN WILLAME

Abstract. Le memory-jogger est organisé autour de définitions et d'exemples présentés de manière aussi claire et concise que possible.

Contents

Date: 14th February 2005.

Introduction

Le memory-jogger présente une liste de fomules et de définitions accompagnées d'exemples et d'un minimum d'explications. Il a pour but d'entretenir les connaissances (*memory jogging*). Ce document ne s'adresse donc pas aux néophytes, mais bien à tous ceux qui ont déjà suivi les cours correspondants. Néanmoins si certains points devaient rester ardus, nous proposons aux lecteurs de reprendre son apprentissage avec de bonnes références, de consulter une bonne encyclopédie[1] ou de trouver de bons matériaux pédagogiques sur internet[2].

Nous tenterons d'utiliser la programmation comme moyen d'expression, et pourquoi pas aussi comme outil de demonstration.

Nous utiliserons autant que faire se peut la notation BNF[3] pour exprimer la syntaxe des structures décrites, et nous emploierons les langages Python[4] et Prolog[5] pour coder les algorithmes.

---

[1] par exemple l'*Encyclopédie Universalis* [2].
[2] par exemple l'*Encyclopédie Wiki* [1].
[3] Backus-Naur Form.
[4] voir le site internet `http://www.python.org`.
[5] vor le site internet `http://www.swi-prolog.org`.

Part 1. La Logique Mathématique

1. La Syntaxe Mathématique

1.1. La Notation BNF.

Avec un ensemble restreint de meta-symboles, la notation BNF permet de définir les règles de production des grammaires informatiques. Les extensions ne seront pas utilisées.

Definition. Les méta-symboles BNF sont :

::=	"est défini comme"
		alternative
<nom>	dénomination des symboles non-terminaux

Example. <expression lambda> ::= lambda <liste des paramètres> : <expression>

1.2. Quelques Définitions.

Quel est l'objet des Mathématiques? Les mathématiciens s'attachent principalement à élaborer des théories relatives à des structures abstraites (e.g. les nombres et les figures géométriques). Ils construisent ainsi des ensembles consistants de formules en utilisant le formalisme et les méthodes de la logique.

Definition. <formule> ::= <propriété> | <calcul>

Les formules permettent d'exprimer tant les aspects structurels (<propriété>) que les aspects fonctionnels (<calcul>) des mathématiques.

Definition. <propriété> ::= <axiome> | <théorème> | <conjecture>

Les propriétés, exprimées sous la forme de propositions et de prédicats, sont soit admises telles quelles (<axiome>[6]), soit dérivées par démonstration (<théorème>[7]), soit à démontrer (<conjecture>).

Definition. <calcul> ::= <égalité> | <expression> | <algorithme>

Les calculs au sens large concernent les transformations des objets mathématiques.

Definition. <égalité>[8] ::= <affectation> | <identité> | <équation>

Le calcul le plus simple consiste en la mise en relation d'objets équivalents.

Definition. <affectation> ::= <variable> = <expression>

L'affectation est l'opération permettant d'assigner le résultat d'un calcul dans une variable.

Example. s = "ceci est une chaîne de caractères!"

Definition. Une identité est une égalité invariante quelque soient les valeurs des variables.

Example. $(a+b)^2 = a^2 + 2ab + b^2$

Definition. Une équation est une égalité qui se réalise pour certaines valeurs des variables.

Example. $x^2 + 1 = 0$, se réalise pour $x \in \{-i, i\}$.

Definition. Une expression est une combinaison de symboles avec des opérateurs en vue d'obtenir un résultat précis.

Example. $1 + 1$, a pour résultat 2.

Example. $lambda\ n\ :\ n * n$, a pour résultat une fonction qui calcule le carré de n.

Example. $(lambda\ n\ :\ n * n)(2)$, a pour résultat 4.

---

[6] ou définition.

[7] ou lemme, proposition, corollaire.

[8] L'opération qui retourne V (vrai) lorsque les 2 membres de l'*égalité* sont identiques et F (faux) sinon, est à considérer comme une expression booléenne et non comme une *égalité* à proprement parlé.

L'évaluation d'une expression se fait en remplaçant les variables par un jeu de données, et en exécutant subséquemment les calculs. L'ordre des calculs est contraint par les parenthèses et est régit par la précédence des opérateurs.

Definition. Un `algorithme` est une suite d'instructions.

Example. Abaque de la division

1	Initialisation (dresser l'abaque et placer le dividende a en haut à gauche et le diviseur b en haut à droite)
2	Déterminer la partie utile de la mantisse de a (digits les plus significatifs formant un nombre a' juste plus grand ou egal à b)
3	Utiliser l'algorithme d'Euclide ($a' = b * q' + r'$) pour calculer le quotient q' de l'étape courante
4	Placer en bas à droite le quotient q' courant, à droite des digits déjà trouvés
5	Calculer le produit $q' * b$ et le placer en-dessous de la partie utile a'
6	Calculer le reste courant r en soustrayant le produit $q' * b$ du dividende a dans la colonne de gauche
7	Arrêt si le reste courant r est nul
8	Arrêt si la séquence des digits quotient se répète (le quotient est un nombre rationnel)
9	Arrêt si le nombre de digits requis après le point décimal est atteint
10	Si le reste courant est plus petit que 0, supprimer le point décimal du reste courant et le placer à droite du quotient courant
11	Aller au point 2

Example. Algorithme itératif de la factorielle

```
def fac(n) :
  res = 1;
  for i in range(1,n+1) :
    res *= i;
  return res;
```

Example. Algorithme récusif du pgcd

```
def pgcd(a,b) :
  if(b==0) :
    return a;
  return pgcd(b, a%b);
```

2. Le Calcul des Propositions

2.1. Quelques Définitions.

Definition. Une proposition est un énoncé déclaratif se référant à l'état des choses ou des événements auquel on peut attribuer la qualification V (vrai) ou F (faux). Une proposition est dite atomique lorsqu'elle n'est pas elle-même décomposable en propositions plus simples, sinon elle est dite moléculaire.

Example. (Socrate est un homme)

Definition. Un raisonnement est une suite finie de propositions liées les unes aux autres selon des principes déterminés et aboutissant à une conclusion. On distingue les raisonnements inductifs ou inductions qui permettent d'obtenir des propositions générales à partir de propositions particulières (ils sont le propre des sciences expérimentales), des raisonnements déductifs ou déductions qui dérivent des conclusions à partir de prémisses (ils sont le propre des sciences mathématiques).

Example. Le raisonnement inductif a pour objet la mise en évidence de "vérités" empiriques. Je sais, de l'avoir déjà vécu, que du gravier laissé dans mon soulier entraine de la douleur. Mais est-ce toujours le cas? Pour répondre à ce genre de question, il faut envisager une batterie de tests dont les résultats devront être interprétés avec la plus grande prudence. Les probabilités conditionnelles avec le théorème de Bayes ($P\{B|A\} = \frac{P\{A|B\}P\{B\}}{P\{A\}}$) et les tests d'hypothèse statistiques sont d'importants outils d'interprétation des résultats expérimentaux.

Example. Le syllogisme est une forme de raisonnement déductif.

(tous les hommes sont mortels)	(majeure, prémisse d'intérêt général)
(tous les grecs sont des hommes)	(mineure, prémisse d'intérêt particulier)
(tous les grecs sont mortels)	(conclusion)

Definition. Un raisonnement est dit valide lorsqu'il ne fait intervenir que des tautologies (i.e. des propositions toujours vraies), sinon il est dit invalide.

Example. Lorsque les prémisses d'un syllogisme concernent un même attribut, alors le syllogisme n'est pas valide.

(tous les singes sont poilus)
(Socrate est poilu)
(Socrate est un singe)

Definition. Une démonstration est un raisonnement déductif valide qui dans le cadre d'une théorie permet de montrer la vérité d'une proposition (la thèse) à partir des prémisses (les hypothèses) acceptées comme vraies (i.e. les axiomes) ou déjà démontrées (i.e. les théorèmes).

Example. Preuve par simple dérivation de la simplification dans un groupe :

$$\begin{array}{rrcll} & x+a & = & y+a & \text{(hypothèse)} \\ \Leftrightarrow & x+a-a & = & y+a-a & \text{(existence d'un symétrique)} \\ \Leftrightarrow & x+(a-a) & = & y+(a-a) & \text{(associativité)} \\ \Leftrightarrow & x+0 & = & y+0 & \text{(existence d'un neutre)} \\ \Leftrightarrow & x & = & y & \text{(thèse)} \end{array}$$

■

Example. Preuve par l'absurde de l'unicité du neutre dans un groupe :

1. Soient 0 et n, 2 neutres différents (négation de l'hypothèse)

2. $$\begin{array}{rrcll} & 0 & = & 0 & \text{(tautologie)} \\ \Leftrightarrow & 0+n & = & 0+n & \text{(simplification à gauche car } n \text{ est neutre)} \\ \Leftrightarrow & 0 & = & 0+n & \text{(simplification à droite car 0 est neutre)} \\ \Leftrightarrow & 0 & = & n & \text{(contradiction)} \end{array}$$

$\Rightarrow$ Le neutre est unique (la thèse)

■

Example. Preuve par récurrence (*proof by induction* en anglais) de $1+3+5+...(2n-1)=n^2$:

1. La base de la récurrence ($n=1$):
   $2n-1=2-1=1$

2. Le corps de la récurrence ($n>1$):

$$\begin{array}{lrcll} & 1+3+5+...(2(n-1)-1) & = & (n-1)^2 & \text{(développement jusqu'à } n-1\text{)} \\ \Leftrightarrow & 1+3+5+...(2n-3) & = & n^2-2n+1 & \text{(développement du carré)} \\ \Leftrightarrow & 1+3+5+...(2n-3)+(2n-1) & = & n^2 & \text{(développement jusqu'à } n\text{)} \end{array}$$

$\Rightarrow$ La formule $1+3+5+...(2n-1)=n^2$ est valide quelque soit n (la thèse)

■

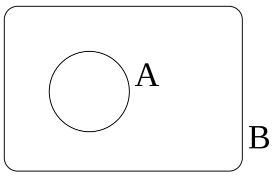
Definition. <proposition conditionnelle> ::= si <prémisses>, alors <conclusions>

Example. (tous les surfers aiment les grandes vagues) $\equiv$ si (vous êtes un surfer), alors (vous aimez les grandes vagues)

Definition.

	p	(vous êtes un surfer)
	q	(vous aimez les grandes vagues)
	$p \supset q$	si (vous êtes un surfer), alors (vous aimez les grandes vagues)
converse	$p \subset q$	si (vous aimez les grandes vagues), alors (vous êtes un surfer)
inverse	$\overline{p} \supset \overline{q}$	si (vous n'êtes pas surfer), alors (vous n'aimez pas les grandes vagues)
contrapositive	$\overline{p} \subset \overline{q}$	si (vous n'aimez pas les grandes vagues), alors (vous n'êtes pas surfer)

2.2. **De la Nécessité et de la Suffisance.**
Soient A et B deux ensembles définis respectivement par les conditions p et q.



$A = B$	$p \equiv q$	p ou q sont des conditions nécessaires et suffisantes pour définir A ou B
$A \subseteq B$	$p \supset q$	il peut exister des éléments de B qui ne réalisent pas la condition p (i.e. qui ne sont pas dans A)
$A \subset B$	$\neg(p \subset q)$	q est une condition nécessaire mais pas suffisante pour définir A (i.e. pas suffisamment restrictive pour définir complètement A) N.B. $\vdash \neg(p \subset q) \equiv (p \supset q) \wedge \neg(p \subset q)$

2.3. **Les Tables de Vérité (Karnaugh).**

p	V	F	
tautologie	V	V	$V, \vdash p$
affirmation	V	F	p
négation (non)	F	V	$\overline{p}$, $\neg\, p$, $\sim p$ (not)
contradiction	F	F	F

p	V	V	F	F		A
q	V	F	V	F		B
affirmation complète	V	V	V	V	$p * q$, $p \top q$	
disjonction (ou inclusif)	V	V	V	F	$p \vee q$, $p + q$ (or)	$A \cup B$
contre-implication (implication converse)	V	V	F	V	$p \subset q$, $p \Leftarrow q$	$A \supseteq B$
	V	V	F	F	p, $p[q]$	
implication	V	F	V	V	$p \supset q$, $p \Rightarrow q$	$A \subseteq B$
	V	F	V	F	q, $q[p]$	
équivalence	V	F	F	V	$p \equiv q$, $p \Leftrightarrow q$ (ssi)	$A = B$
conjonction (et)	V	F	F	F	$p \wedge q$, $p \,.\, q$ (and)	$A \cap B$
incompatibilité	F	V	V	V	$p \mid q$ (nand)	
alternance (ou exclusif)	F	V	V	F	p w q, $p \oplus q$ (xor)	$A \triangle B$
négation de q	F	V	F	V	$\overline{q}$	
négation de l'implication	F	V	F	F	$p \not\Rightarrow q$	$A \supset B$
négation de p	F	F	V	V	$\overline{p}$	
négation de la contre-implication	F	F	V	F	$p \not\Leftarrow q$	$A \subset B$
rejet	F	F	F	V	$p \downarrow q$ (nor)	
négation complète	F	F	F	F	$p \circ q$, $p \perp q$	

2.4. **Quelques Tautologies.**

principe de la double négation	$\vdash \overline{\overline{p}} \equiv p$	
principe du tiers exclu	$\vdash p \vee \overline{p} \equiv V$	
loi de non-contradiction	$\vdash p \mid \overline{p} \equiv V$	
lois de De Morgan	$\vdash p \mid q \equiv \overline{p} \vee \overline{q}$	
	$\vdash p \downarrow q \equiv \overline{p} \wedge \overline{q}$	
règle de la contraposition	$\vdash p \supset q \equiv \overline{p} \subset \overline{q}$	
règle du modus ponens	$\vdash ((p \supset q) \wedge p) \supset q$	$\begin{array}{l} p \Rightarrow q \\ p \\ \hline q \end{array}$
règle du modus tollens	$\vdash ((p \supset q) \wedge \overline{q}) \supset \overline{p}$	$\begin{array}{l} p \Rightarrow q \\ \overline{q} \\ \hline \overline{p} \end{array}$
règle du modus barbara	$\vdash ((p \supset q) \wedge (q \supset r)) \supset (p \supset r)$	$\begin{array}{l} p \Rightarrow q \\ q \Rightarrow r \\ \hline p \Rightarrow r \end{array}$
règle de la distributivité	$\vdash p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	
	$\vdash p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	

3. La Théorie des Ensembles

3.1. **Quelques Définitions.**

Definition. <éléments> ::= | <élément> | <élément>,<éléments>

Une liste d'éléments est constituée soit d'aucun élément, soit d'un seul élément, ou encore de plusieurs éléments.

Definition. Définition en extension :

```
<ensemble en extension> ::= {<éléments>} | {<éléments>...}
```

Example. $\mathbb{N} = \{0, 1, 2...\}$

Algorithm 3.1. *parents = ['mere', 'pere']*

Definition. Définition en compréhension :

```
<ensemble en compréhension> ::=  {<déclaration> : <propriété>} |
                                 {<expression> : <contrainte>}
```

Example. $l'ensemble\,des\,nombres\,premiers\ =\ \{n\ \in\ \mathbb{N}^*\ :\ n\,n'est\,divisible\,que\,par\,2\,nombres\,distincts\}$
$m_{12} = \{12 * k : k \in \mathbb{Z}\}$

Algorithm 3.2. *suivant = [(3*n+1)/2 for n in range(10) if n%2]*[9]

3.2. Ensemble des parties.

$$\forall A\ :\ \wp_A\ =\ \{\ A_i\ :\ Ai\ \subseteq\ A\ \} \tag{3.1}$$

<u>Exemple</u>: $A = \{0, 1\} \Leftrightarrow \wp_A = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$

3.3. Cardinalité.

<u>Exemple</u>: $|\emptyset| = 0$ et $|\{\emptyset\}| = 1$
<u>Exemple</u>: $|\mathbb{N}| = \infty$, $|\mathbb{Z}| = \infty$ et $|\mathbb{R}| = \aleph_1$
<u>Exemple</u>: $|\wp_A| = 2^{|A|}$

4. Les opérations

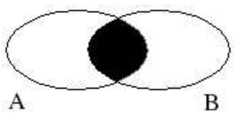
4.1. Le complément $\complement_A$.

$$a \in \complement_A \Leftrightarrow a \notin A \tag{4.1}$$

4.2. L'union $A \cup B$.

$$a \in A \cup B \Leftrightarrow a \in A \vee a \in B \tag{4.2}$$

4.3. L'intersection $A \cap B$.

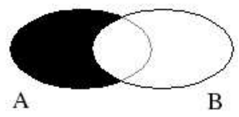


$$a \in A \cap B \Leftrightarrow a \in A \wedge a \in B \tag{4.3}$$

---

[9]la varibale `suivant` contient la liste `[2, 5, 8, 11, 14]`.

4.4. La différence $A \backslash B$.



(4.4) $$a \in A \backslash B \Leftrightarrow a \in A \wedge a \notin B$$

Exemple: $\mathbb{N} \backslash \{0\}$

4.5. La différence symétrique $A \Delta B$.

(4.5) $$a \in A \Delta B \Leftrightarrow a \in A \cup B \wedge a \notin A \cap B$$

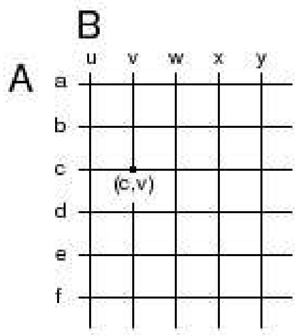
5. Les Relations

5.1. Le produit cartésien.

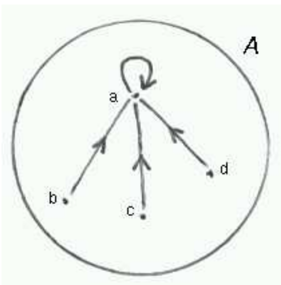
•

(5.1) $$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

Exemple:



- Une ***relation*** R est un sous-ensemble d'un produit cartésien.
  Exemple: $R = \{ \ (a, a), \ (b, a), \ (c, a), \ (d, a) \ \} \ \subset \ A \times A$



- Le ***domaine*** (dom) d'une relation est l'ensemble des points origine.
  Exemple: $dom(R) \ = \ \{a, b, c, d\}$
- L'***image*** (Im) est l'ensemble des points arrivée.
  Exemple: $Im(R) \ = \ \{a\}$

5.2. **Les propriétés des relations de $A \times B$.**

- Relation totale:

$$\forall\, a \in A,\ \exists\, b \in B : (a,b) \in R \Leftrightarrow dom(R) = A \tag{5.2}$$

- Fonction:

$$\forall\, a \in A,\ \forall\, b, b' \in B : (a,b) \in R \wedge (a,b') \in R \Rightarrow b = b' \tag{5.3}$$

- Application (function, map ou mapping en anglais): fonction totale

$$\forall\, a \in A,\ \exists!\, b \in B : (a,b) \in R \tag{5.4}$$

- Relation surjective (onto en anglais):

$$\forall\, b \in B,\ \exists\, a \in A : (a,b) \in R \Leftrightarrow Im(R) = B \tag{5.5}$$

- Relation injective (one to one en anglais):

$$\forall\, a, a' \in A,\ \forall\, b \in B : (a,b) \in R \wedge (a',b) \in R \Rightarrow a = a' \tag{5.6}$$

- Relation bijective:

$$R\ est\ surjective \wedge R\ est\ injective \tag{5.7}$$

5.3. **Les propriétés des relations de $A \times A$ (A^2).**

- Réflexivité:

$$\forall\, a \in A : (a,a) \in R \tag{5.8}$$

- Symétrie:

$$\forall\, (a,b) \in R : (b,a) \in R \tag{5.9}$$

- Transitivité:

$$\forall\, (a,b)\ et\ (b,c) \in R : (a,c) \in R \tag{5.10}$$

5.4. **Quelques relations particulières de $A \times A$ (A^2).**

- Relations d'ordre:

$$R\ est\ une\ relation\ d'ordre \Leftrightarrow R\ est\ antisymétrique\ et\ transitive \tag{5.11}$$

- Relations d'équivalence:

$$R\ est\ une\ relation\ d'équivalence \Leftrightarrow R\ est\ réfexive,\ symétrique\ et\ transitive \tag{5.12}$$

6. Les Systémes Formels

6.0.1. *Définitions* [4].

Definition. $\mathcal{A}$ (alphabet) : ensemble fini de symboles

Example. $\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, -, .\}$

Definition. mot : concaténation de symboles de l'alphabet $\mathcal{A}$

Example. 3.1415 est un mot batit sur l'alphabet $\mathcal{A}$

Definition. $|mot|$: longueur du mot (i.e. le nombre de symboles)

Example. $|3.1415| = 6$

Definition. ϵ : mot de longueur nulle

Example. $|\epsilon| = 0$

Definition. $\mathcal{A}^i$: ensemble des mots de longueur i ($i \geq 0$)

Example. $\mathcal{A}^0 = \{\epsilon\}$ et $\mathcal{A}^1 = \mathcal{A}$

Definition. $\mathcal{A}^*$: ensemble de tous les mots constuits sur l'alphabet $\mathcal{A}$ ($\mathcal{A}^* = \bigcup_{i \geq 0} \mathcal{A}^i$)

Example. $\{0,1\}^* = \{\epsilon, 0, 1, 00, 01, 10, 11, 000...\}$

Definition. $\mathcal{L}$ (langage) : ensemble de mots ($\mathcal{L} \subseteq \mathcal{A}^*$)

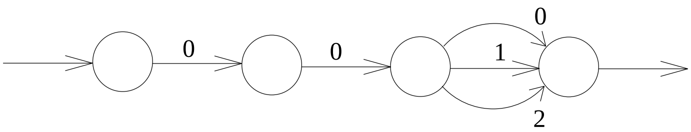
Example. $\{000, 001, 002\}$ est un langage batit sur l'alphabet $\{0, 1, 2\}$

Definition. $\mathcal{G}$ (grammaire) : ensemble des règles de production définissant un langage $\mathcal{L}$

Example. <*mot*>::= 000|001|002 définit tous les mots batis sur $\{0, 1, 2\}$ de 3 symboles et commençant par 00

Definition. $\mathcal{M}$ (machine) : procédure décidant si un mot appartient ou n'appartient pas à un langage $\mathcal{L}$

Example.



Example. `lambda x : (len(x)==3) and (x[0:2]=='00') and (x[2] in ['0','1','2'])`

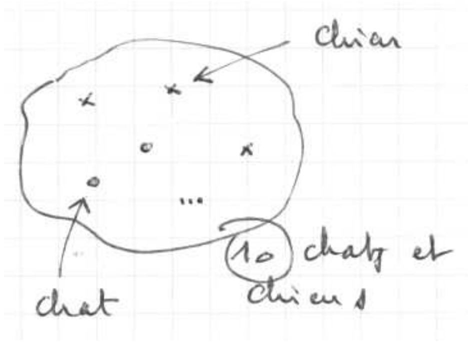
7. Résolution des Problèmes

7.1. Etapes de résolution.

Exemple1: `Il faut 58 biscuits pour nourrir 10 chiens et chats. Combien y a-t-il de chiens et de chats, en sachant qu'un chien mange 6 biscuits et qu'un chat en mange 5?`

7.1.1. *Compréhension du problème.*

Exemple1:



Si x le nombre de chats, le nombre de chiens est alors $10 - x$. $5x$ est ce que mangent les chats et $6(10-x)$ est ce que mangent les chiens.

7.1.2. *Formalisation.*

Exemple1: La solution est donnée par la solution de l'équation suivante

$$5x + 6(10 - x) = 58 \tag{7.1}$$

7.1.3. *Résolution.*

Exemple1:

$$\begin{aligned} 5x + 6(10 - x) &= 58 && (7.2)\\ 5x + 60 - 6x &= 58 && (7.3)\\ -x &= -2 && (7.4)\\ x &= 2 && (7.5) \end{aligned}$$

Le nombre de chats est donc 2 et celui des chiens est 8.

7.1.4. *Vérification.*

Exemple1: 2 chats mangent $5*2$ biscuits et 8 chiens mangent $6*8$ biscuits ce qui donne bien 58 biscuits au total.

Part 2. L'Arithmétique

8. Les nombres négatifs

(8.1) $$\overline{a} = -a = \overline{1} * a$$

9. L'arithmétique des parenthèses

(9.1) $$[(a)] = (a) = a$$

Les parenthèses interveinnent dans l'associativité et la distributivité.
Exemple: $a * (-b) = a * (\overline{1} * b) = a * \overline{1} * b = -a * b$
Exemple: $-(a - b) = \overline{1} * (a + \overline{b}) = (b - a)$

10. La valeur absolue

(10.1) $$|x| = \begin{cases} -x & si\ x < 0 \\ x & si\ x \geq 0 \end{cases}$$

(10.2) $$|a + b| \leq |a| + |b|$$

(10.3) $$|a * b| = |a| * |b|$$

11. La multiplication

(11.1) $$n * x = \underbrace{x + x + \cdots + x}_{nfois}$$

La règle des signes:

(11.2) $$+ * + = +$$
(11.3) $$+ * - = -$$
(11.4) $$- * + = -$$
(11.5) $$- * - = +$$

12. Les puissances

(12.1) $$x^n = \underbrace{x * x * \cdots * x}_{nfois}$$

(12.2) $$(x * y)^m = x^m * y^m$$
(12.3) $$x^m x^n = x^{m+n}$$
(12.4) $$(x^m)^n = x^{m*n}$$

$$x^0 = 1 \tag{12.5}$$

$$x^{-1} = \frac{1}{x} \quad (\forall x \neq 0) \tag{12.6}$$

$$x^{-n} = \frac{1}{x^n} \quad (\forall x \neq 0) \tag{12.7}$$

$$x^{\frac{1}{2}} = \sqrt{x} \tag{12.8}$$

La liste des carrés: $4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400...$
Les puissances de 2: $2, 4, 8, 16, 32, 64, 128, 256, 512, 1024...$

13. Le cas de zéro

$$0^n = 0 \quad (\forall\ n\ >\ 0) \tag{13.1}$$

$$0^0 = ? \quad (0\ ou\ 1\ ?) \tag{13.2}$$

$$0^{-n} = \infty \quad (\ \forall\ n\ >\ 0) \tag{13.3}$$

(13.4)

$$\frac{0}{0} = ? \quad (0\ ou\ \infty\ ?) \tag{13.5}$$

14. Le cas de l'infini

$$\infty \notin \mathbb{Z} \qquad (\infty\ n'est\ pas\ un\ nombre!) \tag{14.1}$$

$$\frac{1}{\infty} = 0 \tag{14.2}$$

$$\infty * \infty = \infty \tag{14.3}$$

$$\frac{\infty}{\infty} = ? \tag{14.4}$$

15. ppcm, pgcd et dénominateur commun

15.1. Les nombres premiers.

Le crible d'Erathostène.

La liste des nombres premiers (p_i): $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97...$

15.2. Factorisation d'un entier.

L'algorithme d'Euclide.

$$\forall\ n \in \mathbb{Z}_{\setminus\{0\}} : n = \prod_{i=1}^{\infty} p_i^{n_i} \tag{15.1}$$

15.3. ppcm (plus petit commun multiple).

$$\forall\ a, b \in \mathbb{Z}_{\setminus\{0\}} : ppcm(a, b) = \prod_{i=1}^{\infty} p_i^{max(n_{a_i}, n_{b_i})} \tag{15.2}$$

<u>Exemple</u>: $ppcm(21, 75) = 2^0 3^1 5^2 7^1 11^0 ... = 525$

15.4. pgcd (plus grand commun diviseur).

$$\forall\ a, b \in \mathbb{Z}_{\setminus\{0\}} : ppcm(a,b) = \prod_{i=1}^{\infty} p_i^{min(n_{a_i}, n_{b_i})} \tag{15.3}$$

Exemple: $pgcd(21,75) = 2^0 3^1 5^0 7^0 11^0 ... = 3$

15.5. Dénominateur commun.

$\forall a, b, c, d \in \mathbb{Z} : \frac{a}{b} + \frac{c}{d} = \frac{a * \frac{ppcm(b,d)}{b} + c * \frac{ppcm(b,d)}{d}}{ppcm(b,d)}$

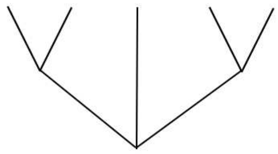
16. La priorité des opérations

16.1. Les expressions arithmétiques et logiques.

(1) $(), [], \{\}, |a|$
(2) a^n
(3) $*, \div$
(4) $\prod, \sum$
(5) $+, -, \pm$
(6) $=, \neq$
(7) $\neg$
(8) $\wedge$
(9) $\vee$
(10) $\Leftrightarrow, \Rightarrow$

Exemple:

`a + n = a = n + a`



Exemple: $2 * (3+5) \neq 2 * 3 + 5$

Exemple:

$$\begin{aligned} 3x + 2 = 0 &\Leftrightarrow 3x = -2 \\ &\Leftrightarrow x = -\tfrac{2}{3} \qquad (-\tfrac{2}{3} \notin \mathbb{Z}) \\ &\Rightarrow Sol = \phi \end{aligned}$$

Exemple: $\sum_{i=0}^{n} a_i x^i = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n$

Exemple:

$$\begin{aligned} \sum_{i=1}^{n} i = \frac{n^2+n}{2} &\Leftrightarrow \sum_{i=1}^{n} i = 1 + 2 + \cdots + (n-1) + n \\ &\Leftrightarrow \sum_{i=1}^{n} i = (1 + n - n) + (2 + n - n) + \cdots + (n-1) + n \\ &\Leftrightarrow \sum_{i=1}^{n} i = n^2 + (1-n) + (2-n) + \cdots - 1 - 0 \\ &\Leftrightarrow \sum_{i=1}^{n} i = n^2 + n - n - (n-1) - (n-2) - \cdots - 1 \\ &\Leftrightarrow \sum_{i=1}^{n} i = n^2 + n - \sum_{i=1}^{n} i \\ &\Leftrightarrow 2\sum_{i=1}^{n} i = n^2 + n \\ &\Leftrightarrow \sum_{i=1}^{n} i = \frac{n^2+n}{2} \end{aligned}$$

Exemple: $a * b = 0 \Leftrightarrow a = 0 \vee b = 0$

16.2. Les prémisses.

(1) $<, \leq, >, \geq, \in$
(2) $\forall, \exists, \exists!$
(3) ,

Exemple: $\forall\ a\ \in\ \mathbb{N},\ \exists!\ n\ \in\ \mathbb{N}$

16.3. Les axiomes, théorèmes, définitions et propriétés.

(1) *pémisses, expressions arithmétiques et logiques*

(2) :

<u>Exemple</u>: $\forall\ a\ \in\ \mathbb{N},\ \exists!\ n\ \in\ \mathbb{N}\ :\ a+n=a=n+a$

Part 3. L'Algèbre

17. Les structures

17.1. Introduction. Une bonne introductions est donnée dans [3].

17.2. Le monoïde $(A, \circ, n)$**.**

$$\text{(17.1)} \quad \textit{interne} \; : \; \forall\, a, b \in A : a \circ b \in A$$
$$\text{(17.2)} \quad \textit{associativité} \; : \; \forall\, a, b, c \in A : (a \circ b) \circ c = a \circ b \circ c = a \circ (b \circ c)$$
$$\text{(17.3)} \quad \textit{neutre unique} \; : \; \forall\, a \in A, \exists!\; n \in A : a \circ n = a = n \circ a$$

Exemples: $(\mathbb{N}, +, 0)$ et $(\mathbb{Z}, *, 1)$

17.3. Le groupe $(A, \circ, n)$**.**

$$\text{(17.4)} \quad (A, \circ, n) \textit{ est un monoïde.}$$
$$\text{(17.5)} \quad \textit{symétrisable} \; : \; \forall a \in A, \exists!\; s \in A : a \circ s = n = s \circ a$$

17.4. Le groupe commutatif $(A, \circ, n)$**.**

$$\text{(17.6)} \quad (A, \circ, n) \textit{ est un groupe.}$$
$$\text{(17.7)} \quad \textit{commutativité} \; : \; \forall a, b \in A : a \circ b = b \circ a$$

Exemples: $(\mathbb{Z}, +, 0)$ et $(\mathbb{Q}_{\setminus\{0\}}, *, 1)$

17.5. L'anneau $(A, +, *, opp, inv)$**.**

$$\text{(17.8)} \quad (A, +, opp) \textit{ est groupe.}$$
$$\text{(17.9)} \quad (A, *, inv) \textit{ est un monoïde.}$$
$$\text{(17.10)} \quad \textit{distributivité} \; : \; \forall a, b, c \in A : a * (b + c) = a * b + a * c$$

Exemple: $(\mathbb{Z}, +, *, 0, 1)$

17.6. Le corps $(A, +, *, opp, inv)$**.**

$$\text{(17.11)} \quad (A, +, opp) \textit{ est groupe.}$$
$$\text{(17.12)} \quad (A_{\setminus\{opp\}}, *, inv) \textit{ est un groupe.}$$
$$\text{(17.13)} \quad \textit{distributivité} \; : \; \forall a, b, c \in A : a * (b + c) = a * b + a * c$$

Exemple: $(\mathbb{Q}, +, *, 0, 1)$

18. Les identités remarquables

$$\text{(18.1)} \quad (a + b)(a - b) = a^2 - b^2$$
$$\text{(18.2)} \quad (a \pm b)^2 = a^2 \pm 2ab + b^2$$
$$\text{(18.3)} \quad (a - 1)(a^n + a^{n-1} + \ldots + a + 1) = a^{n+1} - 1$$

Le triangle de Pascal:

$$\begin{array}{ccccccccc|l}
 & & & & 1 & & & & & (a+b)^0 = 1 \\
 & & & 1 & & 1 & & & & (a+b)^1 = a + b \\
 & & 1 & & 2 & & 1 & & & (a+b)^2 = a^2 + 2ab + b^2 \\
 & 1 & & 3 & & 3 & & 1 & & (a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \\
1 & & 4 & & 6 & & 4 & & 1 & (a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4
\end{array}$$

<u>Remarque</u>: si $b < 0$ (i.e. $(a+\overline{b})^n$) alors les termes où l'exposant de b est impair sont affectés du signe $-$ (e.g. $(a-b)^4 = a^4 - 4a^3b + 6a^2b^2 - 4ab^3 + b^4$).

19. La résolution des équations

19.1. Les principes d'équivalence.

Les principes d'équivalence permettent (1) de simplifier ($\Leftarrow$), et (2) de faire passer des quantités (terme ou facteur) de l'autre côté du signe $=$ ($\Rightarrow$).

Le principe d'addition:

$$\forall a : expr_1 = expr_2 \Leftrightarrow expr_1 + a = expr_2 + a \tag{19.1}$$

Le principe de multiplication:

$$\forall a \neq 0 : expr_1 = expr_2 \Leftrightarrow expr_1 * a = expr_2 * a \tag{19.2}$$

19.2. Le principe de disjonction.

$$(x-a)(x-b)\ ...=0 \Leftrightarrow x = a \vee x = b\ ... \tag{19.3}$$

19.3. Les équations singulières dans $\mathbb{Z}$.

- Les équations impossibles ($sol = \phi$):

  cas 1:

$$0 * x = a \qquad (\forall a \neq 0) \tag{19.4}$$

cas 2:

$$x \notin \mathbb{Z} \tag{19.5}$$

- Les équations indéfinies ($sol = \mathbb{Z}$):

  cas 1:

$$0 * x = 0 \tag{19.6}$$

cas 2:

$$x = x \tag{19.7}$$

19.4. Cas particuliers.

$$|x| = \overline{|x|} \Leftrightarrow sol = \{0\} \tag{19.8}$$

Part 4. La Géométrie

Part 5. La Topologie

References

1. *Wikipédia, l'encyclopédie gratuite et libre*, Internet, http://fr.wikipedia.org/wiki/Accueil.
2. *L'encyclopaedia universalis*, Encyclopaedia Universalis, Paris, France, 2002.
3. Joseph A. Gallian, *Contemporary abstract algebra*, third ed., D. C. Heath and Company, Lexington, Massachusetts, 1994.
4. Allen B. Tucker (ed.), *The computer science and engineering handbook*, first ed., CRC Press, Boca Raton, Florida, 1997.