Résumé de cours :
Semaine 4, du 25 au 29 septembre.

1 Les ensembles (suite et fin)

1.1 Quantificateurs

Définition du quantificateur universel :
Soit E un ensemble et P un prédicat sur E. La propriété "$\forall x \in E,\ P(x)$" signifie que pour tous les éléments x de E, $P(x)$ est vraie, c'est-à-dire que $\{x \in E / P(x)\}$ est égal à E.

Définition du quantificateur existentiel :
Avec les mêmes notations, la propriété "$\exists x \in E,\ P(x)$" signifie qu'il existe au moins un $x \in E$ tel que $P(x)$ est vraie, c'est-à-dire que $\{x \in E / P(x)\} \neq \emptyset$.

Existence et unicité : La propriété "$\exists! x \in E,\ P(x)$" signifie qu'il existe un unique $x \in E$ tel que $P(x)$ est vraie, c'est-à-dire que $\{x \in E / P(x)\}$ est un singleton.

Remarque. L'emploi des quantificateurs en guise d'abréviations est exclu : l'usage d'un "$\forall x$" est toujours suivi d'un "$\in E,\ P(x)$" (ou plus rarement d'un "$,\ P(x)$"), où P est un prédicat sur E.

Remarque. Soit P un prédicat sur un ensemble E. Alors dans les phrases
"$\forall x \in E,\ P(x)$" et "$\exists x \in E,\ P(x)$", on peut remplacer la variable x par y, ou n'importe quel autre symbole. On dit que, dans les phrases "$\forall x \in E,\ P(x)$" et "$\exists x \in E,\ P(x)$", x est une variable muette ou bien que c'est une variable liée.
Dans la propriété "$\exists y \in \mathbb{R},\ x = y^2$", y est une variable liée, et par opposition, on dit que x est une variable libre.

1.2 Parties d'un ensemble

Définition. Soit E et F deux ensembles.
On dit que F est inclus dans E et l'on note $F \subset E$ si et seulement si tout élément de F est un élément de E, c'est-à-dire si et seulement si $\forall x \in F,\ x \in E$.

Transitivité de l'inclusion : Si $A \subset B$ et $B \subset C$, alors $A \subset C$.

Définition. Si E est un ensemble, on note $\mathcal{P}(E)$ l'ensemble de ses parties.

1.3 Opérateurs sur les ensembles

Définition. Soit E et F deux ensembles :
- **Intersection :** $x \in E \cap F$ si et seulement si ($x \in E$ et $x \in F$).
- **Réunion :** $x \in E \cup F$ si et seulement si ($x \in E$ ou $x \in F$).
- **Différence ensembliste :** $E \setminus F = \{x \in E / x \notin F\}$.
- **Différence symétrique :** $E \Delta F = (E \setminus F) \cup (F \setminus E) = (E \cup F) \setminus (E \cap F)$.
- **Complémentaire de F dans E :** Si F est une partie de E, le complémentaire de F dans E est $\overline{F} = E \setminus F$, que l'on note plus rarement $\complement_E^F$.

Propriété. Si F et G sont deux parties d'un ensemble E, alors $F \setminus G = F \cap \overline{G}$.

Propriété. ***Associativité de l'intersection et de la réunion*** : Soit A, B, C trois ensembles. Alors, $A \cap (B \cap C) = (A \cap B) \cap C$ et $A \cup (B \cup C) = (A \cup B) \cup C$.

Définition. Soit I un ensemble et $(E_i)_{i\in I}$ une famille d'ensembles. On définit $\bigcup_{i\in I} E_i$ et $\bigcap_{i\in I} E_i$ par :

$x \in \bigcup_{i\in I} E_i \iff (\exists i \in I,\ \ x \in E_i)$ et $x \in \bigcap_{i\in I} E_i \iff (\forall i \in I,\ \ x \in E_i)$.
Cette dernière définition n'est pas correcte lorsque $I = \emptyset$.

Distributivité de l'intersection par rapport à la réunion :
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. $\quad A \cap \bigcup_{i\in I} B_i = \bigcup_{i\in I} (A \cap B_i)$.

Il faut savoir le démontrer.
Distributivité de la réunion par rapport à l'intersection :
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. $\quad A \cup \bigcap_{i\in I} B_i = \bigcap_{i\in I} (A \cup B_i)$ (avec $I \neq \emptyset$).

Notation. Soit $(E_i)_{i\in I}$ une famille d'ensembles deux à deux disjoints, c'est-à-dire telle que, pour tout $i, j \in I$ avec $i \neq j$, $E_i \cap E_j = \emptyset$.
Alors $\bigcup_{i\in I} E_i$ est appelée une réunion disjointe et elle est notée $\bigsqcup_{i\in I} E_i$.

2 L'ensemble $\mathbb{N}$ des entiers naturels

On admet qu'il existe un ensemble, noté $\mathbb{N}$, satisfaisant les axiomes de Peano suivants :

- $\mathbb{N}$ est muni d'un élément particulier noté 0 et d'une application "successeur", notée s de $\mathbb{N}$ dans $\mathbb{N}$.
- 0 n'est le successeur d'aucun entier : $\forall n \in \mathbb{N},\ \ s(n) \neq 0$.
- s est une application injective : pour tout $n, m \in \mathbb{N}$, si $s(n) = s(m)$, alors $n = m$.
- Pour toute partie F de $\mathbb{N}$, si $0 \in F$ et si pour tout $n \in F$, $s(n) \in F$, alors $F = \mathbb{N}$.

Principe de récurrence : Soit $R(n)$ un prédicat sur $\mathbb{N}$.
Si $R(0)$ est vraie et si pour tout $n \in \mathbb{N}$, $R(n)$ implique $R(s(n))$,
alors pour tout $n \in \mathbb{N}$, $R(n)$ est vraie.

Addition entre entiers : Pour tout $m \in \mathbb{N}$, on pose
$0 + m = m$ et
$\forall n \in \mathbb{N},\ \ s(n) + m = s(n + m)$.
Ces conditions définissent l'addition entre entiers.

Propriétés de l'addition :

- 0 est neutre : $\forall m \in \mathbb{N},\ \ m + 0 = 0 + m = m$.
- Associativité : $\forall n, m, k \in \mathbb{N},\ \ (n + m) + k = n + (m + k)$.
- Commutativité : $\forall n, m \in \mathbb{N},\ \ n + m = m + n$.

3 Produit cartésien

Définition. Si a et b sont deux objets, posons $(a, b) = \{\{a\}, \{a, b\}\}$. On l'appellera le "couple de composantes a et b". Alors, $(a, b) = (c, d)$ si et seulement si $a = c$ et $b = d$.
Il faut savoir le démontrer.

Définition. Si A et B sont deux ensembles, on pose $A \times B = \{(a, b)/a \in A \text{ et } b \in B\}$.
$A \times B$ s'appelle le produit cartésien de A et B.

Définition. Un couple est aussi un 2-uplet. Pour $n \geq 3$, on définit récursivement la notion de n-uplet (ou n-liste) en écrivant : $(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$.
Alors, $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)$ si et seulement si $\forall i \in \{1, \ldots, n\},\ \ a_i = b_i$.

Notation. $\mathbb{N}^*$ désigne $\mathbb{N} \setminus \{0\}$.

Définition. Soit $n \in \mathbb{N}^*$. Si $A_1, \ldots, A_n$ sont n ensembles, on pose
$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) / \forall i \in \{1, \ldots, n\},\ \ a_i \in A_i\}$.
Si E est un ensemble, on note $E^n = \underbrace{E \times \cdots \times E}_{n fois}$.

Remarque. Convention, lorsque $n = 1$, le "1-uplet" (a) est égal à a.
Avec cette convention, $E^1 = E$.

Commutativité de deux quantificateurs universels :
Soit E et F deux ensembles. Notons $P(x, y)$ un prédicat défini sur $E \times F$. Alors
$$\begin{aligned}[\forall (x, y) \in E \times F,\ \ P(x, y)] &\iff [\forall x \in E,\ \ \forall y \in F,\ \ P(x, y)] \\ &\iff [\forall y \in F,\ \ \forall x \in E,\ \ P(x, y)]\end{aligned}$$

Commutativité de deux quantificateurs existentiels :De même,
$$\begin{aligned}[\exists (x, y) \in E \times F,\ \ P(x, y)] &\iff [\exists x \in E,\ \ \exists y \in F,\ \ P(x, y)] \\ &\iff [\exists y \in F,\ \ \exists x \in E,\ \ P(x, y)]\end{aligned}$$

ATTENTION :
Un quantificateur universel ne commute pas avec un quantificateur existentiel.
"$\forall x \in E,\ \ \exists y \in F,\ \ P(x, y)$" si et seulement si il existe une application
$x \longmapsto y(x)$ de E dans F tel que, pour tout $x \in E$, $P(x, y(x))$,
et "$\exists y \in F,\ \ \forall x \in E,\ \ P(x, y)$" si et seulement si il existe une application **constante**
$x \longmapsto y_0$ de E dans F, telle que pour tout $x \in E$, $P(x, y_0)$.
On voit qu'en général, la seconde affirmation implique la première mais que la réciproque est fausse.
À savoir exposer.

4 Formules propositionnelles

4.1 Syntaxe

Définition par induction des formules propositionnelles : on part d'un ensemble $\mathcal{V}$ dont les éléments sont appelés des variables propositionnelles. On utilise également les "connecteurs logiques" suivants : $\wedge, \vee, \Longrightarrow, \Longleftrightarrow, \neg$.
L'ensemble F des formules propositionnelles est défini par induction structurelle :
- Les variables propositionnelles sont des formules propositionnelles.
- si $P, Q \in F$, alors $(P \wedge Q), (P \vee Q), (P \Longrightarrow Q), (P \Longleftrightarrow Q)$ et $\neg P$ sont aussi des formules propositionnelles.

Plus précisément, si l'on note $F_0 = \mathcal{V}$, et pour tout $n \in \mathbb{N}$,
$F_{n+1} = F_n \cup \{\neg P / P \in F_n\} \cup \{(P \alpha Q) / P, Q \in F_n$ et $\alpha \in \{\wedge, \vee, \Longrightarrow, \Longleftrightarrow\}\}$, alors $F = \bigcup\limits_{n \in \mathbb{N}} F_n$.

Remarque. Une formule propositionnelle s'appelle aussi une proposition, une assertion, une formule, un énoncé, une expression booléenne, etc.

Définition. Si P et Q sont deux formules propositionnelles, $P \wedge Q$ (prononcer "P et Q") s'appelle la conjonction de P et de Q, $P \vee Q$ (prononcer "P ou Q") s'appelle la disjonction de P et de Q, $P \Longrightarrow Q$ s'appelle une implication, $P \Longleftrightarrow Q$ est une équivalence, et $\neg P$ est la négation de la proposition P.

4.2 Sémantique

Définition. Une distribution de valeurs de vérité sur l'ensemble $\mathcal{V}$ des variables propositionnelles est une application de $\mathcal{V}$ dans l'ensemble $\{V, F\}$.

Définition. Soit v une distribution de valeurs de vérité sur l'ensemble $\mathcal{V}$. On prolonge v sur l'ensemble des formules propositionnelles construites à partir de $\mathcal{V}$ de la manière suivante : pour toutes formules propositionnelles P et Q,

— $v(P \wedge Q) = 1$ si et seulement si $v(P) = v(Q) = 1$.
— $v(P \vee Q) = 1$ si et seulement si $v(P) = 1$ ou $v(Q) = 1$.
— $v(P \Longrightarrow Q) = 0$ si et seulement si $v(P) = 1$ et $v(Q) = 0$.
— $v(P \Longleftrightarrow Q) = 1$ si et seulement si $v(P) = v(Q)$.
— $v(\neg P) = 1$ si et seulement si $v(P) = 0$.

Définition. La définition précédente est équivalente à la donnée des "tables de vérité" des connecteurs logiques $\wedge$, $\vee$, $\Longrightarrow$, $\Longleftrightarrow$ et $\neg$:

P	Q	$P \wedge Q$	$P \vee Q$	$P \Longrightarrow Q$
V	V	V	V	V
V	F	F	V	F
F	V	F	V	V
F	F	F	F	V

Définition. Lorsque $P \Longrightarrow Q$, on dit que P est une *condition suffisante* pour Q et que Q est une *condition nécessaire* pour P.
Lorsque $P \Longleftrightarrow Q$, on dit que P est une *condition nécessaire et suffisante* pour Q.

Définition. Une tautologie est une formule propositionnelle qui est toujours vraie, quelle que soit la distribution de valeurs de vérité des variables propositionnelles qui interviennent dans la formule.

Exemple. Quelques tautologies à connaître (A, B, C désignent des formules propositionnelles quelconques) :

1. $(A \vee (B \vee C)) \Longleftrightarrow ((A \vee B) \vee C)$: associativité de $\vee$ ($\wedge$ est aussi associatif),
2. $(A \wedge (B \vee C)) \Longleftrightarrow ((A \wedge B) \vee (A \wedge C))$: distributivité de $\wedge$ par rapport à $\vee$,
3. $(A \vee (B \wedge C)) \Longleftrightarrow ((A \vee B) \wedge (A \vee C))$: distributivité de $\vee$ par rapport à $\wedge$,
4. $(A \wedge (A \vee B)) \Longleftrightarrow A$: première loi d'absorption,
5. $((A \vee (A \wedge B)) \Longleftrightarrow A$ seconde loi d'absorption,
6. $(\neg(A \vee B)) \Longleftrightarrow (\neg A \wedge \neg B)$: loi de Morgan,
7. $(\neg(A \wedge B)) \Longleftrightarrow (\neg A \vee \neg B)$: loi de Morgan,
8. $(A \Longrightarrow B) \Longleftrightarrow (\neg A) \vee B$ (une définition de l'implication),
9. $\neg(A \Longrightarrow B) \Longleftrightarrow A \wedge (\neg B)$,
10. $(A \Longrightarrow B) \Longleftrightarrow (\neg B \Longrightarrow \neg A)$: contraposition.
11. $((A \Longrightarrow B) \wedge (B \Longrightarrow C)) \Longrightarrow (A \Longrightarrow C)$ (règle du modus ponens).

Il faut savoir le démontrer.

Définition. On dit que deux propositions P et Q sont logiquement équivalentes si et seulement si la proposition $P \Longleftrightarrow Q$ est une tautologie. On notera alors $P \equiv Q$
Ainsi, lorsque l'on ne s'intéresse qu'à la valeur booléenne des propositions, on peut remplacer toute proposition par une proposition qui lui est logiquement équivalente.

Exemple. $(A \wedge (B \vee C)) \equiv ((A \wedge B) \vee (A \wedge C))$.
$\neg(A \Longrightarrow B) \equiv A \wedge \neg B$ et $A \Longrightarrow B \equiv \neg A \vee B$.

Définition. La contraposée de l'implication $A \Longrightarrow B$ est égale à $\neg B \Longrightarrow \neg A$.
Toute implication est logiquement équivalente à sa contraposée.

5 Négation d'une proposition

◇ $\neg(A \vee B)$ est logiquement équivalente à $(\neg A) \wedge (\neg B)$,
$\neg(A \wedge B)$ est logiquement équivalente à $(\neg A) \vee (\neg B)$.
◇ $\neg(\neg A)$ est logiquement équivalente à A.
◇ $\neg(A \Longrightarrow B)$ est logiquement équivalente à $A \wedge (\neg B)$.
◇ Une équivalence est la conjonction de deux implications, donc
$\neg(A \Longleftrightarrow B)$ est logiquement équivalente à $[\neg(A \Longrightarrow B)] \vee [\neg(B \Longrightarrow A)]$.

Propriété. Soit P un prédicat sur un ensemble E.
$\neg[\forall x \in E,\ \ P(x)] \Longleftrightarrow [\exists x \in E,\ \ \neg P(x)]$
et $\neg[\exists x \in E,\ \ P(x)] \Longleftrightarrow [\forall x \in E,\ \ \neg P(x)]$.

Exemple. Savoir nier qu'une suite $(x_n)_{n\in\mathbb{N}}$ de réels converge vers 0 :
$\neg[\forall \varepsilon > 0,\ \ \exists N \in \mathbb{N},\ \ \forall n \in \mathbb{N},\ \ [n \geq N \Longrightarrow |x_n| \leq \varepsilon]] \equiv \cdots$.

Propriété. Soit A et B deux ensembles de E.
Soit $(E_i)_{i\in I}$ une famille de parties de E, avec $I \neq \emptyset$. Alors,
— $\overline{\overline{A}} = A, \quad \overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{A \cap B} = \overline{A} \cup \overline{B}$,
— $A \subset B \Longleftrightarrow \overline{B} \subset \overline{A}$,
— $\overline{\bigcap_{i\in I} E_i} = \bigcup_{i\in I} \overline{E_i}$, , $\qquad \overline{\bigcup_{i\in I} E_i} = \bigcap_{i\in I} \overline{E_i}$.

6 Relations binaires

6.1 Définitions

Définition. Une relation binaire R sur $E \times F$ est une partie de $E \times F$, mais on notera "xRy" au lieu de "$(x, y) \in R$". Le graphe de R est $\{(x, y) \in E \times F / xRy\}$, donc le graphe de R est ... égal à R.

Définition. Lorsque $E = F$, on dit que
— R est réflexive si et seulement si $\forall x \in E,\ \ xRx$,
— R est symétrique si et seulement si $\forall x, y \in E,\ \ (xRy) \Longrightarrow (yRx)$,
— R est antisymétrique si et seulement si $\forall x, y \in E,\ \ [(xRy) \wedge (yRx) \Longrightarrow x = y]$,
— et R est transitive si et seulement si $\forall x, y, z \in E,\ \ [(xRy) \wedge (yRz) \Longrightarrow (xRz)]$.