## Questions de cours

- ☐ Comme d'habitude, savoir citer toute définition, toute proposition du cours.
- ☐ Soit $p \in \mathbb{N}^*$. Déterminer une condition nécessaire et suffisante sur $n \in \mathbb{N}$ pour que l'application $f : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{C}^* \\ \overline{k} & \mapsto & e^{\frac{2ik\pi}{p}} \end{array}$ soit bien définie.
- ☐ Soit $n \in \mathbb{N}$. Soit $k \in \mathbb{Z}$. Montrer que $\overline{k}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $k$ et $n$ sont premiers entre eux.
- ☐ Soit $G$ un groupe fini de cardinal $p$. Montrer que si $p$ est un nombre premier, alors $G$ est cyclique.
- ☐ Montrer que $\overline{35}$ est inversible dans $\mathbb{Z}/51\mathbb{Z}$, puis déterminer son inverse.
- ☐ Résoudre le système $\begin{cases} x \equiv 5\ [17] \\ x \equiv 4\ [6]. \end{cases}$
- ☐ Soit $n \in \mathbb{N}^*$ un nombre dont la décomposition en facteurs premiers est donnée par $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Déterminer $\varphi(n)$.

---

# Chapitre 26 : Étude de $\mathbb{Z}/n\mathbb{Z}$

## I Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

### I.1 Définition

- $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence pour la relation de congruence modulo $n$.
- $\mathbb{Z}/n\mathbb{Z}$ est de cardinal $n$. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. La classe $\overline{k}$ représente l'ensemble des nombres entiers de reste égal à $k$ dans la division euclidienne par $n$.
- on munit $\mathbb{Z}/n\mathbb{Z}$ de la loi $+ : \overline{a} + \overline{b} = \overline{a+b}$. Alors $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

### I.2 Sous-groupe engendré par une partie

- si $A$ est une partie d'un groupe $G$, alors $\langle A \rangle = \bigcap_{\substack{H \text{ sous-groupe de } G \\ \text{contenant } A}} H$ est le sous-groupe de $G$ engendré par $A$. C'est le plus petit sous-groupe de $G$ contenant $A$.
- $A$ est une partie génératrice de $G$ si $\langle A \rangle = G$.
- si $a \in G$, alors $\langle a \rangle$ est le sous-groupe de $G$ engendré par le singleton $\{a\}$.
  Si le groupe $(G, \times)$ est muni d'une loi multiplicative, alors $\langle a \rangle = \{a^n, n \in \mathbb{Z}\}$.
  Si le groupe $(G, +)$ est muni d'une loi additive, alors $\langle a \rangle = \{na, n \in \mathbb{Z}\}$.
- les générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les $\overline{k}$ tels que $k$ et $n$ sont premiers entre eux.

### I.3 Groupes monogènes et groupes cycliques

- un groupe monogène est un groupe qui est engendré par un singleton. Un groupe cyclique est un groupe monogène et fini.
- $(\mathbb{Z},+)$ est un groupe monogène infini, $(\mathbb{Z}/n\mathbb{Z},+)$ et $(\mathbb{U}_n,\times)$ sont des groupes cycliques.
- tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$.
- tout groupe cyclique de cardinal $n$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

### I.4 Ordre d'un élément dans un groupe

- soit $(G,\times)$ un groupe d'élément neutre $e$. On dit que $a\in G$ est d'ordre fini s'il existe $n\in\mathbb{N}^*$ tel que $a^n=e$. Sinon, $a$ est d'ordre infini.
- si $a$ est d'ordre fini, l'ordre de $a$ est le plus petit entier naturel non nul $n$ tel que $a^n=e$.
- si $(G,+)$ un groupe d'élément neutre 0 et de loi additive, on remplace $a^n=e$ par $na=0$.
- l'ordre de $a$ est égal au cardinal du sous-groupe $\langle a\rangle$.
- si $d$ désigne l'ordre de $a$, alors $a^n=e$ si et seulement si $d$ divise $n$.
- dans un groupe fini, tout élément $a$ est d'ordre fini et son ordre divise le cardinal du groupe.

## II Anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$

### II.1 Structure d'anneau et groupe des inversibles

- on munit $\mathbb{Z}/n\mathbb{Z}$ de la loi $\times$ : $\overline{a}\times\overline{b}=\overline{ab}$. Alors $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un anneau commutatif.
- le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des $\overline{k}$ tels que $k$ et $n$ sont premiers entre eux.
- pour trouver l'inverse de $\overline{k}$ dans le groupe $(U(\mathbb{Z}/n\mathbb{Z}),\times)$, on recherche une relation de Bézout entre $k$ et $n$ à l'aide de l'algorithme d'Euclide.
- $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n$ est un nombre premier. Si $p$ est premier, on note parfois $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$.

### II.2 Théorème des restes chinois

- si $m$ et $n$ sont premiers entre eux, alors l'anneau $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$. Le groupe $U(\mathbb{Z}/mn\mathbb{Z})$ est isomorphe à $U(\mathbb{Z}/m\mathbb{Z})\times U(\mathbb{Z}/n\mathbb{Z})$.
- généralisation au cas de plusieurs facteurs.
- application à la résolution de systèmes de congruences.

### II.3 Indicatrice d'Euler

- pour tout $n\in\mathbb{N}^*$, $\varphi(n)=\text{Card}\{k\in[\![1,n]\!],k\wedge n=1\}$.
- le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est égal à $\varphi(n)$.
- le cardinal du groupe $(U(\mathbb{Z}/n\mathbb{Z}),\times)$ est égal à $\varphi(n)$.
- si $p$ est premier, alors $\varphi(p)=p-1$.
- si $p$ est premier et $k\in\mathbb{N}^*$, $\varphi(p^k)=p^k-p^{k-1}$.
- si $m$ et $n$ sont premiers entre eux, alors $\varphi(mn)=\varphi(m)\varphi(n)$.

- si $n$ est un nombre entier dont la décomposition en facteurs premiers est donnée par $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.
- théorème d'Euler : si $a$ et $n$ sont premiers entre eux, alors $a^{\varphi(n)} \equiv 1\ [n]$.
- petit théorème de Fermat : si $p$ est un nombre premier, alors pour tout $a$, $a^p \equiv a\ [p]$. Si $a$ et $p$ sont premiers entre eux, alors $a^{p-1} \equiv 1\ [p]$.