

Résumé de cours :

Semaine 6, du 6 au 10 octobre.

1 $\mathbb{Z}$

1.1 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 $\overline{(a, b)} + \overline{(c, d)} \triangleq \overline{(a + c, b + d)}$

et $\overline{(a, b)} \times \overline{(c, d)} \triangleq \overline{(ac + bd, ad + bc)}$.

1.2 L'anneau $\mathbb{Z}$

Propriété. L'addition sur $\mathbb{Z}$ vérifie les propriétés suivantes :

- $0 \triangleq \overline{(0, 0)}$ 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 :

- $1 \triangleq \overline{(1, 0)}$ 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.

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

Compatibilité de la relation d'ordre avec l'addition :

$$\forall x, y, x', y' \in \mathbb{Z}, [x \leq y] \wedge [x' \leq y'] \implies x + x' \leq y + y'.$$

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.

1.4 Les sous-groupes de $\mathbb{Z}$

Division euclidienne dans $\mathbb{Z}$: Pour tout $a, b \in \mathbb{Z}$ avec $b \neq 0$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$. q et r sont appelés les quotient et reste.

Définition. Une partie G de $\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ si et seulement si

- $G \neq \emptyset$,
- $\forall (x, y) \in G^2, x + y \in G$,
- $\forall x \in G, -x \in G$.

Propriété. Soit G un sous-groupe de $\mathbb{Z}$.

Pour tout $n \in \mathbb{Z}$ et $g \in G$, $ng \in G$.

Pour tout $n \in G$, $n\mathbb{Z} \subset G$.

Il faut savoir le démontrer.

Corollaire. Soit G un sous-groupe de $\mathbb{Z}$. Alors $\boxed{1 \in G \iff G = \mathbb{Z}}$.

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

Il faut savoir le démontrer.

Propriété. Une intersection de sous-groupes de $\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Il faut savoir le démontrer.

Définition. Soit B une partie de $\mathbb{Z}$. Le groupe engendré par B est l'intersection des sous-groupes de $\mathbb{Z}$ contenant B . C'est le plus petit sous-groupe contenant B . On le note $Gr(B)$.

Propriété. Soient B et C deux parties de $\mathbb{Z}$ telles que $C \subset B$. Alors $Gr(C) \subset Gr(B)$.

Propriété. $Gr(B) = \left\{ \sum_{i=1}^n a_i b_i / n \in \mathbb{N}, (a_1, \dots, a_n) \in \mathbb{Z}^n, (b_1, \dots, b_n) \in B^n \right\}$.

Il faut savoir le démontrer.

1.5 Divisibilité

Définition. Soit $n, m \in \mathbb{Z}$. $n|m$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $m = kn$.

Propriété. Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$. Alors b divise a si et seulement si le reste de la division euclidienne de a par b vaut 0.

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

Remarque. Si $n, m \in \mathbb{Z}$, n divise m si et seulement si $|n|$ divise $|m|$ dans $\mathbb{N}$.

Propriété. Soit $a, b, c \in \mathbb{Z}$.

- si $b|a$, alors pour tout $\alpha \in \mathbb{Z}$, $b|\alpha a$.
- Si $b|a$ et $b|c$, alors $b|(a+c)$.
- Si $b|a$ et $d|c$, alors $bd|ac$.
- si $b|a$, pour tout $p \in \mathbb{N}$, $b^p|a^p$.

Propriété. Soit $p \in \mathbb{N}$ et $b, a_1, \dots, a_p, c_1, \dots, c_p \in \mathbb{Z}$.

Si pour tout $i \in \{1, \dots, p\}$, $b|a_i$, alors $b|\sum_{i=1}^p c_i a_i$.

Propriété. Pour tout $(a, b) \in \mathbb{Z}^2$, $a|b \iff b\mathbb{Z} \subseteq a\mathbb{Z}$.

Propriété. La relation de divisibilité est réflexive et transitive.

Remarque. La relation de divisibilité n'est pas un ordre sur $\mathbb{Z}$ car $-1|1$ et $1|-1$.

Définition. Soit $a, b \in \mathbb{Z}$. On dit que a et b sont premiers entre eux (ou étrangers) si et seulement si les seuls diviseurs communs de a et b sont 1 et -1 .

Définition. Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \dots, a_n \in \mathbb{Z}$.

- $a_1, \dots, a_n$ sont deux à deux premiers entre eux si et seulement si, pour tout $i, j \in \{1, \dots, n\}$ avec $i \neq j$, a_i et a_j sont premiers entre eux.
- $a_1, \dots, a_n$ sont globalement premiers entre eux si et seulement si les seuls diviseurs communs de $a_1, \dots, a_n$ sont 1 et -1 .

Propriété. Si $p \in \mathbb{P}$ et $a \in \mathbb{Z}$, alors ou bien $p|a$, ou bien p et a sont premiers entre eux.

Propriété. Soit $p \in \mathbb{N} \setminus \{0, 1\}$. Les propriétés suivantes sont équivalentes :

1. p est premier.
2. p est premier avec tout entier qu'il ne divise pas.
3. p est premier avec tout nombre premier contenu dans $\llbracket 2, \sqrt{p} \rrbracket$.

Il faut savoir le démontrer.

le crible d'Ératosthène : pour dresser la liste ordonnée des nombres premiers inférieurs à n , initialement, on pose $L = \llbracket 2, n \rrbracket$ et on positionne un curseur sur 2. On supprime de L les multiples de 2, sauf 2, puis on déplace le curseur sur l'entier suivant de L : il s'agit de 3, car il n'a pas été supprimé. On supprime de L tous les multiples de 3, sauf 3, etc. Ainsi, à chaque itération, on déplace le curseur

sur le premier entier suivant qui est encore dans L et l'on supprime de L tous les multiples du curseur, sauf le curseur. On arrête l'algorithme dès que le curseur est strictement supérieur à $\sqrt{n}$.

Théorème. $\mathbb{P}$ est de cardinal infini.

Il faut savoir le démontrer.

1.6 Congruence

Définition. Relation de congruence : Soit $k \in \mathbb{Z}$. $\forall n, m \in \mathbb{Z}$, $n \equiv m [k] \iff k | (n - m)$.
C'est la relation de congruence modulo k , qui est une relation d'équivalence.

Propriété. Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$: il existe $r \in \{0, \dots, |b| - 1\}$ tel que $a \equiv r [b]$.
 r est le reste de la division euclidienne de a par b .

Notation. La classe d'équivalence de n modulo k est $\bar{n} = \{n + kh/h \in \mathbb{Z}\} \triangleq n + k\mathbb{Z}$.

Compatibilités de la congruence avec l'addition et la multiplication :

Pour tout $n, m, h, k \in \mathbb{Z}$,

- $n \equiv m [k] \implies h + n \equiv h + m [k]$ et
- $n \equiv m [k] \implies hn \equiv hm [k]$.

Corollaire : $\forall a, b, k \in \mathbb{Z}$, $\forall n \in \mathbb{N}$, $(a \equiv b [k] \implies a^n \equiv b^n [k])$.

Petit théorème de Fermat : (Admis pour le moment) Si $p \in \mathbb{P}$ et $a \in \mathbb{Z}$,
 $(a \not\equiv 0 [p]) \implies a^{p-1} \equiv 1 [p]$, donc dans tous les cas, $a^p \equiv a [p]$.

Définition. Soit $x_0 \in \mathbb{R}$. Pour tout $x, y \in \mathbb{R}$, on dit que x est congru à y modulo x_0 et on note $x \equiv y [x_0]$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $x - y = kx_0$. La relation de congruence modulo x_0 est une relation d'équivalence sur $\mathbb{R}$. Elle est compatible avec l'addition entre réels mais pas avec la multiplication entre réels.

1.7 PGCD

Définition. Soit $(a, b) \in \mathbb{Z}^2$. $a\mathbb{Z} + b\mathbb{Z}$ est le sous-groupe de $\mathbb{Z}$ engendré par $\{a, b\}$, donc il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On dit que d est le PGCD de a et b . On note $d = \text{PGCD}(a, b) = a \wedge b$.

Propriété. Pour la relation d'ordre de divisibilité dans $\mathbb{N}$, $a \wedge b = \inf_{|} \{|a|, |b|\}$.

Il faut savoir le démontrer.

Remarque. Lorsque a ou b est un entier relatif non nul, au sens de l'ordre naturel sur $\mathbb{N}$, $a \wedge b$ est aussi le plus grand diviseur commun de a et b .

Propriété. a et b sont premiers entre eux si et seulement si $a \wedge b = 1$.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in \mathbb{Z}$, on dit que d est le PGCD de $a_1, \dots, a_k$ si et seulement si $d \in \mathbb{N}$ et $d\mathbb{Z} = a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = \text{Gr}\{a_1, \dots, a_k\}$. Alors $d = \inf_{|} \{a_1, \dots, a_k\}$.

Si B est une partie quelconque de $\mathbb{Z}$, on dit que d est le PGCD de B si et seulement si $d \in \mathbb{N}$ et $d\mathbb{Z} = \text{Gr}(B)$. Alors $d = \inf_{|}(B)$.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in \mathbb{Z}$ et $h \in \{1, \dots, k\}$.

- Commutativité du PGCD :
 $\text{PGCD}(a_1, \dots, a_k)$ ne dépend pas de l'ordre de $a_1, \dots, a_k$.
- Associativité du PGCD :
 $\text{PGCD}(a_1, \dots, a_k) = \text{PGCD}(a_1, \dots, a_h) \wedge \text{PGCD}(a_{h+1}, \dots, a_k)$.
- Distributivité de la multiplication par rapport au PGCD : pour tout $\alpha \in \mathbb{Z}$,
 $\text{PGCD}(\alpha a_1, \dots, \alpha a_k) = |\alpha| \text{PGCD}(a_1, \dots, a_k)$.

Il faut savoir le démontrer.

1.8 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, $a \vee b = \min_{\leq} \{k \in \mathbb{N}^* \mid a|k \text{ et } b|k\}$.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in \mathbb{Z}$, on dit que m est le PPCM de $a_1, \dots, a_k$ si et seulement si $m \in \mathbb{N}$ et $m\mathbb{Z} = a_1\mathbb{Z} \cap \dots \cap a_k\mathbb{Z}$. Alors $m = \sup_{|} \{a_1, \dots, a_k\}$.

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 $k \in \mathbb{N}$, $a_1, \dots, a_k \in \mathbb{Z}$ et $h \in \{1, \dots, k\}$.

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

1.9 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 : $\exists (u, v) \in \mathbb{Z}^2 \quad ua + vb = 1$.

Il faut savoir le démontrer.

Théorème de Bézout (généralisation). Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \dots, a_n \in \mathbb{Z}$.

$a_1, \dots, a_n$ sont globalement premiers entre eux si et seulement si :

$\exists u_1, \dots, u_n \in \mathbb{Z} \quad u_1 a_1 + \dots + u_n a_n = 1$.

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 $a \wedge b = 1$, $\forall (k, l) \in (\mathbb{N}^*)^2 \quad a^k \wedge b^l = 1$.
- ◇ 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 $i \neq j \implies a_i \wedge a_j = 1$, alors $a_1 \times \dots \times a_n \mid b$.
- ◇ $|ab| = (a \wedge b)(a \vee b)$. En particulier, $a \wedge b = 1 \implies a \vee b = |ab|$.

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 $\{p \in \mathbb{P} \mid \nu_p \neq 0\}$ 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 $a \mid b \iff [\forall p \in \mathbb{P}, \nu_p \leq \mu_p]$.

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 $(a, b)R(c, d) \iff ad = bc$. 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 : $\forall x \in \mathbb{Q}^*, \exists y \in \mathbb{Q}^*, xy = 1$.