Résumé de cours :
Semaine 7, du 16 au 20 octobre.

1 $\mathbb{Z}$ (suite)

1.1 PPCM

Définition. Soit $(a,b) \in \mathbb{Z}^2$. $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc il existe un unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. On dit que m est un PPCM de a et b et on note $m = a \vee b$.

Propriété. Soit $(a,b) \in \mathbb{Z}^2$. $a \vee b = \sup_{|}\{|a|, |b|\}$.

Remarque. Lorsque a et b sont des entiers relatifs non nuls, $a \vee b = \min_{\leq}\{k \in \mathbb{N}^* \ / \ a|k \text{ et } b|k\}$.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \ldots, a_k \in \mathbb{Z}$, on dit que m est le PPCM de $a_1, \ldots, a_k$ si et seulement si $m \in \mathbb{N}$ et $m\mathbb{Z} = a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z}$. Alors $m = \sup_{|}\{a_1, \ldots, a_k\}$.
Si B est une partie quelconque de $\mathbb{Z}$, on dit que m est le PPCM de B si et seulement si $m \in \mathbb{N}$ et $m\mathbb{Z} = \bigcap_{b \in B} b\mathbb{Z}$. Alors $m = \sup_{|}(B)$.

Remarque. Dans ce contexte, on convient que si $B = \emptyset$, $\bigcap_{b \in B} b\mathbb{Z} = \mathbb{Z}$, donc 1 est le PPCM de $\emptyset$.
Ainsi, toute partie de $\mathbb{N}$ possède une borne supérieure et une borne inférieure pour la relation d'ordre de divisibilité. On dit que l'ensemble ordonné $(\mathbb{N}, \ | \ )$ est un treillis complet.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \ldots, a_k \in \mathbb{Z}$ et $h \in \{1, \ldots, k\}$.
- Commutativité du PPCM :
  $PPCM(a_1, \ldots, a_k)$ ne dépend pas de l'ordre de $a_1, \ldots, a_k$.
- Associativité du PPCM :
  $PPCM(a_1, \ldots, a_k) = PPCM(a_1, \ldots, a_h) \ \vee \ PPCM(a_{h+1}, \ldots, a_k)$.
- Distributivité de la multiplication par rapport au PPCM :
  pour tout $\alpha \in \mathbb{Z}$, $PPCM(\alpha a_1, \ldots, \alpha a_k) = |\alpha| PPCM(a_1, \ldots, a_k)$.

1.2 Les théorèmes de l'arithmétique

Théorème de *Bézout*. Soit $(a,b) \in \mathbb{Z}^2$.
a et b sont premiers entre eux si et seulement si : $\exists (u,v) \in \mathbb{Z}^2 \ \ ua + vb = 1$.
Il faut savoir le démontrer.

Théorème de Bézout (généralisation). Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \ldots, a_n \in \mathbb{Z}$.
$a_1, \ldots, a_n$ sont globalement premiers entre eux si et seulement si :
$\exists u_1, \ldots, u_n \in \mathbb{Z} \ , \ \ u_1a_1 + \cdots + u_na_n = 1$.

Propriété. Soit $(a,b) \in \mathbb{Z}^2$. Posons $d = a \wedge b$.
Alors il existe $(a', b') \in \mathbb{Z}^2$, avec a' et b' premiers entre eux, tel que $a = a'd$ et $b = b'd$.

Théorème de *Gauss*. Soit $(a,b,c) \in \mathbb{Z}^3$. Si $a|bc$ avec a et b premiers entre eux, alors $a|c$.
Il faut savoir le démontrer.

Corollaire. Soit $p, a, b \in \mathbb{Z}$. Si $p \mid ab$ et si p est premier, alors $p \mid a$ ou $p \mid b$.

Corollaire. Soit $(a, b, c) \in \mathbb{Z}^3$, $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{Z}$.
◇ Si $a \wedge b = a \wedge c = 1$, alors $a \wedge bc = 1$.
◇ On en déduit que, si $a \wedge b = 1$, $\forall (k, l) \in (\mathbb{N}^*)^2 \;\; a^k \wedge b^l = 1$.
◇ Si $a|b$, $c|b$ et $a \wedge c = 1$ alors $ac|b$. Par récurrence, on en déduit que
si pour tout $i \in \{1, \dots, n\}$, $a_i|b$ et si $i \neq j \Longrightarrow a_i \wedge a_j = 1$, alors $a_1 \times \cdots \times a_n \mid b$.
◇ $|ab| = (a \wedge b)(a \vee b)$. En particulier, $a \wedge b = 1 \Longrightarrow a \vee b = |ab|$.
Il faut savoir le démontrer.

Théorème fondamental de l'arithmétique. Pour tout $a \in \mathbb{N}^*$, il existe une unique famille $(\nu_p)_{p \in \mathbb{P}} \in \mathbb{N}^{(\mathbb{P})}$ (i.e telle que $\{p \in \mathbb{P} \;/\; \nu_p \neq 0\}$ est fini) telle que $a = \prod_{p \in \mathbb{P}} p^{\nu_p}$.
C'est la décomposition de a en facteurs premiers. ν_p s'appelle la valuation p-adique de a.
Il faut savoir le démontrer.

Propriété. si $a = \prod_{p \in \mathbb{P}} p^{\nu_p}$ et $b = \prod_{p \in \mathbb{P}} p^{\mu_p}$, Alors $a \mid b \Longleftrightarrow [\forall p \in \mathbb{P}, \;\; \nu_p \leq \mu_p]$.
De plus, $a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(\nu_p, \mu_p)}$ et $a \vee b = \prod_{p \in \mathbb{P}} p^{\max(\nu_p, \mu_p)}$.

Lemme d'Euclide. Soient $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$. Notons q et r les quotient et reste de la division euclidienne de a par b. Alors $a \wedge b = b \wedge r$.

Algorithme d'Euclide. Soit $a_0, a_1 \in \mathbb{N}^*$ avec $a_0 > a_1$.
Pour $i \geq 1$, tant que $a_i \neq 0$, on note a_{i+1} le reste de la division euclidienne de a_{i-1} par a_i.
On définit ainsi une suite strictement décroissante d'entiers naturels $(a_i)_{0 \leq i \leq N}$ telle que $a_N = 0$.
Alors $a_0 \wedge a_1 = a_{N-1}$.
De plus, lorsque $a_0 \wedge a_1 = 1$, cet algorithme permet de calculer des entier s_0 et t_0 tels que $1 = s_0 a_0 + t_0 a_1$.
À connaître précisément.

> **Exercice.** Soit $a, b, c \in \mathbb{Z}$ avec a et b non nuls.
> Résoudre l'équation de Bézout (B) : $au + bv = c$ en l'inconnue $(u, v) \in \mathbb{Z}^2$.
> À connaître.

2 $\mathbb{Q}$

Définition. On définit une relation binaire R sur $\mathbb{Z} \times \mathbb{Z}^*$ par $(a, b) R (c, d) \Longleftrightarrow ad = bc$. C'est une relation d'équivalence. On pose $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/R$.
Pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, on note $\frac{a}{b} = \overline{(a, b)}$.
Pour l'écriture $\frac{a}{b}$, on dit que a est son numérateur et que b est son dénominateur.
Pour tout $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$, on pose $\frac{a}{b} \times \frac{c}{d} \triangleq \frac{ac}{bd}$ et $\frac{a}{b} + \frac{c}{d} \triangleq \frac{ad + cb}{bd}$.
On définit ainsi une addition et une multiplication sur $\mathbb{Q}$.

Propriété. $(\mathbb{Q}, +, \times)$ est un corps, c'est-à-dire que
— $(\mathbb{Q}, +, \times)$ est un anneau,
— $\mathbb{Q}$ n'est pas réduit à $\{0\}$ (on note $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$),
— $\mathbb{Q}$ est commutatif,
— tout élément non nul de $\mathbb{Q}$ est inversible : $\forall x \in \mathbb{Q}^*, \;\; \exists y \in \mathbb{Q}^*, \;\; xy = 1$.

Propriété. Comme tout corps, $\mathbb{Q}$ est intègre, c'est-à-dire que, pour tout $x, y \in \mathbb{Q}$,
$xy = 0 \Longrightarrow [(x = 0) \vee (y = 0)]$.
La démonstration dans un corps quelconque est à connaître.

Propriété. L'application $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Q} \\ n & \longmapsto & \frac{n}{1} \end{array}$ permet d'identifier $\mathbb{Z}$ avec une partie de $\mathbb{Q}$.
On parvient à prolonger l'ordre de $\mathbb{Z}$ en un ordre sur $\mathbb{Q}$, qui reste compatible avec l'addition et qui vérifie la règle des signes pour le produit.
On prolonge aussi sur $\mathbb{Q}$ la notion de valeur absolue ainsi que ses propriétés vues dans $\mathbb{Z}$.

Propriété. Pour tout $x \in \mathbb{Q}$, il existe un unique couple (a, b) tel que $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, tels que a et b sont premiers entre eux. On dit alors que $\frac{a}{b}$ est la forme irréductible de x.
Démonstration à connaître.

Exercice. Montrer que $\sqrt{2}$ est irrationnel.
A connaître.

$\mathbb{Q}$ est archimédien :
Soit x et y deux rationnels strictement positifs. Alors il existe $n \in \mathbb{N}$ tel que $x < ny$.

3 $\mathbb{R}$

3.1 Corps totalement ordonnés

Définition. Soit $(K, +, \times)$ un corps muni d'une relation d'ordre $\preceq$.
On dit que $(K, +, \times, \preceq)$ est un corps ordonné si et seulement si
- *Compatibilité avec l'addition* : $\forall x, y, z \in K,\ \ [x \preceq y] \Longrightarrow [x + z \preceq y + z]$.
- *Compatibilité avec le produit, règle des signes* :
  $\forall x, y \in K,\ \ [0 \preceq x] \wedge [0 \preceq y] \Longrightarrow [0 \preceq xy]$.

3.2 Une caractérisation de $\mathbb{R}$.

Caractérisation de $\mathbb{R}$: (admise)
Il existe au moins un corps K totalement ordonné dans lequel toute partie non vide majorée admet une borne supérieure.
De plus si K' est un autre corps totalement ordonné dans lequel toute partie non vide majorée admet une borne supérieure, il existe une bijection f de K dans K' telle que f est un morphisme de corps ordonnés, c'est-à-dire :
- $\forall x, y \in K,\ \ x \leq y \Longrightarrow f(x) \leq f(y)$,
- $\forall x, y \in K,\ \ f(x + y) = f(x) + f(y)$,
- $\forall x, y \in K,\ \ f(xy) = f(x)f(y)$,
- $f(1_K) = 1_{K'}$.

Cela signifie que, quitte à renommer x en $f(x)$, K et K' sont égaux, tant que dans K et K' on se contente d'utiliser leurs structures de corps totalement ordonnés.
Ainsi, à un morphisme bijectif près, il existe un unique corps totalement ordonné dans lequel toute partie non vide majorée admet une borne supérieure. Il est noté $\mathbb{R}$ et ses éléments sont appelés les réels.
Il existe un morphisme injectif de corps ordonné de $\mathbb{Q}$ dans $\mathbb{R}$, qui permet d'identifier $\mathbb{Q}$ avec une partie de $\mathbb{R}$.

3.3 La droite réelle achevée

Définition. On appelle droite réelle achevée l'ensemble $\overline{\mathbb{R}} \triangleq \mathbb{R} \cup \{-\infty, +\infty\}$, sur lequel l'ordre dans $\mathbb{R}$ est prolongé par les conditions : $\forall x \in \mathbb{R},\ \ -\infty < x < +\infty$.

Propriété. $(\overline{\mathbb{R}}, \leq)$ est un ensemble totalement ordonné dans lequel toute partie possède une borne inférieure et une borne supérieure. En particulier, toute partie A de $\mathbb{R}$ possède une borne supérieure dans $\overline{\mathbb{R}}$. De plus, $\sup(A) = +\infty \iff A$ non majorée et $\sup(A) = -\infty \iff A = \emptyset$.

3.4 Les intervalles

Définition.
- Pour tout $a, b \in \overline{\mathbb{R}}$, l'intervalle $]a, b[$ est défini par $]a, b[= \{x \in \mathbb{R} / a < x < b\}$.
- Pour tout $a, b \in \mathbb{R}$, l'intervalle $[a, b]$ est défini par $[a, b] = \{x \in \mathbb{R} / a \leq x \leq b\}$.
- Si $a \in \mathbb{R}$ et $b \in \overline{\mathbb{R}}$, les intervalles $[a, b[$ et $]b, a]$ sont définis par : $[a, b[= \{x \in \mathbb{R} / a \leq x < b\}$ et $]b, a] = \{x \in \mathbb{R} / b < x \leq a\}$.
- En particulier, $\mathbb{R} =]-\infty, +\infty[$ et $\emptyset =]0, -1[$ sont des intervalles.

Définition.
- Un intervalle est ouvert si et seulement si il est de la première forme $]a, b[$ avec $a, b \in \overline{\mathbb{R}}$.
- On dit qu'un intervalle est fermé si et seulement si son complémentaire est une réunion d'un ou deux d'intervalles ouverts.
- Ainsi, $[a, b]$ est fermé lorsque $a, b \in \mathbb{R}$, mais $[a, +\infty[$ est aussi fermé (avec $a \in \mathbb{R}$).
- $\emptyset$ et $\mathbb{R}$ sont à la fois ouverts et fermés.
- $[0, 1[$ n'est ni ouvert ni fermé. On dit qu'il est semi-ouvert ou semi-fermé.
- Les intervalles fermés bornés sont de la forme $[a, b]$ avec $a, b \in \mathbb{R}$. On les appelle aussi des segments.

Définition. Une partie A de $\mathbb{R}$ est convexe si et seulement si pour tout $a, b \in A$ avec $a < b$, $[a, b] \subset A$.

Théorème. Les parties convexes de $\mathbb{R}$ sont exactement ses intervalles.
Il faut savoir le démontrer.

Corollaire. Une intersection d'intervalles de $\mathbb{R}$ est un intervalle de $\mathbb{R}$.
Il faut savoir le démontrer.

Propriété. Pour une famille d'intervalles deux à deux non disjoints, l'union de ces intervalles est encore un intervalle.
Il faut savoir le démontrer.

3.5 la valeur absolue

Propriété. Le signe au sens large du produit de deux réels est égal au produit des signes de ces réels.

Définition. Pour tout $x \in \mathbb{R}$, on note $|x| = \max\{-x, x\}$.
$\forall x, y \in \mathbb{R}, \ |xy| = |x||y|$.

Inégalité triangulaire : $\forall x, y \in \mathbb{R}, \ |x + y| \leq |x| + |y|$, avec égalité si et seulement si x et y sont de même signe.

Corollaire de l'inégalité triangulaire : $\forall x, y \in \mathbb{R}, \ ||x| - |y|| \leq |x - y|$.
A savoir démontrer.

Formule : Pour tout $a, b \in \mathbb{R}$, $\min(a, b) = \dfrac{(a + b) - |a - b|}{2}$ et $\max(a, b) = \dfrac{(a + b) + |a - b|}{2}$.
Il faut savoir le démontrer.

Distance entre réels : Lorsque $x, y \in \mathbb{R}$, la quantité $d(x, y) = |x - y|$ est appelée la distance entre les deux réels x et y. Elle vérifie l'inégalité triangulaire : $d(x, z) \leq d(x, y) + d(y, z)$.

3.6 Propriétés usuelles des réels

Propriété. $\mathbb{R}$ **est archimédien :** Pour tout $a, b \in \mathbb{R}_+^*$, $\exists n \in \mathbb{N}$, $na > b$.

Définition. Soit A une partie de $\mathbb{R}$. On dit que A est dense dans $\mathbb{R}$ si et seulement si pour tout $x, y \in \mathbb{R}$ avec $x < y$, il existe $a \in A$ tel que $x \leq a \leq y$.

Propriété. A est dense dans $\mathbb{R}$ si et seulement si, pour tout $x \in \mathbb{R}$, il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A telle que $a_n \underset{n\to+\infty}{\longrightarrow} x$.
Il faut savoir le démontrer.

Propriété. $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans $\mathbb{R}$.
Il faut savoir le démontrer.

Définition. Soit $x \in \mathbb{R}$. On appelle partie entière de x le plus grand entier relatif inférieur ou égal à x. Elle est notée $\lfloor x \rfloor$. C'est l'unique entier n tel que $n \leq x < n + 1$.
On appelle partie entière supérieure de x le plus petit entier supérieur ou égal à x. Elle est notée $\lceil x \rceil$. C'est l'unique entier n tel que $n - 1 < x \leq n$.

Une inégalité très utile : Pour tout $x, y \in \mathbb{R}$, $|xy| \leq \dfrac{x^2 + y^2}{2}$.
A savoir établir.

4 Développement décimal

4.1 Développement décimal d'un entier naturel

Propriété. Si (x_n) une suite strictement croissante d'entiers naturels, on montre par récurrence que pour tout $n \in \mathbb{N}$, $x_n \geq n$.

Définition. Les chiffres en base 10 sont $0, 1, \ldots, 9$.

Théorème. Pour tout $n \in \mathbb{N}$, il existe une unique suite presque nulle de chiffres $(a_k)_{k\in\mathbb{N}} \in \{0, \ldots, 9\}^{(\mathbb{N})}$ telle que $n = \sum_{k\in\mathbb{N}} a_k 10^k$.

Remarque. On peut généraliser et développer en base a où a est un entier supérieur ou égal à 2.

CNS de divisibilité : Soit $n \in \mathbb{N}$, dont le développement décimal est noté $n = \sum_{k\in\mathbb{N}} a_k 10^k$. On note $s = \sum_{k\in\mathbb{N}} a_k$ la somme des chiffres de n.

- n est divisible par 2 si et seulement si $a_0 \in \{0, 2, 4, 6, 8\}$.
- n est divisible par 5 si et seulement si $a_0 \in \{0, 5\}$.
- n est divisible par 10 si et seulement si $a_0 = 0$.
- n est divisible par 3 si et seulement si $s \equiv 0$ [3].
- n est divisible par 9 si et seulement si $s \equiv 0$ [9].
- n est divisible par 11 si et seulement si $\sum_{k\in\mathbb{N}} (-1)^k a_k \equiv 0$ [11].

Il faut savoir le démontrer.

4.2 L'ensemble $\mathbb{D}$ des nombres décimaux

Définition. $\mathbb{D} = \left\{ \dfrac{n}{10^k} / n \in \mathbb{Z} \text{ et } k \in \mathbb{N} \right\}$. C'est une partie stricte de $\mathbb{Q}$ dont les éléments sont appelés les nombres décimaux.

Propriété. Soit $x \in \mathbb{Q}$. x est un nombre décimal si et seulement si son écriture irréductible est de la forme $x = \dfrac{p}{2^h 5^k}$, où $p \in \mathbb{Z}$ et $h, k \in \mathbb{N}$.

Remarque. $(\mathbb{D}, +, \times)$ est un anneau.

Propriété. $d \in \mathbb{D}$ si et seulement si il existe une famille presque nulle de chiffres indexée par $\mathbb{Z}$, $(a_k)_{k\in\mathbb{Z}} \in \{0, \dots, 9\}^{(\mathbb{Z})}$ telle que $d = \sum_{k\in\mathbb{Z}} a_k 10^k$.

4.3 Approximation d'un réel

Définition. Soit $x, \alpha \in \mathbb{R}$ et $\varepsilon \in \mathbb{R}_+^*$.
- On dit que α est une valeur approchée de x à ε près si et seulement si $d(x, \alpha) \leq \varepsilon$.
  On note alors $x = \alpha \pm \varepsilon$.
- On dit que α est une valeur approchée de x à ε près par défaut si et seulement si $\alpha \leq x \leq \alpha + \varepsilon$,
- On dit que α est une valeur approchée de x à ε près par excès si et seulement si $\alpha - \varepsilon \leq x \leq \alpha$.

Propriété. Soit $x \in \mathbb{R}$ et $p \in \mathbb{N}$. Posons $\alpha = \dfrac{\lfloor 10^p x \rfloor}{10^p}$. $\alpha \in \mathbb{D}$.
Alors α est une valeur approchée de x par défaut à 10^{-p} près,
et $\alpha + 10^{-p}$ est une valeur approchée de x par excès à 10^{-p} près.
Il faut savoir le démontrer.

Corollaire. $\mathbb{D}$ est dense dans $\mathbb{R}$.

4.4 Développement d'un réel en base quelconque

Notation. On fixe un entier naturel a supérieur ou égal à 2.

Propriété. Soit $(v_n)_{n\geq 1}$ une suite d'entiers telle que, pour tout $n \in \mathbb{N}^*$, $0 \leq v_n \leq a - 1$.
Pour tout $n \in \mathbb{N}$, posons $x_n = \sum_{k=1}^{n} v_k a^{-k}$. La suite (x_n) est croissante et majorée, donc elle converge vers une limite x que l'on notera $x = \sum_{n=1}^{+\infty} v_n a^{-n}$. Dans ces conditions, on dit que $(v_n)_{n\geq 1}$ est un développement de x en base a et on note $x = 0, \overline{v_1 v_2 \cdots v_n v_{n+1} \cdots}$.
De plus, $x \in [0, 1]$ et $[x = 1 \iff (\forall n \in \mathbb{N}^*,\ v_n = a - 1)]$.
Il faut savoir le démontrer.

Notation. Posons $\mathcal{V} = \{(v_n)_{n\geq 1} / \forall n \in \mathbb{N}^*\ v_n \in \mathbb{N} \cap [0, a[\text{ et } \forall N \in \mathbb{N}^*\ \exists n \geq N\ v_n \neq a - 1\}$. Ainsi, les éléments de $\mathcal{V}$ sont les suites de chiffres qui ne sont pas tous égaux à $a - 1$ à partir d'un certain rang.

Théorème. Tout réel de $[0, 1[$ admet un unique développement en base a dans $\mathcal{V}$.
Il faut savoir le démontrer.

Remarque. Soit $x \in \mathbb{R}_+$. On peut écrire $x = \lfloor x \rfloor + \{x\}$, où $\lfloor x \rfloor \in \mathbb{N}$ et où $\{x\} = x - \lfloor x \rfloor \in [0, 1[$ est la partie fractionnaire de x. On obtient le développement en base a du réel x en concaténant le développement en base a de l'entier $\lfloor x \rfloor$ avec celui du réel $\{x\} \in [0, 1[$.

On terminera ce paragraphe à la rentrée avec :
Théorème hors programme : caractérisation d'un rationnel. Soit $x \in [0, 1[$.
Notons $x = 0, \overline{v_1 \cdots v_n \cdots}$ le développement en base a de x.
x est un rationnel si et seulement si son développement en base a est périodique à partir d'un certain rang, c'est-à-dire si et seulement si il existe $N \in \mathbb{N}^*$ et $p \in \mathbb{N}^*$ tel que $\forall n > N,\ v_n = v_{n+p}$.
Il faut savoir le démontrer.