Fondement des mathématiques

Cédric Milliet

Version préliminaire

Cours de première année de licence

Université Galatasaray

Année 2011-2012

Ces notes de cours doivent beaucoup au cours du même nom de Marie-Christime Pérouème.

Chapitre 1

Introduction : un peu de logique

Avant d'apprendre la poésie, il faut connaître la grammaire et l'orthographe de la langue. De la même manière, on peut voir la logique comme une grammaire des mathématiques. Les phrases en sont les énoncés, et peuvent être connectées entre elles, ou quantifiées pour former d'autres phrases.

1.1 Enoncés, équivalence logique

Définition 1 (*énoncé*)

*Un **énoncé** est une phrase dont on peut dire si elle est vraie ou fausse sans ambiguïté (dans un contexte donné).*

Exemple. "$10 < 100$", "$1 = 2$", "10 est un entier pair", "$100 < 10$" sont tous des énoncés. "$x^2 = x$" aussi. Mais "$1 + 2 + 3 + \cdots + n$" n'est pas un énoncé.

Définition 2 (*implication*)

*A et B sont deux énoncés. On dit que A **implique** B si B est vrai dès que A est vrai. On note $A \implies B$.*

Exemple. $(x = 1) \implies (x^2 = 1)$.

Définition 3 (*équivalence logique*)

*Deux énoncés A et B sont **équivalents** si A implique B et B implique A. On note alors $A \iff B$ et on dit que "A est équivalent à B", on encore que "A est vrai si et seulement si B l'est".*

Exemple. Si a et b sont deux nombres réels, on a les équivalences suivantes :

$$(a^2 = b^2) \iff (a^2 - b^2 = 0) \iff (a - b)(a + b) = 0 \iff (a = b \text{ ou } a = -b)$$

Nota bene. Les symboles $\implies$ et $\iff$ relient deux **énoncés**, et seulement deux énoncés. Ne pas écrire n'importe quoi. La suite de symboles "$2^2 \implies 4$" ne veut rien dire.

Nota bene. A, B et C sont des énoncés. L'énoncé A implique toujours A. Si A implique B et B implique C, alors A implique C. En particulier, si A et B sont équivalents, et si B et C sont équivalents, alors A et C sont équivalents.

1.2 Opérations sur les énoncés

Dans la suite, A et B sont des énoncés.

Définition 4 (*négation*)

*La **négation** de A est un énoncé qui est vraie si et seulement si A est faux. On le note $non(A)$.*

Nota bene. On $nonnon(non(A))$ est toujours équivalenet à A.

Définition 5 (*conjonction*)

*La **conjonction** de A et B est l'énoncé $AetB$ est vrai si et seulement si A est vrai et B est vrai. On la note $AetB$.*

Définition 6 (*disjonction*)

*La **disjonction** de A et B est l'énoncé noté $AouB$ qui est vrai si et seulement si A est vrai ou B est vrai. On la note $AouB$*

On résume souvent par des "tables de vérités" qui indiquent la valeur (vrai ou faux) que peut prendre l'énoncé en fonction des valeurs de A et B. Le 1 est associé à "vrai" et le 0 à "faux".

A	non(A)	non(non(A))
0	1	0
1	0	1

A et B		A	
		0	1
B	0	0	0
	1	0	1

A ou B		A	
		0	1
B	0	0	1
	1	1	1

Proposition 7

A, B et C sont trois énoncés. Les équivalences suivantes sont toujours vraies.

1. $non(AetB) \iff non(A)ounon(B)$
2. $non(AouB) \iff non(A)etnon(B)$
3. $Aet(BetC) \iff (AetB)etC$ *(associativité du "et" logique)*
4. $Aou(BouC) \iff (AouB)ouC$ *(associativité du "ou" logique)*
5. $Aet(BouC) \iff (AetB)ou(AetC)$ *(distributivité de "et" sur "ou")*
6. $Aou(BetC) \iff (AouB)et(AouC)$ *(distributivité de "ou" sur "et")*

Démonstration : 4 ou 8 cas à vérifier. ■

Définition 8 (*contraposée d'une implication*)

*On appelle **contraposée** de l'impliquation $A \implies B$ l'impliquation $non(B) \implies non(A)$.*

Proposition 9

Une implication est toujours équivalente à sa contraposée.

Démonstration : On utilise les règles de la propostion 7 :

$$(A \implies B) \iff (Bou(nonA)) \iff (non(nonB))ou(nonA) \iff ((nonB) \implies (nonA))$$

■

Définition 10 (*réciproque d'une implication*)

*On appelle **réciproque de l'implication** $(A \implies B)$, l'implication $(B \implies A)$.*

Nota bene. Une implication n'est en général pas équivalente à sa réciproque. Prendre par exemple l'implication $x = 1 \implies x^2 = 1$. Sa réciproque est fausse.

1.3 Quantificateurs

Définition 11 (*variable, pour tout, il existe*)

*Il arrive souvent qu'un énoncé dépende d'un objet x (ou de plusieurs $x, y, \dots$) qui peut varier dans un ensemble E fixé. Par exemple $x^2 + x - 1 = 0$ où x est un réel. On note alors $A(x)$ cet énoncé, et on appelle x une **variable**. On définit alors deux nouveaux énonés $(\forall \mathbf{x} \in \mathbf{E})\mathbf{A}(\mathbf{x})$ et $(\exists \mathbf{x} \in \mathbf{E})\mathbf{A}(\mathbf{x})$ par :*

$(\forall x \in E)A(x)$ si et seulement si "pour tout x dans E, $A(x)$ est vraie".

$(\exists x \in E)A(x)$ si et seulement si "il existe un x dans E, tel que $A(x)$ soit vraie".

Remarque. Les symboles $\forall$ et $\exists$ sont de vieilles conventions typographiques. Le premier est un "A" à l'envers venant du A de l'anglais "for All" (pour tout), et le second un "E" à l'envers, provenant du E de "there Exists" (il existe).

Exemple. Avec $x^2 = x$, on peut former les énoncers $(\forall x \in \{0, 1\})(x^2 = x)$, $(\exists x \in \mathbb{R})(x^2 = x)$.

Nota bene. Si l'énoncé A dépend de plusiseurs variables, on peut avoir plusieurs quanitificateurs :

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 0)$$

Attention. L'ordre des quantificateurs est **très** important.

Proposition 12 (*négation des quatificateurs*)

Les équivalences suivantes sont toujours vraies.

$$non((\forall x \in E)(A(x))) \iff ((\exists x \in E)(nonA(x)))$$
$$non((\exists x \in E)(A(x))) \iff ((\forall x \in E)(nonA(x)))$$

Exemples. donner la négation des énoncés suivants : $(\forall x \in \mathbb{R})(x = 1)$, $(\forall x \in \mathbb{N})(x$ est soit pair, soit impair), $(\exists x \in \mathbb{Z})(x = 0)$, $(\forall x \in \mathbb{R}^+)(\exists z \in \mathbb{R}^+)(x = z^2)$.

Chapitre 2

Ensembles

Les objets fondamentaux des mathématiques sont les ensembles.

2.1 Définition

Définition 13 (*ensemble*)

On dit que E est un ***ensemble*** *si pour tout objet x, on peut répondre par oui ou non à la question "x est-il un élément de E ?". On dit que deux ensembles sont* ***égaux*** *si ils ont les mêmes éléments.*

Si x est un élément de E, on le note par $x \in E$ et on dit que x **appartient** à E. Dans le cas contraire, on dit que x n'appartient pas à E, et on note $x \notin E$. Si E est composée des éléments a, b, et c, on note $E = \{a, b, c\}$.

Exemples fondamentaux.

1. $\{0, 1, 2, 3, \ldots\}$ est l'ensemble des entiers naturels. On le note $\mathbb{N}$.
2. $\{0, 1, -1, 2, -2, 3, -3, \ldots\}$ est l'ensemble des entiers relatifs. On le note $\mathbb{Z}$ (comme "Zahlen" qui veut dire "nombres" en allemand).
3. $\mathbb{R}$ est l'ensemble des nombres réels.

Le plus souvent, un ensemble F est défini comme l'ensemble des éléments d'un ensemble E connu pour lesquels un énoncé $A(x)$ est vraie. On a alors :

$$x \in F \iff x \in E \text{ et } A(x)$$

On note $F = \{x \in E \ : \ A(x)\}$ pour dire que F est l'ensemble des éléments x de E pour lesquels $A(x)$ est vraie.

Exemples.

1. Si on note $2\mathbb{Z}$ l'ensemble des entiers relatifs pairs, on a :

   $$n \in 2\mathbb{Z} \iff (\exists k \in \mathbb{Z})(n = 2k)$$

   On note donc $2\mathbb{Z} = \{n \in \mathbb{Z} \ : (\exists k \in \mathbb{Z}) \ n = 2k\}$
2. $\{p/q : (p, q) \in \mathbb{N}^2 \text{ et } q \neq 0\}$ est l'ensemble des rationnels, noté $\mathbb{Q}$ (comme quotient).
3. $\{a + ib : (a, b) \in \mathbb{R}^2\}$ est l'ensemble des nombres complexes, noté $\mathbb{C}$.
4. On note $\mathbb{R}^+$ l'ensemble $\{x \in \mathbb{R} : x \geq 0\}$
5. On note $\mathbb{R}^*$ l'ensemble $\{x \in \mathbb{R} \ : \ x \neq 0\}$. Plus généralement, si E est ensemble dans $\mathbb{C}$, on note E^* l'ensemble $\{x \in E : x \neq 0\}$.

2.2 Parties d'un ensemble

Définition 14 (*partie d'un ensemble*)

A et E sont deux ensembles. On dit que l'ensemble A est une ***partie*** *de l'ensemble E, ou un* ***sous-ensemble*** *de E si tous les éléments de A sont aussi des éléments de E.*

On dit aussi que A **est inclus dans** E. On note alors $A \subset E$. On a donc :

$$A \subset E \iff (\forall x \in A)(x \in E)$$

L'**inclusion** $\subset$ est une relation binaire entre parties de E (on définira plus tard ce qu'est une relation binaire). Elle a les propriétés suivantes :

Proposition 15

A, B et C sont trois ensembles

1. *A est toujours inclus dans A. (on dit que $\subset$ est **réflexive**)*
2. *Si A est inclus dans B et B est inclus dans A, alors A est égal à B. (on dit que $\subset$ est **antisymétrique**)*
3. *Si A est inclus dans B et B est inclus dans C, alors A est inclus dans C. (on dit que $\subset$ est **transitive**)*

On note $P(E)$ l'ensemble de toutes les parties de E. On a ainsi :

$$(A \in P(E)) \iff (A \subset E)$$

Exemples. Déterminer $P(E)$ dans chacun des cas suivants.

1. $E = \emptyset$ (on note aussi $E = \{\}$).
2. $E = \{x\}$
3. $E = \{1, 2\}$
4. $E = \{1, 2, 3\}$

2.2.1 Réunion de deux parties

Définition 16 (*réunion*)

*Soient A et B deux parties d'un ensemble E. On définit la **réunion** de A et B, notée $A \cup B$ par :*

$$x \in A \cup B \iff (x \in A) \text{ ou } (x \in B)$$

On a donc

$$A \cup B = \{x \in E \ : \ (x \in A) \text{ ou } (x \in B)\}$$

La réunion $\cup$ est associée au "ou" logique. C'est une application : $P(E) \times P(E) \to P(E)$ qui à un couple (A, B) associe l'ensemble $A \cup B$. Plus précisément, c'est une **loi de composition interne** (lci). Elle a les propriétés suivantes :

Proposition 17

Pour toutes parties A, B, C d'un ensemble E, on a toujours :

1. *$(A \cup B) \cup C = A \cup (B \cup C)$ (on dit que $\cup$ est **associative**)*
2. *$A \cup B = B \cup A$ (on dit que $\cup$ est **commutative**)*
3. *$\emptyset \cup A = A \cup \emptyset = A$ (on dit que $\cup$ a un **élément neutre** : $\emptyset$)*

2.2.2 Intersection de deux parties

Définition 18 (*intersection*)

*Soient A et B deux parties d'un ensemble E. On définit leur **intersection** $A \cap B$ par :*

$$x \in A \cap B \iff x \in A \text{ et } x \in B$$

On a donc

$$A \cap B = \{x \in E \ : \ x \in A \text{ et } x \in B\}$$

L'intersection $\cap$ est associée au "et" logique. C'est une loi de composition interne : $P(E) \times P(E) \to P(E), (A, B) \mapsto A \cap B$, qui a les propriétés suivantes :

Proposition 19

Pour tout $A, B, C \in P(E)^3$, on a :

1. *$(A \cap B) \cap C = A \cap (B \cap C)$ ($\cap$ est associative)*
2. *$(A \cap B = B \cap A)$ ($\cap$ est commutative)*
3. *$E \cap A = A \cap E = A$ ($\cap$ a un élément neutre qui est E)*

Proposition 20 (*Lois de Morgan*)

Pour toute parties A, B, C de E, on a les égalités :

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(on dit que $\cap$ est* ***distributive*** *sur $\cup$)*
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(on dit que $\cup$ est* ***distributive*** *sur $\cap$)*

Démonstration :

2.2.3 Complémentaire d'une partie

Définition 21 (*complémentaire*)

Soit A une partie de E. On définit le ***complémentaire*** *de A dans E par $\{x \in E \ : \ x \notin A\}$.*

On note $E \setminus A$ cet ensemble, ou encore $A^{\complement}$ si l'ensemble E est implicite et évident. Le complémentaire est une application $P(E) \to P(E), A \mapsto E \setminus A$ qui a les propriétés suivantes :

Proposition 22

Pour toutes parties A et B de E, on a toujours :

1. $(A^{\complement})^{\complement} = A$ *(on dit que l'application complémentaire est* ***involutive****).*
2. $A \subset B \iff B^{\complement} \subset A^{\complement}$ *(elle est "décroissante")*
3. $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$
4. $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$
5. $A \subset B^{\complement} \iff A \cap B = \emptyset$
6. $A^{\complement} \subset B \iff A \cup B = E$

Démonstration :

Nota bene. Si A et B sont deux parties d'un ensemble E, on note souvent $A \setminus B$ pour $A \cap B^{\complement}$, et $A \Delta B$ pour $(A \cup B) \setminus (A \cap B)$.

2.2.4 Fonction caractéristique d'une partie

Définition 23 (*fonction caractéristique*)

Soit E un ensemble et A une partie de E fixée. On définit la ***fonction caractéristique*** *ϕ_A de A par :*

$$\begin{array}{rcl} \phi_A : E & \to & \{0,1\} \\ x & \mapsto & 1 \textit{ si } x \in A \\ & & \textit{ou } 0 \textit{ si } x \notin A \end{array}$$

Puisqu'un ensemble est déterminé uniquement par ses éléments, on a :

Proposition 24

Si A et B sont deux parties de E, on a toujours :

$$(\phi_A = \phi_B) \iff (A = B)$$

La fonction caractéristique a les propriétés suivantes :

Proposition 25

Soit A et B deux parties de E et si x est un élément de E, on a toujours :

1. $(\phi_A(x))^2 = \phi_A(x)$
2. $\phi_{A \cap B}(x) = \phi_A(x) \cdot \phi_B(x)$
3. $\phi_{A^{\complement}}(x) = 1 - \phi_A(x)$
4. $\phi_{A \cup B}(x) = \phi_A(x) + \phi_B(x) - \phi_A(x) \cdot \phi_B(x)$
5. $\phi_{A \setminus B}(x) = \phi_A(x) \cdot (1 - \phi_B(x))$

Démonstration :

Exercice 1. Calculer $\phi_{A \Delta B}(x)$ en fonction de $\phi_A(x)$ et $\phi_B(x)$.

2.3 Produit cartésien

Définition 26 (*produit cartésien*)

Soient E et F deux ensembles. On appelle ***produit cartésien*** *de E et F l'ensemble de tous les couples (x, y) formés avec un élément x de E et y de F. On le note $E \times F$. On a donc*

$$E \times F = \{(x, y) \ : \ x \in E, \ y \in F\}$$

Nota bene. L'égalité $(x, y) = (a, b)$ est vraie si et seulement si $x = a$ et $y = b$.

Nota bene. Ne pas confondre le couple (x, y) avec l'ensemble $\{x, y\}$. Si x est différent de y, alors (x, y) est différent de (y, x)., mais on a toujours $\{x, y\} = \{y, x\}$.

Chapitre 3

Applications

3.1 Définitions

Pour définir une application, il faut se donner trois choses :

1. Un ensemble de départ E,
2. un ensemble d'arrivée F,
3. une façon d'associer à **tout** élément x de E un **unique** élément $f(x)$ de F.

Pour signifier que pour tout x de E, $f(x)$ appartient à F, on note alors : $\begin{array}{rcl} f : E & \to & F \\ x & \mapsto & f(x) \end{array}$

Notation. On note $F(E,F)$, ou F^E l'ensemble de toutes les applications de E dans F.

Vocabulaire. Soit x un élément de E et y un élément de F. Si $y = f(x)$ on dit que "y est **l'image** de x" ,et que "x est **un antécédent** de y".

Nota bene. Deux applications f et g sont égales si et seulement si elles ont même ensemble de départ E, même ensemble d'arrivée F, et si tout élément de E a même image par f et par g.

Définition 27 (*graphe*)

*Le **graphe** de l'application $f : E \to F$ est la partie Γ_f du produit cartésien $E \times F$ définie par*

$$\Gamma_f = \{(x,y) \in E \times F \ : \ f(x) = y\}$$

Exemple. Graphe de $\mathbb{R} \to \mathbb{R}, x \mapsto x^2$

3.2 Image directe, image réciproque

Soient E et F deux ensembles, $f : E \to F$ une application, A une partie de E et B une partie de F.

Définition 28 (*image directe*)

*L'**image** de A par f est l'ensemble des images de tous les éléments de A. On la note $f(A)$. On a donc :*

$$y \in f(A) \iff (\exists A \in A)(f(x) = y) \iff y \text{ a un antécédent dans } A$$

Exemples.
1. Si $f : \mathbb{R} \to \mathbb{R}, x \mapsto cos(x)$, on a $f(\mathbb{R}) = [-1,1]$.
2. Si $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, alors $f(\mathbb{R}) = [0, +\infty[$.

Définition 29 (*image réciproque*)

*L'**image réciproque** de B est l'ensemble de tous les antécédents des éléments de B. On la note $f^{-1}(B)$. On a donc :*

$$x \in f^{-1}(B) \iff f(x) \in B \iff \text{l'image de } x \text{ est dans } B$$

Exemples.
1. Si $f : \mathbb{R} \to \mathbb{R}, x \mapsto cos(x)$, on a $f^{-1}(\{0\}) = \{\pi/2 + k\pi \ : \ k \in \mathbb{Z}\}$.
2. Si $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, alors $f^{-1}(]-\infty, 0[) = \emptyset$.

En résumé :

$$\boxed{f(A) = \{y \in F \ : \ \exists x \in A, \ f(x) = y\} = \{f(x) \ : \ x \in A\}}$$

$$\boxed{f^{-1}(B) = \{x \in E \ : \ f(x) \in B\}}$$

Proposition 30

Les inclusions suivantes sont toujours vérifiées :

1. $A \subset f^{-1}(f(A))$
2. $f(f^{-1}(B)) \subset B$

Démonstration :

3.3 Injection, surjection et bijection

Soient E et F deux ensembles et $f : E \to F$ une application.

Définition 31 (*application injective*)

*On dit que f est **injective** si tout élément de F a au plus un antécédent i.e. si,*

$$(\forall (x, x) \in E^2)(f(x) = f(x') \implies x = x')$$

Nota bene. En prenant la contraposée, f est injective ssi pour tout x et x' de E, on a $x \neq x' \implies f(x) \neq f(x')$.

Exemple. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ n'est pas injective, mais $f : \mathbb{R}^+ \to \mathbb{R}, x \mapsto x^2$ l'est.

Définition 32 (*application surjective*)

*On dit que f est **surjective** si tout élément de F a au plus un antécédent, i.e. si*

$$(\forall y \in F)(\exists x \in E)(y = f(x))$$

Nota bene. Autrement dit, $f : E \to F$ est surjective ssi $f(E) = F$.

Définition 33 (*application bijective*)

*On dit que f est **bijective** si elle est à la fois injective et surjective, i.e. si tout élément de F a exactement un antécédent.*

Exercice 2.
1. f n'est pas injective ssi
2. f n'est pas surjective ssi

Proposition-Définition 34 (*bijection réciproque*)

Si $f : E \to F$ est bijective, alors il existe une unique application notée $f^{-1} : F \to E$ qui vérifie les deux propriétés :

$$(\forall x \in E) \ f^{-1}(f(x)) = x$$

$$(\forall y \in F) \ f(f^{-1}(y)) = y$$

*f^{-1} est aussi bijective. On l'appelle la **bijection réciproque** de f.*

Démonstration : Existence, unicité.

Définition 35 (*restriction*)

*Soit $f : E \to F$, et A une partie de E. On appelle **restriction** de f à A l'application $A \to F, x \mapsto f(x)$. On la note $f|_A$.*

3.4 Cas où f est une application de $\mathbb{R}$ dans $\mathbb{R}$

Soit $f : \mathbb{R} \to \mathbb{R}$ une application. On note Γ_f sont graphe. On peut facilement voir sur le graphe de f si f est injective, surjective ou bijective : pour trouver les antécédents d'un élément y de $\mathbb{R}$, on commence par placer le point $M(0, y)$ sur le graphe, et on trace la droite D_M parallèle à l'axe des abscisses (Ox) passant par M. On regarde ensuite l'intersection $\Gamma_f \cap D_M$, qui est constituée de points de la forme (x, y) avec $y = f(x)$.On en déduit que l'application f est :

- *injective* ssi toute horizontale coupe Γ_f en au plus un point.
- *surjective* ssi toute horizontale coupe Γ_f en au moins un point.
- *bijective* ssi toute horizontale coupe Γ_f en exactement un point.

3.5 Composition des applications

Exemple. Pour quelles valeurs de x peut-on définir le nombre $ln(\cos x)$?

$$\cos x > 0 \iff x \in]-\frac{\pi}{2}, \frac{\pi}{2}[+2k\pi \ (k \in \mathbb{Z})$$

$$\cos :]-\frac{\pi}{2}, \frac{\pi}{2}[\to \mathbb{R}^{+*} \qquad ln : \mathbb{R}^{+*} \to \mathbb{R}$$

Définition 36 (*composition*)

*Plus généralement, si $f : E \to F$ et $g : F \to G$ sont deux applications, on peut définir la **composée** $g \circ f$ de f et g, en posant $g \circ f(x) = g(f(x))$ pour tout x de E.*

$$E \xrightarrow{f} F \xrightarrow{g} G$$

$$\begin{array}{rccc} g \circ f : & E & \to & G \\ & x & \mapsto & g(f(x)) \end{array}$$

Si on connaît des propriétés de deux fonctions, on peut en déduire des propriétés de leur composée :

Proposition 37

1. *La composée de deux injections est injective.*
2. *La composée de deux surjections est surjective.*
3. *La composée de deux bijections est bijective.*

Démonstration :

Inversement, certaines propriétés de $g \circ f$ permettent de déduire des propriétés de f et g :

Proposition 38

1. *Si $g \circ f$ est injective, alors f est injective.*
2. *Si $g \circ f$ est surjective, alors g est surjective.*

Démonstration :

3.6 Applications réciproques

Si E est un ensemble, on note Id_E l'application dite identité dans E qui à un x de E associe x. On peut maintenant reformuler la proposition 34.

Théorème 39

Si $f : E \to F$ est une application bijective, alors il existe une unique application notée $g : F \to E$ qui vérifie les deux propriétés :

$$g \circ f = Id_E$$

$$f \circ g = Id_F$$

*On note $g = f^{-1}$. Cette application est bijective. On l'appelle la **bijection réciproque** de f.*

3.6.1 Cas des fonctions de $\mathbb{R}$ dans $\mathbb{R}$

Proposition 40

A et B sont deux parties de $\mathbb{R}$ et $f : A \to B$ est une application bijective. Le graphe de f^{-1} est le symétrique du graphe de f par la première bissectrice (ie la droite d'équation $y = x$).

Démonstration :

Exemple. Construction de $\sqrt{\ }$ à partir de la fonction carrée, et de exp à patir de ln. Construction de $arccos$ et $arcsin$.

Chapitre 4

Relations binaires

4.1 Définitions

E est un ensemble.

Définition 41 (*relation binaire*)

Une ***relation binaire*** *sur E (ou entre éléments de E) est une application R de $E \times E$ dans un ensemble à deux éléments souvent noté $\{0,1\}$ ou bien $\{faux,\ vrai\}$.*

Si a et b sont deux éléments de E, on note souvent aRb à la place de $R(a,b) = 1$ pour dire que a est en relation avec B. Dans le cas contraire, ie si $R(a,b) = 0$, on note $a \not R b$.

Exemples. Si l'on prend pour E l'ensemble $\mathbb{Z}$, les relations $x = y$, $x \neq y$, x divise y, $x \leq y$, $|x| = |y|$, $x^3 = y$, x et y ont la même parité, sont toutes des relations binaires sur $\mathbb{Z}$.

Définition 42 (*propriétés des relations binaires*)

R est une relation binaire sur E. On dit que R est

1. ***réflexive*** *si $(\forall a \in E)(aRa)$*
2. ***symétrique*** *si $(\forall a \in E)(\forall b \in E)(aRb \implies bRa)$*
3. ***antisymétrique*** *si $(\forall a \in E)(\forall b \in E)(aRb \text{ et } bRa \implies a = b)$*
4. ***transitive*** *si $(\forall a \in E)(\forall b \in E)(\forall c \in E)(aRb \text{ et } bRc \implies aRc)$*

Exemples. Etudier les propriétés des relations dans l'exemple précédent.

4.2 Relations d'ordre

E est un ensemble, R une relation binaire sur E.

Définition 43 (*relation d'ordre*)

On dit que R est une ***relation d'ordre*** *sur E si elle est réflexive, antisymétrique et transitive.*

On dit d'un ensemble muni d'une relation d'ordre que c'est un **ensemble ordonné**.

Exemples. :

1. $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{R}, \leq)$ sont des ensembles ordonnés :
2. $(\mathbb{N}, /)$ est un ensemble ordonné (on note a/b si a divise b, i.e. s'il existe un entier n tel que $a = n.b$) :
3. $(P(E), \subset)$ est un ensemble ordonné

4.2.1 Ordre totale, ordre partiel

Définition 44 (*ordre total, partiel*)

Une relation d'ordre R sur E est ***totale*** *si elle vérifie*

$$(\forall (x,y) \in E^2)(xRy \text{ ou } yRx)$$

On dit dans ce cas que E est un ensemble ***totalement ordonné****. On dit que R est une relation d'ordre*

partielle *si elle n'est pas totale, c'est-à-dire si elle vérifie*

$$(\exists (x,y) \in E^2)(non(xRy) \text{ et } non(yRx))$$

On dit alors que E est ***partiellement ordonné****.*

Exemples.

Nota bene. Une relation d'ordre R est totale si deux éléments sont toujours ordonnés par R. Elle est partielle s'il existe deux éléments qui ne sont pas comparables.

4.2.2 Partie majorée, minorée

Définition 45 (*majorant, minorant*)

Soit (E,R) un ensemble ordonné, et A une partie de E. On dit que M est un ***majorant*** *de A si*

$$(M \in E) \text{ et } (\forall a \in A)(aRM)$$

On dit que M est un ***minorant*** *de A si*

$$(M \in E) \text{ et } (\forall a \in A)(mRa)$$

Si A possède un majorant (respectivement un minorant), on dit qu'il est **majoré** (respectivement **minoré**).

Exemples.
1. dans $(\mathbb{N}, \leq)$, la partie $A = \{3, 7\}$ est minorée par $0, 1, 2$ et 3 et majorée par $7, 8, 9, \ldots$.
2. dans $(\mathbb{N}, /)$, la partie $A = \{3, 7\}$ est minorée par 1 et majorée par $21, 42, 63, \ldots$.
3. dans $(\mathbb{Q}, \leq)$, avec la partie $A = \{\frac{E(\sqrt{2}\cdot 10^n)}{10^n},\ n \in \mathbb{N}\}$.

Nota bene. Attention, un majorant ou un minorant n'est en général pas unique. On dit bien UN majorant, ou UN minorant.

4.2.3 plus grand élément, plus petit élément

Définition 46 (*plus grand élément, plus petit élément*)

(E,R) est un ensemble ordonné et A une partie de E. On dit que a est le ***plus grand élément de*** *A si a est un majorant de A,* ***ET*** *$a \in A$. On dit que a est le* ***plus petit élément de*** *A si a est un minorant de A,* ***ET*** *$a \in A$.*

On note $max(A)$ le plus grand élément de A, et $min(A)$ sont plus petit élément.

Proposition 47

S'ils existent, $max(A)$ et $min(A)$ sont uniques.

Démonstration :

4.2.4 Borne supérieure/borne inférieure

Définition 48 (*borne supérieure, inférieure*)

Soit (E,R) un ensemble ordonné et A une partie de E. La ***borne supérieure de*** *A est le plus petit élément de l'ensemble des majorants de A (s'il existe). La* ***borne inférieure de*** *A est le plus grand élément de l'ensemble des minorants de A (s'il existe).*

La borne supérieure est donc le "plus petit des majorants de A". On le note $sup(A)$. La borne inférieure de A est le plus grand des minorants de A. On le note $inf(A)$.

Nota bene. $s = sup(A)$ ssi $\begin{cases} (\forall a \in A)(aRs) \text{ (c'est un majorant)} \\ \text{et } (\forall M \in E)(\forall a \in A)(aRM \implies sRM) \text{ (c'est le plus petit)} \end{cases}$

Nota bene. $inf(A)$ et $sup(A)$ sont tous les deux le max ou le min d'un ensemble : ils sont uniques s'ils existent.

Exemples.

4.3 Relations d'équivalence

Définition 49 (*relation d'équivalence*)

Une ***relation d'équivalence sur*** *E est une relation binaire sur E qui est* ***réflexive***, ***symétrique*** *et* ***transitive****.*

Exemples. 1. l'égalité sur $\mathbb{R}$.

2. l'équivalence logique " $\iff$ " sur "l'ensemble" des énoncés.
3. $D \parallel D'$ sur l'ensemble des droites du plan.
4. Pour deux entiers relatifs a et b, on dit que a **est congru à** b **modulo** n si n divise $(b-a)$. On note alors $a \equiv b[n]$. C'est une relation d'équivalence sur $\mathbb{Z}$.

Notation. On note souvent $\sim$ une relation d'équivalence.

Définition 50 (*classe d'équivalence*)

Soit E un ensemble, x un élément de E et $\sim$ une relation d'équivalence sur E. La ***classe d'équivalence de*** *x est l'ensemble des éléments de E qui lui sont équivalents. On la note $\bar{x}$.*

$$\bar{x} = \{y \in E : x \sim y\}$$

Exemples. 1. congruence modulo 2 : $\bar{0} = \{0, 2, -2, 4, -4, \ldots\} = 2\mathbb{Z}$ et $\bar{1} = \{1, -1, 3, -3, \ldots\} = 2\mathbb{Z} + 1$. On a

$$\mathbb{Z} = (2\mathbb{Z}) \amalg (2\mathbb{Z} + 1)$$

2. congruence modulo 3 : $\bar{0} = \{0, 3, -3, 6, -6, \ldots\} = 3\mathbb{Z}$, $\bar{1} = 3\mathbb{Z} + 1$ et $\bar{2} = 3\mathbb{Z} + 2$. On a

$$\mathbb{Z} = (3\mathbb{Z}) \amalg (3\mathbb{Z} + 1) \amalg (3\mathbb{Z} + 2)$$

3. congruence modulo n : pour tout entier k on a $\bar{k} = n\mathbb{Z} + k$ et

$$\mathbb{Z} = (n\mathbb{Z}) \amalg (n\mathbb{Z} + 1) \amalg \cdots \amalg (n\mathbb{Z} + n - 1)$$

Définition 51 (*partition*)

E est un ensemble et $(A_i)_{i \in I}$ une famille de parties de E. On dit que $(A_i)_{i \in I}$ réalise une ***partition*** *de A si*

$$\begin{cases} \bigcap_{i \in I} A_i = E \\ \text{et } A_i \cap A_j = \emptyset \text{ pour tout } i \neq j \end{cases}$$

Nota bene. Si $(A_i)_{i \in I}$ réalise une partition de E, chaque x de E appartient à un unique A_i.

Théorème 52

1. *Si $\sim$ est une relation d'équivalence sur E, les classes d'équivalences de $\sim$ réalisent une partition de E.*
2. *Réciproquement, toute partition de E permet de définir une relation d'équivalence (compatible avec cette partition).*

Démonstration :

Définition 53 (*ensemble quotient*)

Soit $\sim$ une relation d'équivalence sur E. On appelle ensemble quotientl'ensemble des classes d'équivalences pour $\sim$. On le note $E/\sim$. On a donc

$$E/\sim = \{\bar{x} : x \in E\}$$

Exemple. Pour la congruence modulo 2, l'ensemble quotient est $\{\bar{0}, \bar{1}\}$. On le note $\mathbb{Z}/2\mathbb{Z}$. Pour la congruence modulo n, on a $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

Chapitre 5

Entiers naturels

5.1 Structure et propriétés

On note $\mathbb{N}$ l'ensemble $0, 1, 2, \ldots$ des entiers naturels et $\mathbb{N}^*$ pour $\mathbb{N} \setminus \{0\}$.

Structure de $(\mathbb{N}, +)$

L'addition $+$ est une **loi de composition interne** sur $\mathbb{N}$ **commutative, associative**, ayant 0 pour **élément neutre**, et pour laquelle chaque élément est **simplifiable** (ou **régulier**).

Structure de $(\mathbb{N}, +, \times)$

La multiplication $\times$ est une loi de compostion interne sur $\mathbb{N}$, commutative, associative, ayant 1 pour élément neutre, et **distributive** sur l'addition. 0 est **absorbant** pour $\times$. Tout élément non nul est simplifiable pour $\times$.

Axiomes de $\mathbb{N}$ 54

1. *Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.*
2. *Toute partie non vide majorée de $\mathbb{N}$ adment un plus grand élément.*

Théorème 55 (*Récurrence*)

Soit $P(n)$ un énoncé sur un entier naturel n. Si $P(0)$ est vrai et si pour tout n, $P(n)$ implique $P(n+1)$, alors pour tout n, $P(n)$ est vraie.

Vocabulaire. $P(0)$ **l'initialisation**. L'implication $(P(n) \implies P(n+1))$ est **l'hérédité**.

5.2 Division euclidienne

Théorème 56

Pour tout entier naturel a et tout entier naturel b non nul, il existe un unique couple d'entiers (q, r) tels que

$$a = bq + r \quad et \quad 0 \leq r < b$$

Application (Ecriture d'un nombre en base b).

5.3 Ensembles finis, ensembles dénombrables

Lemme 57

Soit f est une application de $\{1, \ldots, n\}$ dans $\{1, \ldots, p\}$.

1. *Si f est injective, alors $n \leq p$.*
2. *Si f est surjective, alors $n \geq p$.*

Proposition-Définition 58

*Un ensemble E est **fini** s'il existe un n tel que E soit en bijection avec $\{1, \dots, n\}$. Si E est fini, l'entier n est unique. On l'appelle le **cardinal** de E.*

On note $|E|$ le cardinal de E. Par convention, le cardinal du vide est 0.

Propriétés 59

Soit E un ensemble fini et A une partie de E.

1. *A est fini et $|A| \leq |E|$.*
2. *$A = E$ si et seulement si $|A| = |E|$.*
3. *$P(E)$ est fini et $|P(E)| = 2^{|E|}$.*

Applications entre ensembles finis

Proposition 60

Soient E et F deux ensembles finis de cardinal n et p respectivement. F^E est fini et son cardinal est p^n.

Proposition 61

Soient E et F deux ensembles finis de cardinal n et p respectivement et f une application de E dans F.

1. *Si f est injective, alors $n \leq p$.*
2. *Si f est surjective, alors $n \geq p$.*
3. *Si f est bijective, alors $n = p$.*

Proposition 62 (*nombre d'injections*)

Soient E et F deux ensembles finis de cardinal n et p respectivement. Si $p \geq n$, il y a $p!/(p-n)!$ injections de E dans F.

Proposition 63 (*nombre de bijections*)

Soient E et F deux ensembles finis de cardinal n et p respectivement. Si $p = n$, il y a $n!$ bijections de E dans F.

Coefficients binômiaux

Définition 64 (*coefficient binômial*)

*Pour $n \geq p$, on note C_n^p le **coefficient binômial** $\frac{n!}{p!(n-p)!}$.*

Proposition 65 (*propriétés des coefficients binômiaux*)

1. *C_n^p est le nombre de parties à p éléments dans un ensemble à n éléments.*
2. *$C_n^p = C_n^{n-p}$.*
3. *$C_n^p + C_n^{p+1} = C_{n+1}^{p+1}$ (égalité de Pascal).*
4. *$C_n^1 = C_n^{n-1} = 1$ et $C_n^0 = C_n^n = 1$.*

Proposition 66 (*binôme de Newton*)

n est un entier non nul et a, b deux nombres complexes.

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

Ensembles dénombrables

Définition 67 (*ensembles dénombrables*)

Un ensemble E est ***dénombrable*** *s'il existe une bijection de E dans $\mathbb{N}$.*

Exemples. $\mathbb{N}$, $\mathbb{N}^*$, $2\mathbb{N}$, $\mathbb{N}^2$, $\mathbb{N}^n$, $\mathbb{Z}$, $\mathbb{Z}^n$, $\mathbb{Q}$ et $\mathbb{Q}^n$ sont dénombrables. (cf devoir)

Chapitre 6

Les entiers relatifs

6.1 Structure et propriétés

On note $\mathbb{Z}$ l'ensemble $\{0, 1, -1, 2, -2, \ldots\}$ des entiers relatifs, et $\mathbb{Z}^*$ pour $\mathbb{Z} \setminus \{0\}$.

Structure de $(\mathbb{Z}, +)$

L'addition $+$ est une loi de composition interne commutative associative, ayant un élément neutre, et pour laquelle tout élément a un inverse. On dit que $(\mathbb{Z}, +)$ est un **groupe** commutatif (ou **abélien**).

Structure de $(\mathbb{Z}, \times)$

La multiplication $\times$ est une loi de composition interne commutative associative, ayant 1 pour élément neutre, et distributive sur $+$. On dit que $(\mathbb{Z}, +, \times)$ est un **anneau**. Les seuls éléments inversibles pour $\times$ sont 1 et -1.

Axiomes de $\mathbb{Z}$ 68

1. *Toute partie non vide minorée de $\mathbb{Z}$ admet un plus petit élément.*
2. *Toute partie non vide majorée de $\mathbb{Z}$ adment un plus grand élément.*

Théorème 69 (*division euclidienne*)

Pour tout entier relatif a et tout entier naturel b non nul, il existe un unique couple d'entiers relatifs (q, r) tels que

$$a = bq + r \quad et \quad 0 \leq r < b$$

Application (sous-groupes de $(\mathbb{Z}, +)$). On cherche les parties G de $\mathbb{Z}$ qui ont une structure de groupe, c'est-à-dire telles que :

1. G est inclus dans $\mathbb{Z}$
2. $+$ est une loi de composition interne sur G : pour tout x et y dans G, $x + y$ reste dans G (on dit aussi que G est stable par addition).
3. $+$ est associative (découle directement de l'associativité dans $\mathbb{Z}$).
4. 0 appartient à G
5. tout élément de G a un inverse dans G (ie si x est dans G, $-x$ doit aussi être dans G).

Des exemples évidents de sous-groupes de $(\mathbb{Z}, +)$:

1. $\{0\}$
2. $\mathbb{Z}$
3. $2\mathbb{Z} = \{2a : a \in \mathbb{Z}\}$: l'ensemble des entiers pairs.
4. $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$: l'ensemble des multiples de n.

Théorème 70

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, où n parcourt $\mathbb{N}$.

6.2 Congruence modulo n

Définition 71

*Soit n dans $\mathbb{N}$, et x, y dans entiers relatifs. On dit que x **est congru à** y **modulo** n si $x - y \in n\mathbb{Z}$.*

Notation. On note alors $x \equiv y[n]$.

Remarque.
1. si $n = 0$, on a $x \equiv y[0]$ si et seulement si $x - y \in \{0\}$, c'est à dire si $x = y$. La congruence modulo 0, c'est l'égalité dans $\mathbb{Z}$.
2. si $n = 1$, on a $x \equiv y[0]$ si et seulement si $x - y \in \mathbb{Z}$, ce qui est toujours vrai. Les cas $n = 0$ et $n = 1$ n'ayant pas d'intérêt particulier, on supposera toujours que $n \geq 2$.

Structure de la congruence

La congruence est une relation binaire sur $\mathbb{Z}$ qui est réflexive, symmétrique et transitive : c'est donc une relation d'équivalence. On peut donc parler de classe d'équivalence d'un élément, et d'ensemble quotient. Pour tout entier relatif x, la classe d'équivalence de x modulo n est par définition :

$$\overline{x} = \{y \in \mathbb{Z} : y \equiv x[n]\} = \{y \in \mathbb{Z} : y - x \in \mathbb{Z}\} = x + n\mathbb{Z}$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient correspondant à cette relation, c'est-à-dire :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{x} : x \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

C'est un ensemble fini de cardinal n. Chaque classe $\overline{x}$ a une infinité de représentants (x, $x + n$, etc.). Mais un seul de ces représentants est compris entre 0 et $n - 1$ (c'est une conséquence de la division euclidienne de x par n).

Structure de $\mathbb{Z}/n\mathbb{Z}$

Il est facile d'additionner deux entiers relatifs. On va voir que l'on peut aussi additioner deux classes modulo n, et donc définir une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ qui a les mêmes propriétés que l'addition sur $\mathbb{Z}$: associativité, commutativité, élément neutre ($\overline{0}$), et tout élément a un inverse.

Proposition 72 (*addition dans* $\mathbb{Z}/n\mathbb{Z}$)

Soient x et y dans $\mathbb{Z}$. On définit $\bar{+}$ en posant

$$\overline{x} \bar{+} \overline{y} = \overline{x + y}$$

$(\mathbb{Z}/n\mathbb{Z}, \bar{+})$ est un groupe ablélien.

Nota bene. Par abus de notation et pour éviter les lourdeurs d'écriture, on note souvent $\overline{x} + \overline{y}$ au lieu de $\overline{x} x \bar{+} \overline{y}$.

De la même manière, on peut multiplier deux classes modulo n :

Proposition 73 (*multiplication dans* $\mathbb{Z}/n\mathbb{Z}$)

Soient x et y dans $\mathbb{Z}$. On définit $\bar{\times}$ en posant

$$\overline{x} \bar{\times} \overline{y} = \overline{x \times y}$$

$(\mathbb{Z}/n\mathbb{Z}, \bar{+}, \bar{\times})$ est un anneau commutatif.

Nota bene. On note souvent $\overline{x}\overline{y}$ au lieu de $\overline{x} \bar{\times} \overline{y}$.

Exemple. Tables de multiplication dans $\mathbb{Z}/n\mathbb{Z}$ pour $n = 2$, 3, 4 et 5.

Diviseurs de zéro, éléments simplifiables

Définition 74 (*diviseur de zéro*)

*Soient a et b dans $\mathbb{Z}$. On dit que $(\overline{a}, \overline{b})$ est un **couple de diviseur de zéro** si $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$ et $\overline{a}\overline{b} = \overline{0}$. On dit que $\overline{a}$ est un **diviseur de zéro** s'il existe un b dans $\mathbb{Z}$ tel que $(\overline{a}, \overline{b})$ soit un couple de diviseur de zéro.*

Définition 75 (*élément simplifiable*)

Soient a dans $\mathbb{Z}$. On dit que a est simplifiable si pour tout b et c dans $\mathbb{Z}$, l'égalité $ab = ac$ implique $b = c$.

Proposition 76

Dans $\mathbb{Z}/n\mathbb{Z}$ un élément est un diviseur de zéro si et seulement si il n'est pas simplifiable.

Nota bene. Dans un exercice sur les congruences, on commence par étudier si n est premier. S'il est premier, tout élément non nul est simplifiable et on peut faire des calculs comme dans $\mathbb{Z}$. Si n n'est pas premier, faire attention aux diviseurs de zéro. On commence en général par dresser une liste de tous les couples de diviseurs de zéro, et des éléments inversibles, qui sont exactement les éléments simplifiables :

Proposition 77

Dans $\mathbb{Z}/n\mathbb{Z}$, les éléments inversibles sont exactement les éléments simplifiables.

Théorème 78

n est premier si et seulement si tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible.

Vocabulaire. Lorsque n est premier, on dit que $\mathbb{Z}/n\mathbb{Z}$ est un **corps**.