(i) Si $f : G \to H$ et $g : H \to K$ sont deux morphismes de groupes, alors $g \circ f$ est aussi un morphisme de groupes.

(ii) Si $f : G \to H$ est un isomorphisme, alors $f^{-1} : H \to G$ est aussi un isomorphisme.

Éléments de preuve. Vérifications faciles pour la composée. Pour la réciproque, considérer $f^{-1}(f(f^{-1}(x)f^{-1}(y)))$. □

1.2 Sous-groupes

Définition 1.8 (Sous-groupe). *Soit $(G, \star)$ un groupe. Un sous-ensemble H de G est appelé* sous-groupe de G *si H est stable pour la loi de G et si la loi induite définit sur H une structure de groupe. Le neutre de H est alors nécessairement le même que celui de G.*

Théorème 1.9 (Caractérisation des sous-groupes). *Un sous-ensemble H d'un groupe $(G, \star)$ (de neutre e_G) est un sous-groupe de G si et seulement si :*

(i) H est non vide,

(ii) H est stable pour $* : \forall (x, y) \in H, x * y \in H$,

(iii) H est stable par prise de symétrique : $\forall x \in H, x^* \in H$.

Dans la pratique, pour montrer que H est non vide, on vérifie souvent que $e_G \in H$.

Théorème 1.10 (Caractérisation des sous-groupes, version condensée). *Un sous-ensemble H d'un groupe $(G, \star)$ (de neutre e_G) est un sous-groupe de G si et seulement si :*

(i) H est non vide,

(ii) $\forall (x, y) \in H^2, x * y^* \in H$.

On traduit cette dernière propriété dans les deux cas les plus fréquents :

- *pour un sous-groupe d'un groupe additif, la vérification de stabilité à faire est donc : $\forall (x, y) \in H^2, x - y \in H$;*
- *pour un sous-groupe d'un groupe multiplicatif, la vérification de stabilité à faire est donc : $\forall (x, y) \in H^2, xy^{-1} \in H$.*

Proposition 1.11 (Image directe et réciproque de sous-groupes par un homomorphisme). *Soit G et H deux groupes, et soit $f \in Hom(G, H)$ un morphisme de groupes.*

(i) Soit G' un sous-groupe de G. Alors $f(G')$ est un sous-groupe de H.

(ii) Soit H' un sous-groupe de H. Alors $f^{-1}(H')$ est un sous-groupe de G.

Définition 1.12 (Noyau). *Soit G et H deux groupes et $f \in Hom(G, H)$ un morphisme de groupes. Le noyau de f est le sous-groupe de G défini par :*

$$Ker(f) = f^{-1}(\{e_H\}) = \{y \in G \mid f(y) = e_H\}.$$

Théorème 1.13 (Caractérisation de l'injectivité). *Soit $f \in Hom(G, H)$. Le morphisme f est injectif si et seulement si $Ker(f) = \{e_G\}$.*

Proposition 1.14 (Intersection de sous-groupes)**.** *Soit G un groupe, et $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Éléments de preuve. Sans difficulté à l'aide de l'une ou l'autre des caractérisations des sous-groupes. □

Proposition 1.15 (Sous-groupe engendré par une partie)**.** *Soit $(G,\star)$ un groupe, et X une partie de G. Le sous-groupe $\langle X\rangle$ de G engendré par X est le plus petit sous-groupe de G contenant X. Ce sous-groupe est défini explicitement par*

$$\langle X\rangle = \bigcap_{X\subset H} H,$$

l'intersection étant prise sur tous les sous-groupes H de G.

Proposition 1.16 (Description par le bas du sous-groupe engendré par une partie)**.** *Soit X une partie d'un groupe G. Alors $\langle X\rangle$ est l'ensemble des éléments pouvant s'écrire sous la forme $x_1\cdots x_n, n\in\mathbb{N}$, où les x_i vérifient soit $x_i\in X$, soit $x_i^{-1}\in X$. Le produit vide est par convention égal au neutre e de G.*

Éléments de preuve. Justifier que l'ensemble de ces éléments est forcément inclus dans $\langle X\rangle$, et que c'est un sous-groupe contenant X. □

Définition 1.17 (Partie génératrice d'un groupe)**.** *Soit $X\subset G$ une partie de G. On dit que X est une partie génératrice de G si $\langle X\rangle = G$.*

Proposition 1.18. *Les sous-groupes de $\mathbb{Z}$ sont les groupes $a\mathbb{Z} = \langle a\rangle, a\in\mathbb{N}$.*

Éléments de preuve. Considérer a l'élément minimal de $G\cap\mathbb{N}^*$. Justifier que $a\mathbb{Z}\subset G$, et si l'inclusion est stricte, contredire la minimalité de a en effectuant une division euclidienne. □

Exercise 1.19.

1. *Soit G un sous-groupe de $(\mathbb{R},+)$, non réduit à 0.*
   - *(a) Justifier l'existence de $a = \inf G\cap\mathbb{R}_+^*$.*
   - *(b) Justifier que si $a>0$, alors $a\in G\cap\mathbb{R}_+^*$, puis montrer que $G = a\mathbb{Z}$.*
   - *(c) Justifier que si $a=0$, alors G est dense dans $\mathbb{R}$.*

   Ainsi, tout sous-groupe de $\mathbb{R}$ est soit de la forme $a\mathbb{Z}$, soit dense dans $\mathbb{R}$.
2. *Soit $f:\mathbb{R}\to\mathbb{R}$ une fonction périodique. Montrer que l'ensemble T de ses périodes est soit de la forme $a\mathbb{Z}$, soit dense dans $\mathbb{R}$. Donner un exemple de fonction non constante dont l'ensemble des périodes est dense dans $\mathbb{R}$.*
3. *Soit $\theta\in\mathbb{R}\setminus\mathbb{Q}$. Montrer que l'ensemble $\{a+\theta b,\ a,b\in\mathbb{Z}\}$ est dense dans $\mathbb{R}$.*
4. *Déterminer l'ensemble des valeurs d'adhérence de $(\cos(n))_{n\in\mathbb{N}}$. On admettra que π est irrationnel.*

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:*