Chapitre 1

Groupes, sous-groupes

Il faut sans doute attribuer à Cayley, en 1854, la définition abstraite d'un groupe telle que nous la connaissons aujourd'hui. Auparavant, de nombreux groupes particuliers avaient déjà fait l'objet d'études approfondies en vue de la résolution de problèmes spécifiques, le plus célèbre d'entre eux étant le problème de la résolubitité par radicaux des équations polynomiales. Parmi les précurseurs de la théorie citons Lagrange (1770), Ruffini (1799), Galois (1829), Cauchy (1844), Cayley (1849, 1854), C. Jordan *Traité des substitutions* (1870), Klein *Erlanger Program* (1872).

1.1 Groupes

Définition 1.1 On appelle ***groupe*** tout couple $(G, *)$ formé d'un ensemble G appelé ensemble sous-jacent et d'une application

$$*\colon G \times G \to G, \qquad (g, h) \mapsto g * h$$

dite loi de composition interne, qui satisfait aux conditions suivantes :

1. La loi $*$ est ***associative*** :

   $(g * h) * k = g * (h * k)$ pour tout (g, h, k) dans $G \times G \times G$.

2. La loi $*$ admet un ***élément neutre*** $e \in G$:

   $e * g = g = g * e$ pour tout g dans G.

3. Tout élément de G admet un ***inverse*** pour la loi $*$:

   pour tout g dans G il existe h dans G tel que $g * h = e = h * g$.

Définition 1.2 Le groupe $(G, *)$ est dit ***commutatif*** (ou ***abélien)*** si

$$g * h = h * g \text{ pour tout couple } (g, h) \text{ dans } G \times G.$$

L'***ordre du groupe***, noté $|G|$, est le cardinal de l'ensemble sous-jacent G. Si l'ensemble G contient un nombre fini $n \in \mathbb{N}$ d'éléments, on dit que le groupe $(G, *)$ est d'ordre n ; sinon, il est dit d'ordre infini.

L'ensemble G contient un élément neutre et n'est donc jamais vide. Si la loi du groupe découle sans ambiguïté du contexte, on note le groupe G au lieu de $(G, *)$. Il existe deux notations classiques pour la loi de groupe, l'une additive, l'autre multiplicative. La notation additive sous-entend toujours que la loi est commutative. Désormais, sauf mention contraire, nous utiliserons la notation multiplicative. L'application $*$ est appelée la multiplication ou encore la loi de composition. Pour $(g, h) \in G \times G$ l'élément $g * h$ est appelé produit de g par h et on le note gh. Ce produit n'est pas supposé être commutatif. Dans cette notation par juxtaposition, l'élément neutre e est parfois noté 1 ou 1_G. L'associativité de la multiplication entraîne qu'un produit de n éléments ($n \geq 3$) est indépendant de la position des parenthèses et que l'on peut écrire sans risque de confusion des expressions telles que $g_1 g_2 \cdots g_n$. On vérifie facilement que l'élément $e \in G$ est le seul élément neutre de G et que l'inverse d'un élément est unique. Dans la notation multiplicative, l'inverse de g est noté g^{-1} (*jamais* $\frac{1}{g}$). Pour l'inverse d'un produit on a : $(gh)^{-1} = h^{-1}g^{-1}$.

Dans le cas d'un groupe commutatif, et seulement dans ce cas, la loi de composition est parfois notée à l'aide du symbole $+$. Dans ce cas, l'élément neutre est noté 0 ou 0_G et l'inverse de $g \in G$ est noté $-g$.

Règles de calcul dans un groupe : soient g, h et k des éléments d'un groupe G :

1. (Simplification) Si $gk = hk$, alors $g = h$. En effet, puisque k admet un inverse k^{-1} et que la loi de groupe est une application, nécessairement $g = (gk)k^{-1} = (hk)k^{-1} = h$. De même, $kg = kh$ entraîne $g = h$.
2. (Translation à gauche) Dans G, l'équation $gx = h$ possède une unique solution $x = g^{-1}h$. Il en résulte que, pour tout $g \in G$, l'application $x \mapsto gx$ est une bijection de G dans G. L'équation $xg = h$ possède également une unique solution hg^{-1} qui, lorsque le groupe est non commutatif, peut-être différente de la solution $g^{-1}h$. C'est à cause de cette ambiguïté que les notations $\frac{1}{g}$ et $\frac{h}{g}$ sont à proscrire.

Pour décrire un groupe fini dont l'ordre est petit, il est possible de donner sa table de multiplication (ou table de Cayley). Pour un groupe $(G, *)$ d'ordre 4 dont les éléments sont $\{e, g_1, g_2, g_3\}$, il s'agit de compléter la table suivante, en inscrivant ligne g_i et colonne g_j le produit $g_i g_j \in \{e, g_1, g_2, g_3\}$:

$*$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1			
g_2	g_2			
g_3	g_3			

Comme la translation à gauche et à droite sont des bijections, tous les éléments de G apparaissent sur chaque ligne et sur chaque colonne exactement une fois (un sudoku avec un seul carré...). Cela garantit aussi l'existence d'un inverse pour chaque élément. Il reste donc trois choix pour fixer l'inverse de g_1. Regardons le cas où g_1 est son propre inverse :

$*$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e		
g_2	g_2			
g_3	g_3			

Comme tous les éléments apparaissent exactement une fois dans chaque ligne, il reste les possibilités $g_1g_2 = g_2$ ou $g_1g_2 = g_3$. Puisque $g_1g_2 = g_2$ entraîne $g_1 = e$ on en déduit que $g_1g_2 = g_3$. En argumentant de manière semblable sur les colonnes nous obtenons :

$*$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3		
g_3	g_3	g_2		

Il reste deux possibilités pour remplir la table, qui, comme on le verra plus tard, correspondent à deux groupes structurellement différentes :

$G_{4,1}$:

$*$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3	e	g_1
g_3	g_3	g_2	g_1	e

et $G_{4,2}$:

$*$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3	g_1	e
g_3	g_3	g_2	e	g_1

.

Les autres choix possibles pour le produit g_1g_1 sont g_2 et g_3 qui conduisent également aux deux structures de groupes ci-dessus (dans le sens qu'après réarrangement et ajustement du nom des éléments nous obtenons les mêmes tables de multiplication). Cette approche est déjà très complexe pour les groupes avec un petit nombre d'éléments et une table de multiplication comme celle que nous avons obtenue ne définit pas encore un groupe, puisque l'associativité de la loi de composition reste à vérifier et peut faire défaut à ce stade.

EXEMPLES. Voici quelques exemples de groupes.

1. « Le » groupe trivial $G = \{e\}$ (un groupe possède au moins un élément).
2. Les groupes additifs (et donc commutatifs) d'anneaux $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$, $(\mathbb{Z}[X], +)$ et les groupes multiplicatifs de corps $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ et $(\mathbb{C}^*, \cdot)$ (également commutatifs, malgré la notation multiplicative). La définition d'un anneau et celle d'un corps sont rappelées dans l'annexe A.
3. Pour $n \in \mathbb{N}$ non nul et $a \in \mathbb{Z}$ notons $\overline{a}$ le reste de la division de a par n dans $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des restes $\{\overline{a} \mid a \in \mathbb{Z}\}$. On a $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour l'addition définie par $\overline{a} + \overline{b} = \overline{a+b}$. Ici $\overline{a+b}$ est le reste de la division de $a + b$ par n. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est fini.
   Il est possible de définir une multiplication sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{a} \cdot \overline{b} = \overline{ab}$. Si $n = p$ est un nombre premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps. Dans ce cas les éléments non nuls $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}$ forment un groupe multiplicatif $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ d'ordre $p - 1$.
   Les groupes $(\mathbb{Z}/4\mathbb{Z}, +)$ et $((\mathbb{Z}/5\mathbb{Z})^*, \cdot)$ sont tous les deux d'ordre 4. Après réarrangement des éléments, les deux groupes ont une table de multiplication correspondant à $G_{4,2}$. Ces deux groupes possède donc la même « structure de groupe ».
4. Groupe de transformations, groupe symétrique (cf. chapitre 5) : étant donné un ensemble X on note $\mathfrak{S}(X)$ l'ensemble des bijections de X vers lui-même. L'ensemble $\mathfrak{S}(X)$ est un groupe pour la composition des applications. Il n'est pas commutatif lorsque X a plus de deux éléments. Pour $x \in X$ et $f, g \in \mathfrak{S}(X)$ on a $f \circ g(x) = f(g(x))$ (d'abord g puis f).
   Pour $X = \{1, 2, \ldots, n\}$ le groupe symétrique $\mathfrak{S}(X)$ est d'ordre $n!$. Dans ce cas, on note $\mathfrak{S}_n$ au lieu de $\mathfrak{S}(\{1, 2, \ldots, n\})$. Le groupe $\mathfrak{S}_3$ est un groupe non abélien d'ordre 6 (chapitre 5), alors que le groupe $(\mathbb{Z}/6\mathbb{Z}, +)$ est abélien. Il s'agit donc de deux structures de groupes différentes.
5. Si V est un espace vectoriel sur un corps K, alors $(V, +)$ est un groupe additif. L'ensemble des éléments de $\mathfrak{S}(V)$ qui sont des applications linéaires forment le ***groupe (général) linéaire*** noté $\mathrm{GL}(V)$. Pour $n \in \mathbb{N}$ et $V = K^n$, le groupe de matrices correspondant est noté $\mathrm{GL}(n, K)$.
6. Pour un corps fini K à q éléments (on sait que q doit être la puissance d'un nombre premier p, cf. proposition 13.5) et $n \in \mathbb{N}$ le groupe $\mathrm{GL}(n, K)$ est noté $\mathrm{GL}(n, q)$. C'est un groupe fini à $\prod_{i=0}^{n-1}(q^n - q^i)$ éléments (proposition 14.10). Par exemple, $\mathrm{GL}(2, 2)$ est un groupe fini dont les 6 éléments sont

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

   (attention, il faut calculer modulo deux).

7. Les groupes définis par des courbes elliptiques (annexe C) sont très utilisés en cryptographie.

■

1.2 Sous-groupes

Définition 1.3 On appelle ***sous-groupe*** d'un groupe G tout sous-ensemble H de G sur lequel la multiplication de G induit une structure de groupe, c'est-à-dire, tel que les propriétés suivantes soient vérifiées :

1. $e \in H$,
2. $h_1 h_2 \in H$ pour tout $(h_1, h_2) \in H \times H$ et
3. $h^{-1} \in H$ pour tout $h \in H$.

Un sous-groupe H de G est dit ***distingué*** dans G, et on note $H \lhd G$, si $ghg^{-1} \in H$ pour tout $g \in G$ et tout $h \in H$.

Un sous-groupe d'un groupe abélien est toujours distingué.

EXEMPLES.

1. Pour tout groupe G, les sous-groupes $\{e\}$ et G sont toujours des sous-groupes distingués de G.
2. Soient K un corps et $n \in \mathbb{N}$. L'ensemble $\mathrm{SL}(n, K)$ des matrices de déteminant 1 dans $\mathrm{GL}(n, K)$ est un sous-groupe distingué de $\mathrm{GL}(n, K)$.
3. Pour n dans $\mathbb{Z}$, l'ensemble $n\mathbb{Z} = \{n \cdot k | k \in \mathbb{Z}\}$ des multiples de n est un sous-groupe de $(\mathbb{Z}, +)$.

■

Lemme 1.4 Soit G un groupe. Une partie H de G est un sous-groupe de G si et seulement si les conditions suivantes sont satisfaites :

1. L'ensemble H n'est pas vide ;
2. $h_1 h_2^{-1} \in H$ pour tout $(h_1, h_2) \in H \times H$.

DÉMONSTRATION. Si H est un sous-groupe de G, alors les deux conditions découlent directement de la définition d'un sous-groupe.

Supposons les deux conditions du lemme vérifiées. D'après la 1re condition H est non vide et donc il existe un élément h dans H. En appliquant la 2e condition au couple (h, h) nous obtenons $e = hh^{-1} \in H$. Pour tout h dans H la 2e condition appliquée au couple (e, h) montre que $eh^{-1} = h^{-1}$ appartient à H. Nous en déduisons que l'inverse de tout élément de H est dans H. Pour tout h_1 et tout h_2 dans H la 2e condition appliquée au couple $(h_1, h_2^{-1}) \in H \times H$ montre que le produit $h_1 h_2 = h_1 (h_2^{-1})^{-1}$ appartient à H. D'où le résultat. ■

Lemme 1.5 Soient I un ensemble et H_i ($i \in I$) des sous-groupes d'un groupe G. L'intersection $\cap_{i\in I} H_i$ est un sous-groupe de G. Pour $I = \emptyset$ on convient que $\cap_{i\in I} H_i = G$. Si pour tout i le sous-groupe H_i est distingué dans G, alors $\cap_{i\in I} H_i$ est un sous-groupe distingué dans G.

DÉMONSTRATION. Un élément g de G appartient à $\cap_{i\in I} H_i$ si et seulement si g appartient à tous les H_i. Puisque e appartient à tous les sous-groupes H_i l'ensemble $\cap_{i\in I} H_i$ est non vide. Si g appartient à tous les sous-groupes H_i alors g^{-1} appartient aussi à tous les sous-groupes H_i et donc à leur intersection $\cap_{i\in I} H_i$. Pour g_1 et g_2 dans $\cap_{i\in I} H_i$ nous en déduisons que les éléments g_1 et g_2^{-1} appartiennent à tous les sous-groupes H_i et donc $g_1 g_2^{-1}$ aussi. Il en résulte que $g_1 g_2^{-1}$ appartient à $\cap_{i\in I} H_i$ pour tout g_1 et tout g_2 dans $\cap_{i\in I} H_i$ et d'après le lemme précédent l'ensemble non vide $\cap_{i\in I} H_i$ est un sous-groupe de G.
Soient $g \in G$ et $h \in \cap_{i\in I} H_i$. Si les sous-groupes H_i sont tous distingués, alors, comme h appartient à tous les H_i, l'élément ghg^{-1} appartient aussi à tous les H_i et donc à $\cap_{i\in I} H_i$. Le sous-groupe $\cap_{i\in I} H_i$ est donc distingué dans G. ∎

En particulier, pour un sous-ensemble X de G l'intersection H de tous les sous-groupes de G qui contiennent X est un sous-groupe de G. Comme le sous-groupe H de G est contenu dans tous les sous-groupes de G qui contiennent X, c'est le plus petit sous-groupe de G qui contient X.

Proposition et définition 1.6 Etant donné un groupe G et un sous-ensemble X de G il existe un plus petit sous-groupe de G contenant X (i.e., contenu dans tous les sous-groupes de G qui contiennent X) qu'on appelle le ***sous-groupe de*** G ***engendré par*** X et que l'on note $\langle X\rangle_G$ ou simplement $\langle X\rangle$. Pour un sous-ensemble fini $\{g_1, g_2, \ldots, g_n\}$ de G on note $\langle\{g_1, g_2, \ldots, g_n\}\rangle$ simplement $\langle g_1, g_2, \ldots, g_n\rangle$.
Un groupe G est appelé ***groupe cyclique*** ou ***monogène*** s'il existe un élément g dans G tel que $\langle g\rangle$ est égal à G.
On appelle ***ordre d'un élément*** g de G l'ordre du sous-groupe $\langle g\rangle$ engendré par g.

REMARQUE. Dans la littérature française un groupe cyclique est un groupe monogène fini, alors que la définition ci-dessus n'implique pas qu'un groupe cyclique soit fini. Nous suivons ici la nomenclature anglaise. ∎

EXEMPLES.

1. Le groupe $(\mathbb{Z}/4\mathbb{Z}, +)$ est un groupe cyclique d'ordre 4 car il est engendré par $a = \overline{1}$ (mais il n'est pas engendré par l'élément $\overline{2}$ qui, lui, engendre un sous-groupe d'ordre deux). Par une dénomination adéquate des éléments $\{e, g_1, g_2, g_3\}$ de $\mathbb{Z}/4\mathbb{Z}$, par exemple $\overline{0} \rightsquigarrow e$, $\overline{1} \rightsquigarrow g_2$, $\overline{2} \rightsquigarrow g_1$ et $\overline{3} \rightsquigarrow g_3$, la table de multiplication du groupe $(\mathbb{Z}/4\mathbb{Z}, +)$ est $G_{4,2}$. Ceci montre que la table de multiplication $G_{4,2}$ est bien la table de multiplication d'un groupe et vérifie donc la règle d'associativité, question restée en suspens à la fin de la page 3. Notons qu'un groupe dont la table de multiplication est $G_{4,1}$ n'est pas cyclique

car tous les éléments sont d'ordre un ou deux. Les deux tables $G_{4,1}$ et $G_{4,2}$ correspondent donc à deux structures de groupes différentes.

2. Dans le groupe $\mathrm{GL}(2,2)$ d'ordre 6 (cf. exemple 6 page 4) il y a trois éléments d'ordre 2, deux éléments d'ordre 3 et un unique élément d'ordre 1 qui est l'identité. Ce groupe n'est donc pas cyclique.
3. Considérons les trois éléments suivants du groupe $\mathrm{GL}(2,2)$:

$$m_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; m_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } m_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Comme $m_i^2 = e$, les groupes $\langle m_i \rangle$ contiennent exactement les deux éléments m_i et $e = m_i^2$. Comme $m_2 m_1 (m_2)^{-1} = m_3$ n'appartient pas à $\langle m_1 \rangle$, le sous-groupe $\langle m_1 \rangle \subset \mathrm{GL}(2,2)$ n'est pas distingué.

∎

Un groupe engendré par $X = \{x_j \,|\, j \in J\}$ contient également l'inverse des générateurs x_i. En notation *multiplicative* $\langle X \rangle$ contient l'ensemble de tous les *mots de longueur finie* en les $x_i \in X$ et leurs inverses x_i^{-1}. Un exemple de mot est $x_2 x_3^{-1} x_2 x_3 x_1^{-1}$. Cependant des « mots » distincts peuvent représenter les mêmes éléments de G. Dans l'exemple précédent on a $X = \{m_1, m_2, m_3\} \subset \mathrm{GL}(2,2)$ avec $m_2 m_1 (m_2)^{-1} = m_3$, $m_1 m_1 = m_2 m_2 = m_3 m_3 = e$ et $m_2^{-1} = m_2$.

Proposition 1.7 Soient G un groupe et $X \subset G$ un sous-ensemble de G. Le sous-groupe $\langle X \rangle$ de G engendré par X est l'ensemble de tous les mots de longueur finie en les $x_i \in X$ et leurs inverses x_i^{-1}.

DÉMONSTRATION. Notons $\mathcal{M}(X)$ le sous-ensemble de G des mots de longueur finie en les $x_i \in X$ et leurs inverses x_i^{-1}. Le mot vide est l'élément neutre et il appartient à $\mathcal{M}(X)$. Pour $z = z_1^{\epsilon_1} z_2^{\epsilon_2} \cdots z_n^{\epsilon_n}$ et $y = y_1^{\omega_1} y_2^{\omega_2} \cdots y_m^{\omega_m}$ avec $y_i \in X$, $z_i \in X$, $\epsilon_i = \pm 1$ et $\omega_i = \pm 1$, on a $zy^{-1} = z_1^{\epsilon_1} z_2^{\epsilon_2} \cdots z_n^{\epsilon_n} y_m^{-\omega_m} \cdots y_2^{-\omega_2} y_1^{-\omega_1} \in \mathcal{M}(X)$, car c'est bien un mot en les $x_i \in X$ et leurs inverses x_i^{-1} et donc un élément de $\mathcal{M}(X)$. Donc, l'ensemble $\mathcal{M}(X)$ est un sous-groupe de G. Tout sous-groupe de G qui contient X contient tous les mots de longueur finie en les $x_i \in X$ et leurs inverses x_i^{-1} et donc $\mathcal{M}(X) \subset \langle X \rangle$. Comme $\langle X \rangle$ est le plus petit sous-groupe qui contient X, nécessairement $\mathcal{M}(X) = \langle X \rangle$. ∎

Corollaire 1.8 Soient G un groupe et $g \in G$ un élément d'ordre fini $n \in \mathbb{N}$. Alors, n est le plus petit entier strictement positif ayant la propriété $g^n = e$ et on a $\langle g \rangle = \{g, g^2, \ldots, g^n = e\}$. Pour $k \in \mathbb{Z}$ on a $g^k = e$ si et seulement si n divise k.

DÉMONSTRATION. Si $g = e$ nous obtenons le résultat avec $n = 1$. Supposons maintenant $g \neq e$. Le groupe $\langle g \rangle$ consiste en les mots en g et g^{-1} et donc ne contient que des éléments de la forme g^i avec $i \in \mathbb{Z}$. Comme le groupe possède un nombre fini

d'éléments, il doit exister $0 < i < j$ avec $g^i = g^j$. Dans ce cas $g^{j-i} = g^{j-i-1}g = e$ et nous obtenons $g^{-1} = g^{j-i-1}$ avec $0 \leq j - i - 1$. Le groupe $\langle g \rangle$ ne contient donc que des éléments de la forme g^i avec $i \in \mathbb{N}$. Soit m le plus petit entier strictement positif qui vérifie $g^m = e$. Alors, les éléments $g, g^2, \ldots, g^m$ sont tous distincts. En effet, $g^j = g^i$ pour $1 \leq i < j < m$ entraîne $g^{j-i} = e$, ce qui contredit la minimalité de m. Puisque $\langle g \rangle$ est d'ordre n, on a $m \leq n$. Pour un entier positif k nous obtenons par division euclidienne $k = q \cdot m + r$ avec $0 \leq r < m$ et donc $g^k = (g^m)^q g^r = g^r$. Comme $g^0 = e = g^m$, il en résulte que $\langle g \rangle$ est contenu dans $\{g, g^2, \ldots, g^m\}$ et donc $m = n$. Pour $k \in \mathbb{Z}$ la division euclidienne précédente montre que $g^k = e$ si et seulement si n divise k. ∎

Dans la suite de ce paragraphe nous utilisons la notation additive dans laquelle la notion de mot est moins naturelle. Dans le groupe engendré par $n \in (\mathbb{Z}, +)$ un exemple de *mot* est $n + n + (-n) + n + (-n) + n = 2n$. Le sous-groupe $\langle n \rangle$ contient donc tous les éléments $\{kn | k \in \mathbb{Z}\}$ et on note ce sous-groupe $n\mathbb{Z}$.

Proposition 1.9 Soit H un sous-groupe de $(\mathbb{Z}, +)$. Alors, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

DÉMONSTRATION. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon H contient un élément non nul et son opposé et donc contient un entier positif non nul. Comme toute partie non vide de $\mathbb{N}$ possède un plus petit élément, il existe un plus petit entier positif non nul n dans H. Il en résulte que $n\mathbb{Z}$ est contenu dans H et nous voulons montrer que $H \subset n\mathbb{Z}$. Soit $m \in H$, nous devons montrer que $m \in n\mathbb{Z}$. Par division euclidienne dans $\mathbb{Z}$ nous obtenons $m = kn + r$ avec k et r dans $\mathbb{Z}$ et $0 \leq r < n$. Comme $r = m - kn$, il en résulte que r appartient à H. Puisque $0 \leq r < n$, la minimalité de n implique $r = 0$. Donc, $m = kn \in n\mathbb{Z}$ et le résultat s'ensuit. ∎

1.3 Groupes diédraux

On définit souvent des groupes comme sous-groupes qui préservent une propriété (ou une figure). Ainsi les isométries du plan affine sont les transformations du plan qui conservent les distances, celles-ci forment un sous-groupe du groupe affine. En se restreignant aux isométries qui préservent un polygone régulier, on obtient des sous-groupes du groupe des isométries du plan affine. Ce sont ces sous-groupes auxquels nous nous intéressons dans ce paragraphe.

Définition 1.10 Soit $n \in \mathbb{N}$ avec $n \geq 3$. Dans le plan complexe $\mathbb{C}$ identifié à $\mathbb{R}^2$ considérons le polygone régulier connexe $\mathcal{P}_n$ à n sommets formé par les affixes des racines n^{es} de l'unité $\omega_k = e^{2ik\pi/n}$ ($k \in \{0, 1, \ldots, n-1\}$). Le ***groupe diédral*** D_n pour $n \geq 3$ est le sous-groupe des isométries du plan affine qui laissent $\mathcal{P}_n$ invariant.