Résumé de cours :
Semaine 5, du 30 septembre au 4 octobre.

1 Relations d'équivalence (suite et fin)

Définition. Une partition $\mathcal{P}$ de E est une partie de $\mathcal{P}(E)$ telle que :
- pour tout $A, B \in \mathcal{P}$, $A \neq B \implies A \cap B = \emptyset$,
- pour tout $A \in \mathcal{P}$, $A \neq \emptyset$,
- et $\bigcup_{A \in \mathcal{P}} A = E$.

Théorème. Si R est une relation d'équivalence sur E, son ensemble quotient E/R est une partition de E. Réciproquement, si $\mathcal{P}$ est une partition de E, il existe une unique relation d'équivalence R sur E telle que $\mathcal{P} = E/R$: Elle est définie par $\forall x, y \in E,\ \ [xRy \iff (\exists C \in \mathcal{P},\ \ x, y \in C)]$. En résumé, la donnée d'une relation d'équivalence sur E est équivalente à la donnée d'une partition de E.
Il faut savoir démontrer la première phrase.

2 Ordres dans $\mathbb{N}$

2.1 L'ordre naturel et la soustraction

L'ordre naturel : Pour tout $n, m \in \mathbb{N}$,
on convient que $n \leq m$ si et seulement si $\exists k \in \mathbb{N},\ \ m = n + k$.
Dans ce cas, k est unique. On le note $k = m - n$.
La relation binaire $\leq$ ainsi définie est un ordre total sur $\mathbb{N}$.

Définition. On vient de montrer que, si n est un entier naturel,
pour tout $h, k \in \mathbb{N}$, $n + h = n + k$ implique $h = k$. On dit que n est régulier.
Il faut savoir le démontrer.

Propriété. Soit $m, n \in \mathbb{N}$. Si $m < n$, alors $m + 1 \leq n$.

2.2 Multiplication dans $\mathbb{N}$ et relation de divisibilité

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

Propriétés de la multiplication :
- 0 est absorbant : $\forall m \in \mathbb{N},\ \ m \times 0 = 0 \times m = 0$.
- 1 est neutre : $\forall m \in \mathbb{N},\ \ m \times 1 = 1 \times m = m$.
- Distributivité de la multiplication par rapport à l'addition :
  $\forall n, m, p \in \mathbb{N},\ \ n(m + p) = (nm) + (np) = nm + np$: les dernières parenthèses sont inutiles si l'on convient que la multiplication est prioritaire devant l'addition.
- Associativité : $\forall n, m, k \in \mathbb{N},\ \ (n \times m) \times k = n \times (m \times k)$.

— Commutativité : $\forall n, m \in \mathbb{N},\ \ n \times m = m \times n$.

La relation d'ordre est compatible avec la multiplication :
Pour tout $a, b, c, d \in \mathbb{N}$, si $a \leq b$ et $c \leq d$, alors $ac \leq bd$.

Propriété. Soit $n, k \in \mathbb{N}$.
Si $nk = 0$, alors $n = 0$ ou $k = 0$.
Si $nk = 1$, alors $n = k = 1$.

Définition. Soit $n, m \in \mathbb{N}$. On dit que n divise m, que n est un diviseur de m, ou encore que m est un multiple de n si et seulement si il existe $k \in \mathbb{N}$ tel que $m = kn$. On note $n|m$.

Remarque. Tout entier divise 0 mais 0 ne divise que lui-même.

Définition. un nombre premier est un entier n supérieur à 2 dont les seuls diviseurs sont 1 et n.

Propriété. La relation de divisibilité est une relation d'ordre partiel sur $\mathbb{N}$.
Il faut savoir le démontrer.

2.3 Maximum et minimum dans $\mathbb{N}$

Propriété. Toute partie non vide et majorée de $\mathbb{N}$ possède un maximum.
Il faut savoir le démontrer.

Propriété. Soit $a, b \in \mathbb{N}$ avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$ et $0 \leq r < b$. On dit que q et r sont le quotient et le reste de la division euclidienne de a par b.
Il faut savoir le démontrer.

Propriété. Toute partie non vide de $\mathbb{N}$ possède un minimum.
Il faut savoir le démontrer.

Remarque. Un ensemble ordonné dont toute partie non vide possède un plus petit élément est appelé un ensemble bien ordonné.

Principe de la descente infinie : pour montrer que "$\forall n \in \mathbb{N},\ \ R(n)$", une alternative à la récurrence est de raisonner par l'absurde en supposant qu'il existe $n \in \mathbb{N}$ tel que $\neg[R(n)]$. Ainsi, l'ensemble $F = \{n \in \mathbb{N} / \neg R(n)\}$ possède un minimum n_0. On peut parfois aboutir à une contradiction en construisant un entier vérifiant $m < n_0$ et $m \in F$.

3 Axiome du choix

En voici deux énoncés équivalents.

— Pour tout ensemble I, pour toute famille $(E_i)_{i \in I}$ d'ensembles tous non vides, il existe une famille $(x_i)_{i \in I}$ telle que, pour tout $i \in I$, $x_i \in E_i$.
— Pour tout ensemble E, pour toute relation d'équivalence sur E, il existe un ensemble R tel que l'intersection de R avec chaque classe d'équivalence est un singleton.

4 L'art de la démonstration

La structure d'une démonstration se construit avant tout en fonction de la structure de la propriété à démontrer. En conséquence, on regarde d'abord la cible à atteindre et seulement lorsque c'est nécessaire les hypothèses dont on dispose pour y parvenir. On ne sait pas a priori sous quelles formes ces hypothèses seront utilisées.

4.1 Démontrer une disjonction

Pour montrer $P \vee Q$, on peut supposer que P est fausse et démontrer Q, ou bien supposer que Q est fausse et montrer P.

4.2 Démonstration par disjonction de cas

Pour démontrer une propriété dépendant de certains paramètres, on peut être amené à étudier plusieurs cas selon les valeurs de ces paramètres. Il importe que la réunion des différents cas étudiés recouvre toutes les valeurs possibles des paramètres.

4.3 Résoudre une équation

Définition. Si P est un prédicat sur un ensemble E, "résoudre l'équation P(x), en l'inconnue $x \in E$", c'est calculer $\{x \in E / P(x)\}$ qu'on appelle alors l'ensemble des solutions de l'équation.
"calculer" signifie "donner l'ensemble des solutions sous la forme la plus simple possible".

Remarque. La plupart des équations sont de la forme "$f(x) = g(x)$", où f et g sont deux applications de E dans un autre ensemble F.
Lorsque $F = \mathbb{R}$, on rencontre parfois des équations de la forme "$f(x) \leq g(x)$", ou "$f(x) < g(x)$". Dans ce cas, on parle plutôt d'*inéquations*.

Méthode :

- Précisez d'abord pour quelles valeurs $x \in E$ l'équation a bien un sens. Par exemple, pour une équation de la forme "$f(x) = g(x)$", il faudra d'abord rechercher les domaines de défnition de f et de g.
- Autant que possible, raisonnez par équivalence comme dans l'exemple précédent.
  Cependant le fait de raisonner par équivalence impose parfois trop de lourdeur à la rédaction. Lorsqu'on choisit de raisonner par implication, après avoir montré que $P(x) \Longrightarrow x \in S$, pour un certaine partie S de E, il restera à rechercher quels sont les éléments de S qui sont effectivement solutions.

4.4 Implication

Pour montrer $[P \Longrightarrow Q]$, on suppose que P est vraie (hypothèse supplémentaire) et on démontre Q.

Raisonnement par contraposition : l'implication $P \Longrightarrow Q$ est logiquement équivalente à $(\neg Q) \Longrightarrow (\neg P)$, qui est appelée sa contraposée. Ainsi, pour démontrer $P \Longrightarrow Q$, on peut raisonner par contraposition, c'est-à-dire démontrer $(\neg Q) \Longrightarrow (\neg P)$: on suppose que Q est fausse et on démontre que P est fausse.

Le raisonnement par l'absurde : cela consiste à supposer que R est fausse et à aboutir à une contradiction, souvent de la forme $S \wedge (\neg S)$.

Pour montrer que $[P \Longleftrightarrow Q]$, on montre souvent $[P \Longrightarrow Q]$ puis la réciproque $[Q \Longrightarrow P]$.
Dans des cas simples, on peut raisonner par une succession d'équivalences.

Pour montrer que les propriétés $P_1, \ldots, P_k$ sont équivalentes, on peut se contenter de montrer le cycle d'implications $P_1 \Longrightarrow P_2 \Longrightarrow \cdots \Longrightarrow P_k \Longrightarrow P_1$. Mais la liste $P_1, \ldots, P_k$ n'est pas toujours donnée dans l'ordre idéal. Il convient donc parfois de la réordonner.

4.5 Quantificateurs

Pour montrer que $[\forall x \in E,\ P(x)]$, le plus souvent, on prend x quelconque dans E,
en écrivant "soit $x \in E$", puis on démontre $P(x)$.

Pour montrer que $[\exists x \in E,\ P(x)]$, la méthode directe consiste à construire un élément x de E satisfaisant $P(x)$.
On peut aussi raisonner par l'absurde, en supposant que $[\forall x \in E,\ \neg(P(x))]$ et en recherchant une contradiction. Il faut cependant que cette nouvelle hypothèse se marie bien avec les autres hypothèses.

Pour montrer que $\neg(\forall x \in E,\ P(x))$, on peut rechercher un x dans E tel que $P(x)$ est fausse. Dans ce contexte, x est appelé un contre-exemple du prédicat $P(x)$.

4.6 Existence et unicité

Comment montrer une propriété de la forme $[\exists! x \in E,\ P(x)]$?

Dans de nombreux exercices et problèmes, l'énoncé d'une telle propriété se présente sous la forme : "montrer qu'il existe $x \in E$ tel que $P(x)$, puis montrer que x est unique".
Sur le plan ontologique, tout objet mathématique est unique, mais ce n'est pas du tout ce qui est demandé par l'énoncé. La propriété "x est unique" dépend de P.
En mathématiques, l'unicité est toujours prononcée relativement à un prédicat. Par exemple, 2 est l'unique entier premier et pair, mais 2 n'est pas l'unique entier pair inférieur à 10.

Pour montrer qu'il existe un unique $x \in E$ tel que $P(x)$, il est souvent préférable de séparer l'existence et l'unicité. Pour l'unicité, il faut montrer que $\{x \in E / P(x)\}$ ne possède pas deux éléments distincts, par exemple en supposant qu'il existe $x, y \in E$ vérifiant $P(x)$ et $P(y)$ et en prouvant que $x = y$.

Mais il y a d'autres méthodes :
- On peut montrer que $\{x \in E / P(x)\}$ est un singleton.
- On peut résoudre l'équation "$P(x)$" en l'inconnue x pour montrer qu'elle admet une seule solution.
- On peut raisonner par analyse-synthèse :

4.7 Démonstration par analyse-synthèse

Ce mode de raisonnement est envisageable lorsque la propriété à démontrer est de la forme $[\exists x \in E,\ P(x)]$. Il se décompose en deux parties :
◇ **L'analyse :** on suppose qu'il existe $x \in E$ tel que $P(x)$.
C'est a priori très étrange, car on suppose justement ce qu'il faut démontrer !
A partir du fait que x vérifie $x \in E$ et $P(x)$, on cherche à préciser quelles sont les valeurs possibles pour x,.
Il est fréquent que l'analyse conduise à une seule valeur possible pour x.
◇ **La synthèse :** Parmi ces différentes valeurs possibles, on en recherche une qui vérifie $P(x)$.

4.8 Démonstrations par récurrence

Principe de récurrence :
Soit $n_0 \in \mathbb{N}^*$. Soit $R(n)$ un prédicat défini pour tout entier $n \geq n_0$.
Si $R(n_0)$ est vraie et si pour tout $n \geq n_0$, $R(n)$ implique $R(n+1)$,
alors pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, $R(n)$ est vraie.

Principe de récurrence ascendante finie : Soit $n, m \in \mathbb{N}$ avec $n \leq m$.
Soit $R(k)$ un prédicat défini pour $k \in [\![n, m]\!]$.
Si $R(n)$ est vraie et si pour tout $k \in [\![n, m-1]\!]$, $R(k)$ implique $R(k+1)$,

alors $R(k)$ est vraie pour tout $k \in [\![n, m]\!]$.

Principe de récurrence descendante finie : Soit $n, m \in \mathbb{N}$ avec $n \leq m$.
Soit $R(k)$ un prédicat défini pour $k \in [\![n, m]\!]$.
Si $R(m)$ est vraie et si pour tout $k \in [\![n+1, m]\!]$, $R(k)$ implique $R(k-1)$,
alors $R(k)$ est vraie pour tout $k \in [\![n, m]\!]$.

Principe de récurrence forte :
Soit $n_0 \in \mathbb{N}$. Soit $R(n)$ un prédicat défini pour tout entier $n \geq n_0$.
Si $R(n_0)$ est vraie et si pour tout $n \geq n_0$, $[\forall k \in \{n_0, \dots, n\}, R(k)]$ implique $R(n+1)$,
alors pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, $R(n)$ est vraie.

Principe de récurrence double :
Soit $n_0 \in \mathbb{N}$. Soit $R(n)$ un prédicat défini pour tout entier $n \geq n_0$.
Si $R(n_0)$ et $R(n_0+1)$ sont vraies et si
pour tout $n \geq n_0$, $[R(n) \ \wedge \ R(n+1)]$ implique $R(n+2)$,
alors pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, $R(n)$ est vraie.

5 $\mathbb{Z}$

5.1 Construction de $\mathbb{Z}$

Définition. $\mathbb{Z} = \mathbb{N}^2/R$, où R est la relation d'équivalence suivante sur $\mathbb{N}^2$:
$\forall a, b, c, d \in \mathbb{N}, \ (a, b)R(c, d) \iff a + d = b + c$.
Si $\overline{(a, b)}, \overline{(c, d)} \in \mathbb{Z}$, on pose $\overline{(a, b)} + \overline{(c, d)} \stackrel{\Delta}{=} \overline{(a + c, b + d)}$
et $\overline{(a, b)} \times \overline{(c, d)} \stackrel{\Delta}{=} \overline{(ac + bd, ad + bc)}$.

5.2 L'anneau $\mathbb{Z}$

Propriété. L'addition sur $\mathbb{Z}$ vérifie les propriétés suivantes :
- $0 \stackrel{\Delta}{=} \overline{(0, 0)}$ est neutre : $\forall m \in \mathbb{Z}, \ m + 0 = 0 + m = m$.
- Associativité : $\forall n, m, k \in \mathbb{Z}, \ (n + m) + k = n + (m + k)$.
- Commutativité : $\forall n, m \in \mathbb{Z}, \ n + m = m + n$.
- Tout élément possède un symétrique : $\forall n \in \mathbb{Z}, \ \exists m \in \mathbb{Z}, \ n + m = 0$.

On résume ces propriétés en disant que $(\mathbb{Z}, +)$ est un groupe commutatif.

Propriété. La multiplication sur $\mathbb{Z}$ vérifie les propriétés suivantes :
- $1 \stackrel{\Delta}{=} \overline{(1, 0)}$ est neutre : $\forall m \in \mathbb{Z}, \ m \times 1 = 1 \times m = m$.
- Distributivité de la multiplication par rapport à l'addition :
  $\forall n, m, p \in \mathbb{Z}, \ n(m + p) = nm + np$.
- Associativité : $\forall n, m, k \in \mathbb{Z}, \ (n \times m) \times k = n \times (m \times k)$.
- Commutativité : $\forall n, m \in \mathbb{Z}, \ n \times m = m \times n$.

On résume ces propriétés et le fait que $(\mathbb{Z}, +)$ est un groupe commutatif en disant que $(\mathbb{Z}, +, \times)$ est un anneau commutatif.

5.3 L'ordre de $\mathbb{Z}$

Compatibilité de la relation d'ordre avec l'addition :
$\forall x, y, x', y' \in \mathbb{Z}, \ [x \leq y] \wedge [x' \leq y'] \Longrightarrow x + x' \leq y + y'$.

Identification de $\mathbb{N}$ avec une partie de $\mathbb{Z}$: on identifie $n \in \mathbb{N}$ avec $\overline{(n, 0)}$.

Règle des signes :
- $\forall n \in \mathbb{Z},\ n \geq 0 \iff n \in \mathbb{N}$.
- $\forall n, m \in \mathbb{Z},\ ([n \geq 0] \wedge [m \geq 0]) \implies nm \geq 0$.
- $\forall n \in \mathbb{Z},\ n \geq 0 \iff -n \leq 0$.
- $\forall x, y, a \in \mathbb{Z},\ \begin{cases} \text{si } a \geq 0,\ x \leq y \implies ax \leq ay, \\ \text{si } a \leq 0,\ x \leq y \implies ax \geq ay. \end{cases}$

Propriété. Toute partie non vide majorée de $\mathbb{Z}$ possède un maximum.
Toute partie non vide minorée de $\mathbb{Z}$ possède un minimum.

Définition. Soit $n \in \mathbb{Z}$.
Le signe de n au sens large est
- 1 ou bien "positif" lorsque $n \geq 0$,
- -1 ou bien "négatif" lorsque $n \leq 0$.

Le signe de n au sens strict est
- 1 ou bien "strictement positif" lorsque $n > 0$,
- 0 ou bien "nul" lorsque $n = 0$,
- -1 ou bien "strictement négatif" lorsque $n < 0$.

Définition. Pour tout $n \in \mathbb{Z}$, on note $|n| = \max\{-n, n\}$.

Propriété. Pour tout $n \in \mathbb{Z}$, $n \leq |n|$, avec égalité si et seulement si $n \geq 0$. De plus $|n|^2 = n^2$.

Propriété. $\forall n, m \in \mathbb{Z},\ |nm| = |n||m|$.

Propriété. $\mathbb{Z}$ est un anneau intègre, c'est-à-dire que, pour tout $n, m \in \mathbb{Z}$,
$nm = 0 \implies [(n = 0) \vee (m = 0)]$.

Propriété. Soit $n, m \in \mathbb{Z}^2$. $nm \geq 0$ si et seulement si n et m sont de même signe au sens large.

Propriété. Soit $a, b, n \in \mathbb{Z}$ tels que $an \leq bn$. Si $n > 0$ alors $a \leq b$ et si $n < 0$, alors $a \geq b$.

Inégalité triangulaire : $\forall n, m \in \mathbb{Z},\ |n+m| \leq |n| + |m|$, avec égalité si et seulement si n et m sont de même signe.
Il faut savoir le démontrer.