Semaine 02

lundi 15 septembre 2025
> ven. 19 septembre 2025

Chapitre 1 **Notions de logique, ensembles**

Notions de logique

- **Vocabulaire :** « *assertion* » (ou « *proposition mathématique* »)
  Il s'agit d'une phrase non ambigüe à laquelle est associée une valeur de vérité « vrai » ou « faux » dans le cadre d'une théorie axiomatique.
- **Définitions :**
  - La négation ;
  - Les connecteurs logiques (binaires) : il existe 16 connecteurs logiques binaires ; parmi ceux-ci on présente : « $\wedge$ » (conjonction), « $\vee$ » (disjonction), « $\Rightarrow$ » et « $\iff$ ».
- **Propriétés :** Le « ou » est inclusif ; on peut écrire « $A \Rightarrow B$ » sous la forme « $(\neg A) \vee B$ ».
- **Définition :** La réciproque de l'implication « $A \Rightarrow B$ » est l'implication « $B \Rightarrow A$ » (à ne pas confondre ni avec la contraposée, ni avec la négation).

Propriétés (connecteurs logiques) :
- Associativité de « $\wedge$ » et « $\vee$ » ;
- Transitivité de « $\Rightarrow$ » ;
- Distributivité de « $\wedge$ » sur « $\vee$ » ;
- Distributivité de « $\vee$ » sur « $\wedge$ ».

Propriétés (Lois de De Morgan) :
Soit A et B deux assertions. On a :

$$\neg(A \wedge B) \iff (\neg A) \vee (\neg B)$$

$$\neg(A \vee B) \iff (\neg A) \wedge (\neg B)$$

- **Définitions :** Référentiel ; Prédicat à une variable $\mathscr{P}(x)$; Les quantificateurs ; le quantificateur universel $\forall$, le quantificateur existentiel $\exists$. Notation $\exists!$ (traduite à l'aide de $\forall$ et $\exists$).

Ensembles

- **Notations :** $\in$, $\ni$, $\subset$ et $\supset$; $x \in E \iff \{x\} \subset E$.
  Famille des parties d'un ensemble E : $\mathcal{P}(E)$; $F \subset E \iff F \in \mathcal{P}(E)$.
- **Définition (opérations usuelles dans $\mathcal{P}(E)$) :** Si A et B sont deux parties d'un ensemble E, on définit :
  - La réunion : $A \cup B = \{x \in E \mid (x \in A) \vee (x \in B)\}$;
  - L'intersection : $A \cap B = \{x \in E \mid (x \in A) \wedge (x \in B)\}$;
  - Le complémentaire dans E : $E \setminus A = \{x \in E \mid x \notin A\}$;
  - La différence de A et B : $A \setminus B = A \cap (E \setminus B)$.
- **Vocabulaire :** Deux parties A et B sont dites *disjointes* si $A \cap B = \varnothing$ et *distinctes* si $A \neq B$.

Chapitre 2 **Divers modes de raisonnement**

- **Raisonnement par déduction :** $A \implies B$, exemples.
- **Raisonnement par équivalence :** $A \iff B$, exemples.
- **Raisonnement par analyse-synthèse :** Propriétés du type « $\exists!\, x \in E,\ \mathscr{P}(x)$ », exemples.
- **Raisonnement par contraposée :**
  $(\neg B \implies \neg A) \iff (A \implies B)$, exemples.
- **Raisonnement par l'absurde :** $\neg A$ faux $\iff$ A vrai, exemples.
- **Raisonnement par disjonction de cas :**
  Si $(A_1 \wedge A_2 \dots) \iff A$, il suffit de montrer A_1, A_2, ..., exemples.
- **Raisonnement par récurrence :** Cf. chapitre 6.

Chapitre 3 **Applications**

Correspondances, fonctions, applications

- **Définition :** Produit cartésien ; $\operatorname{card}(E \times F) = \operatorname{card}(E) + \operatorname{card}(F)$; Produit cartésien d'un nombre fini d'ensembles.
- **Définition :** Une application f de E vers F est la donnée d'un triplet (E,F,Γ) où Γ est une partie de $E \times F$ telle que :
  $\forall (x,y,y') \in E \times F \times F,\ [(x,y) \in \Gamma \text{ et } (x,y') \in \Gamma] \implies y = y'$.
  On écrit $y = f(x)$ plutôt que $(x,y) \in \Gamma$.
- **Définition :** Une application est une fonction dont l'ensemble de définition est égal à l'ensemble de départ. En pratique, on tolère l'utilisation de « fonction » et « application » indifféremment. On note l'ensemble des fonctions de E dans F par $\mathcal{F}(E,F)$ ou F^E.
- **Définition :** L'ensemble de définition de f est :
  $\{x \in E \mid \exists y \in F,\ (x,y) \in \Gamma\}$.

- **Propriété :** Soient E et F deux ensembles non vides. Soit $u = (\Gamma, E, F)$ une application, avec Γ le graphe de u. On a alors : $\forall\, x \in E,\ \exists\,!\, y \in F, \quad (x,y) \in \Gamma$.
- **Définition :** L'ensemble image de f, noté $\mathrm{Im}(f)$ ou $f(E)$ est l'ensemble $\{f(x) \mid x \in E\}$.
- **Définition :** Restriction, prolongement.

Applications injectives, surjectives et bijectives

- **Définitions :**
  - f injective : $\forall\,(x_1,x_2) \in E^2, \quad x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$.
  - f surjective : $\forall\, y \in F, \exists\, x \in E, \quad y = f(x)$.
  - f bijective : injective et surjective.
- **Propriété (caractérisation des injections) :** Les propositions suivantes sont équivalentes :

(*i*) L'application f est injective.
(*ii*) Tout élément de F possède au plus un antécédent par f.
(*iii*) Pour tout $y \in F$, l'équation $f(x) = y$ possède au plus une solution.
(*iv*) $\forall\,(x_1,x_2) \in E^2, \quad (f(x_1) = f(x_2) \implies x_1 = x_2)$.

- **Propriété (caractérisation des surjections) :** Les propositions suivantes sont équivalentes :

(*i*) L'application f est surjective.
(*ii*) Tout élément de F a au moins un antécédent par f.
(*iii*) Pour tout $y \in F$, l'équation $f(x) = y$ possède au moins une solution.
(*iv*) $\forall\, y \in F, \exists\, x \in E, \quad y = f(x)$.

- **Propriété (caractérisation des bijections) :** Les propositions suivantes sont équivalentes :

(*i*) L'application f est bijective.
(*ii*) Tout élément de F a un et un seul antécédent par f.
(*iii*) Pour tout $y \in F$, l'équation $f(x) = y$ possède une unique solution.
(*iv*) $\forall\, u \in F, \exists! x \in E, \quad y = f(x)$.

Composition des applications

- **Définition :** L'application $h : E \longrightarrow G$ définie par : $\forall\, x \in E, \quad h(x) = g[f(x)]$ est appelée *composée* de f par g et notée $g \circ f$.
- **Définition et propriétés :** La composition des applications « $\circ$ » est une opération associative mais non commutative en général : $(f \circ g) \circ h = f \circ (g \circ h)$ mais $g \circ f \neq f \circ g$ en général.
- **Exemple :** Composition des translations de vecteur du plan.

Propriétés (composée d'injections, surjections, bijections) : Soient $f \in F^E$ et $g \in G^F$.
1. Si f et g sont injectives, alors $g \circ f$ est injective.
2. Si f et g sont surjective, alors $g \circ f$ est surjective.
3. Si f et g sont bijectives, alors $g \circ f$ est bijective.

Propriétés : Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ des applications.
1. Si $g \circ f$ est injective, alors f est injective.
2. Si $g \circ f$ est surjective, alors g est surjective.

Application réciproque

- **Définition :** Application identité $\mathrm{Id}_E : E \longrightarrow E : \mathrm{Id}_E(x) = x$.

Définition (caractérisation de la fonction réciproque) : Si $f : E \to F$ est une application, les deux propriétés suivantes sont équivalentes :
1. f est bijective de E sur F ;
2. Il existe une application $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$.

De plus, si l'une des conditions est vérifiée, la fonction g est unique et est appelée *fonction réciproque de f*, notée f^{-1}.

- **Remarque :** On peut avoir $f \circ g = \mathrm{Id}_F$ ou $g \circ f = \mathrm{Id}_E$ sans que f et g soient bijectives.
- **Corollaire :**
  1. Si $f \in F^E$ est bijective, alors u^{-1} est bijective et $(u^{-1})^{-1} = u$.
  2. Si $u \in F^E$ et $v \in G^F$ sont deux applications bijectives, alors $(v \circ u)^{-1} = u^{-1} \circ v^{-1}$.

À suivre...

Chapitre 21 Divisibilité dans $\mathbb{Z}$

Diviseurs d'un entier relatif

- **Définition (Divisibilité dans $\mathbb{Z}$) :** Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. On dit que b *divise* a si et seulement si

$$\exists\, k \in \mathbb{Z}, \quad a = b \times k.$$

Lorsque b divise a, on note $b|a$.
L'ensemble des diviseurs de a, noté $\mathrm{Div}(a)$ est défini par

$$\mathrm{Div}(a) = \{b \in \mathbb{Z}^* \mid b|a\} = \{b \in \mathbb{Z}^* \mid a = b \times k,\ k \in \mathbb{Z}\}.$$

- **Remarque :**
  - Lorsque b divise a, on dit aussi que b *est un diviseur de* a, ou bien, a *est un multiple de* b.
  - $\mathrm{Div}(0) = \mathbb{Z}$.
  - Par contre, aucun entier relatif non nul est divisible par 0.
- **Exemple :** L'ensemble des entiers relatifs n tels que $2n+5$ divise 7 est $\{-6, -3, -2, 1\}$.
- **Propriété :** Quel que soit $a \in \mathbb{Z}$, $\mathrm{Div}(a) = \mathrm{Div}(|a|)$.
- **Remarque :** Cette proposition permet, dans la recherche des diviseurs d'un entier relatif a, de restreindre la détermination de $\mathrm{Div}(a)$ à $\mathrm{Div}(|a|)$, avec $|a| \in \mathbb{N}$.
- **Algorithme (de recherche brute des diviseurs d'un entier naturel) :**

```python
def diviseurs(n) :
    L=[]
    for k in range(1,n+1) :
        if n%k==0 :
            L.append(k)
    return L
```

Propriété : La relation « divise » est une relation d'ordre dans $\mathbb{Z}$, c'est-à-dire qu'elle est réflexive, antisymétrique et transitive.

- **Remarques :**
  - La relation $|$ est une relation d'ordre partiel car deux entiers relatifs ne sont pas toujours comparables pour $|$, par opposition à la relation $\leqslant$ qui est d'ordre total dans $\mathbb{Z}$.
  - Nous avons $\{-1, 1, -a, a\} \subset \mathrm{Div}(a)$.
- **Propriété (Lien entre $|$ et $\leqslant$) :** Soient a et b deux entiers relatifs non nuls.

$$b|a \implies |b| \leqslant |a|.$$

- **Remarques :**
  - Lorsque $b = 0$, la proposition est fausse.
  - La réciproque est évidemment fausse.
- **Propriété (Divisibilité et combinaison linéaire) :** Soient a, b et c trois entiers relatifs avec $c \neq 0$.
Si $c|a$ et $c|b$, alors, quels que soient les entiers relatifs α et β,

$$c|\alpha a + \beta b.$$

En particulier, nous avons : $c|a + b$ et $c|a - b$.
- **Remarque :** Comme souvent en arithmétique, la réciproque de cette proposition est fausse.
- **Exemple :** L'ensemble des diviseurs communs aux deux entiers relatifs $a = 6n + 5$ et $b = 7n + 6$, avec $n \in \mathbb{Z}$, est

$$\mathrm{Div}(a) \cap \mathrm{Div}(b) = \{-1, 1\}.$$

Dans ce cas, on dit que a et b sont premiers entre eux.
- **Propriété :** Soient $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$.
Si $a|b$, alors $a|bc$ et $ac|bc$.
- **Remarques :**
  - La réciproque de $(a|b \implies a|bc)$ est fausse, ce qui est justifié par le contre exemple qui suit.
  Pour $a = 6$, $b = 4$ et $c = 9$, nous avons $6|4 \times 9$ mais 6 ne divise ni 4, ni 9.
  - Lorsque $c \in \mathbb{Z}^*$, la réciproque de $(a|b \implies ac|bc)$ est vraie.

Division euclidienne dans $\mathbb{Z}$

- **Axiome du plus petit élément :** Toute partie B non vide de $\mathbb{N}$ admet un plus petit élément p, ce qui signifie

$$\exists\, p \in \mathbb{N}, \forall\, b \in B, \quad (b \geqslant p) \wedge (p \in B).$$

Lemme d'Archimède : Quels que soient les entiers naturels x et y, avec $x \neq 0$, il existe un entier naturel n tel que

$$nx > y.$$

- **Remarques :**
  - Ce résultat est encore vrai lorsque $(x, y) \in \mathbb{R}_+^* \times \mathbb{R}_+$. On dit que $\mathbb{R}$ est archimédien.
  - Ce lemme est faux si x est nul.

Propriété (Division euclidienne dans $\mathbb{N}$) : Quels que soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$, il existe un couple unique d'entiers naturels (q, r) satisfaisant à

$$a = bq + r, \quad \text{avec } 0 \leqslant r < b.$$

- **Remarque :** La double inégalité $0 \leqslant r < b$ signifie également

$$r \in \{0, 1, 2, \ldots, b - 1\}, \quad \text{c'est-à-dire } r \in [\![0, b - 1]\!].$$

- **Exemple :** La division euclidienne d'un entier naturel par 2 induit une partition de $\mathbb{N}$ qui est constituée par l'union disjointe de l'ensemble des entiers naturels pairs avec l'ensemble des entiers naturels impairs.
- **Remarque :** Plus généralement, lors de la division euclidienne d'un entier naturel n par un entier naturel b non nul, nous définissons une partition de $\mathbb{N}$ en b sous-ensembles disjoints deux à deux, qui sont classifiés selon leur reste dans cette division par b.
- **Exemple :** Nous montrons, quel que soit l'entier naturel n, que l'entier

$$u_n = n(n + 1)(2n + 1)$$

est divisible par 3, puis par 6.

► **Algorithme** Nous disposons en Python des procédures suivantes :

- `a%b` qui restitue le reste de la division euclidienne de a par b.
- `a//b` qui restitue le quotient de la division euclidienne de a par b.

Ceci permet de proposer la fonction Python

```
def divisioneucli(a,b) :
    q=a//b
    r=a%b
    return(q,r)
```

Propriété (Division d'un entier relatif par un entier naturel non nul) : Quels que soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un couple unique d'entiers relatifs (q,r) satisfaisant à

$$a = bq + r, \quad \text{avec } 0 \leqslant r < b.$$

► **Exemple :** Nous prouvons que tout entier relatif n qui n'est pas divisible par 3 a un carré qui donne 1 pour reste dans sa division euclidienne par 3.

Propriété (Division d'un entier relatif par un entier relatif non nul) : Quels que soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, il existe un couple unique d'entiers relatifs (q,r) satisfaisant à

$$a = bq + r, \quad \text{avec } 0 \leqslant r < |b|.$$

► **Exemple :** La division euclidienne de -202 par -13 restitue un quotient $q = 16$ et un reste $r = 6$.

► **Remarque :** La double inégalité $0 \leqslant r < |b|$ signifie également

$$r \in \{0,1,2,\ldots,|b|-1\}, \quad \text{c'est-à-dire } r \in [\![0,|b|-1]\!].$$

► **Exemple :** Tout entier relatif a, dans la division euclidienne par -4, peut s'écrire par disjonction

$$(a = -4q) \vee (a = -4q+1) \vee (a = -4q+2) \vee (a = -4q+3),$$

avec $q \in \mathbb{Z}$, ce qui définit une partition de $\mathbb{Z}$.

!

► Pour les parties désignées par un symbole

Propriété : une démonstration est exigible.

► Une colle comporte une question de cours choisie *a priori* parmi celles indiquées dans le programme de la semaine en cours (normalement, ±15 min).

► Un cours non appris sera sanctionné par une note inférieure à 10 (même si l'exercice est fait correctement !).