(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.

1.5 Ordre d'un élément

Définition 1.32 (Ordre d'un élément)**.** *Soit $(G, \times)$ un groupe, de neutre e, et $x \in G$. L'ordre de x est*

- *$ord(x) = +\infty$ si pour tout $n \in \mathbb{N}^*, x^n \neq e$;*
- *$ord(x) = \min\{n \in \mathbb{N}^* | x^n = e\}$ sinon.*

On dit que x admet un ordre fini si $ord(x) \neq +\infty$.

Exemple 1.33. *1. Dans $(\mathbb{Z}, +)$, $ord(1) = +\infty$*

2. Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, $ord(\overline{1}) = n$

3. Dans $(\mathbb{Z}/42\mathbb{Z}, +)$, $ord(\overline{12}) = 7$.

Proposition 1.34 (Résolution de $x^k = e$)**.** *Soit $(G, \times)$ un groupe de neutre e. Soit x un élément d'ordre fini n. Alors*

$$x^k = e \iff n \mid k.$$

Proposition 1.35 (Description de ord(x) par le groupe engendré)**.** *Soit $(G, \times)$ un groupe, et $x \in G$. Alors*

$$ord(x) = |\langle x \rangle|.$$

Éléments de preuve. Dans le cas où ord(x) est fini, égal à n, le théorème 7.1.29 donne $\langle x \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Passer au cardinal. □

Définition 1.36 (Ordre d'un groupe)**.** *L'ordre d'un groupe est son cardinal. C'est un élément de $\mathbb{N}^* \cup \{+\infty\}$.*

Corollaire 1.37. *Si G est un groupe fini, tout $x \in G$ admet un ordre fini.*

Éléments de preuve. Sinon, $\mathbb{Z} \simeq \langle x \rangle \subset G$. □

Exercise 1.38. *Soit G un groupe abélien fini et x et y deux éléments de G d'ordres respectifs a et b. On suppose que a et b sont premiers entre eux. Montrer que xy est d'ordre ab.*

Théorème 1.39 (Lagrange)**.** *Soit G un groupe fini, et $x \in G$. Alors $ord(x) \mid Card(G)$. Ainsi l'ordre d'un élément d'un groupe fini divise l'ordre de ce groupe.*

Éléments de preuve. La démonstration n'est exigible que dans le cas où G est abélien. Montrer que l'application $\varphi : g \mapsto xg$ est une bijection et en déduire que

$$\prod_{g \in G} g = \prod_{g \in G} (xg),$$

puis simplifier. □