1.3 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $n \in \mathbb{N}^*$. On rappelle les définitions suivantes, cas particulier des définitions générales liées aux relations d'équivalence.

Définition 1.20 (Classe de congruence, représentant)**.**
- *Pour $a \in \mathbb{Z}$, on note $\overline{a}$ la classe de congruence de a modulo n, c'est-à-dire la classe d'équivalence de a pour la relation de congruence modulo n.*
- *Explicitement, $\overline{a} = a + n\mathbb{Z}$.*
- *Étant donné c une classe de congruence, tout élément $a \in c$ est appelé représentant de la classe c. On a alors $c = \overline{a}$.*

On rappelle que la congruence modulo n respecte la somme et le produit, c'est-à-dire :

$$\forall (a, a', b, b') \in \mathbb{Z}^4, \begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases} \implies \begin{cases} a + b \equiv a' + b'[n] \\ ab \equiv a'b'[n] \end{cases}$$

Cela permet de définir la somme et le produit directement sur les classes de congruence.

Définition 1.21 ($\mathbb{Z}/n\mathbb{Z}$ et ses lois)**.** *L'ensemble des classes de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$. Il peut être muni d'une somme et d'un produit, définis, pour $\overline{a}$ et $\overline{b}$ deux classes de $\mathbb{Z}/n\mathbb{Z}$, par*

- $\overline{a} + \overline{b} = \overline{a + b}$;
- $\overline{a} \cdot \overline{b} = \overline{ab}$.

En vertu de ce qui précède, ces définitions sont indépendantes du choix des représentants a et b des deux classes.

Exemple 1.22. *Décrire la table des lois de $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \{2, 3, 4\}$.*

Proposition 1.23 (Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$)**.**
- *$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien d'ordre n.*
- *L'application $\pi : \mathbb{Z} \mapsto \mathbb{Z}/n\mathbb{Z}$ définie par $\pi(a) = \overline{a}$ est un morphisme de groupe, et $Ker(\pi) = n\mathbb{Z}$.*

Proposition 1.24 (Générateurs de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Les propositions suivantes sont équivalentes:*

(i) $\mathbb{Z}/n\mathbb{Z} = \langle \overline{a} \rangle$

(ii) *il existe $k \in \mathbb{N}$ tel que $\overline{k}a = \overline{1}$*

(iii) $a \wedge n = 1$

Éléments de preuve. Montrer $(i) \iff (ii)$, qui est assez clair, et $(ii) \iff (iii)$ qui provient de Bezout. □

Proposition 1.25 (Définir un morphisme $\mathbb{Z}/n\mathbb{Z} \to G$)**.** *Soit $(G, \times)$ un groupe, et $f : \mathbb{Z} \to G$ un morphisme de groupe. Les propositions suivantes sont équivalentes:*

(i) il existe un morphisme $g : \mathbb{Z}/n\mathbb{Z} \to G$ *tel que* $f = g \circ \pi$*;*

(ii) $n\mathbb{Z} \subset Ker(f)$.

Éléments de preuve. Le sens direct est évident. Réciproquement (ii) donne la condition pour que la valeur de f soit la même pour tout représentant d'une classe de congruence, ce qui donne une façon naturelle de définir g. Le reste n'est que de la vérification facile. □

Proposition 1.26 (Comparaison de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$)**.** *Les groupes* $(\mathbb{Z}/n\mathbb{Z}, +)$ *et* $(\mathbb{U}_n, \times)$ *sont isomorphes.*

Éléments de preuve. Considérer $\mathbb{Z} \longrightarrow \mathbb{U}_n$ défini par $f(k) = e^{\frac{2\pi ik}{n}}$, puis passer au quotient. □

1.4 Groupes monogènes

Définition 1.27 (Groupe monogène)**.** *(i) Un groupe* G *est monogène s'il existe* $x \in G$ *tel que* $G = \langle x \rangle$.

(ii) Si G *est fini et monogène, on dit que* G *est un groupe cyclique.*

(iii) Un générateur d'un groupe monogène est un élément x *tel que* $G = \langle x \rangle$.

Exemple 1.28. *1.* $(\mathbb{Z}, +)$ *est monogène, engendré par 1 ou par -1. Ce sont les seuls générateurs possibles de* $\mathbb{Z}$.

2. Tous les sous-groupes de $\mathbb{Z}$ *sont monogènes. En effet, ils sont de la forme* $a\mathbb{Z} = \langle a \rangle = \langle -a \rangle$. *Ce sont les seuls éléments générateurs de* $a\mathbb{Z}$.

3. $(\mathbb{Z}/n\mathbb{Z}, +)$ *est monogène, ses éléments générateurs sont les* $\overline{k}$*, avec* $k \wedge n = 1$.

4. $(\mathbb{U}_n, \times)$ *est monogène. Ses générateurs sont les images par l'isomorphisme de la proposition 7.1.25 des générateurs de* $\mathbb{Z}/n\mathbb{Z}$*, à savoir* $e^{\frac{2\pi ik}{n}}$*, avec* $k \wedge n = 1$. *Ces éléments générateurs sont appelés racines nièmes primitives de l'unité.*

Proposition 1.29 (Description explicite d'un sous-groupe monogène)**.** *Soit* $(G, \times)$ *un groupe, et* $x \in G$. *Alors*

$$\langle x \rangle = \{x^k, k \in \mathbb{N}\} = Im(\varphi_x),$$

où $\varphi_x : \mathbb{Z} \mapsto G$ *est le morphisme défini par* $\varphi_x(k) = x^k$.

Théorème 1.30 (Structure des groupes monogènes)**.** *Tout groupe monogène* $\langle x \rangle$ *est isomorphe :*

- *soit à* $(\mathbb{Z}, +)$*, si* $Ker(\varphi_x) = \{0\}$*;*
- *soit à* $(\mathbb{Z}/n\mathbb{Z}, +)$*, si* $Ker(\varphi_x) = n\mathbb{Z}$*; dans ce cas,* $n = \min\{k \in \mathbb{N}^*, x^k = e\}$.

Éléments de preuve. Dans le cas 2, passer φ_x au quotient par la proposition 7.1.24 pour définir $\widetilde{\varphi}_x : \mathbb{Z}/n\mathbb{Z} \to G$. Vérifier que c'est un isomorphisme. □

Exercise 1.31. *1. Soit* $n \in \mathbb{N}$. *Déterminer tous les sous-groupes de* $\mathbb{Z}/n\mathbb{Z}$.

2. Montrer que les sous-groupes d'un groupe cyclique sont cycliques.