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 résolubilité par radicaux des équations polynomiales. Parmi les précurseurs de la théorie citons Lagrange (1770), Ruffini (1799), Galois (1829), Cauchy (1844), Cayley (1849, 1854), 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 $*\colon G \times G \to G; (g, h) \mapsto g * h$, 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. Il existe dans G un élément neutre e pour la loi $*$: $e * g = g = g * e$ 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 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 $(g_1(g_2g_3)\cdots g_n)$ 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 $g_1g_2\cdots g_n$. 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 : soit 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) dont les colonnes et les lignes sont numérotées par les éléments de G et dont l'entrée à la ligne g_i et la colonne g_j est le produit g_ig_j. Afin de déterminer toutes les structures de groupe possibles d'un groupe à 4 éléments, considérons un groupe $(G, *)$ dont les éléments sont $\{e, g_1, g_2, g_3\}$. Comme le produit avec l'élément neutre est toujours donné, il s'agit de compléter la table suivante, en inscrivant en ligne g_i et colonne g_j le produit $g_ig_j \in \{e, g_1, g_2, g_3\}$:

$*$	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 les translations 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 la contradiction $g_1 = e$, 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 différents :

$G_{4,1}$:

$*$	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 être mise en 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).

3. Soit F un corps et V un espace vectoriel. Le groupe $(V, +)$ est un groupe abélien. L'ensemble des applications linéaires bijectives forme le ***groupe (général) linéaire*** pour la composition des application noté $\mathrm{GL}(V)$. Si V est de dimension finie $n \in \mathbb{N}$, alors après le choix d'une base nous avons $V \cong F^n$ et les éléments de $\mathrm{GL}(V)$ sont les applications linéaires dont la matrice est inversible. Dans ce cas, le groupe correspondant des matrices $n \times n$ inversibles est noté $\mathrm{GL}(n, F)$.
4. Groupe de transformations, groupe symétrique (cf. chapitre 6) : 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 la cardinalité de X est ≥ 3. Pour $x \in X$ et f, g dans $\mathfrak{S}(X)$ on a $f \circ g(x) = f(g(x))$. 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 6).
5. Les groupes définis par des courbes elliptiques (annexe B) 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 sont vérifiées :

1. $e \in H$,
2. $h_1 h_2 \in H$ pour tout $(h_1, h_2) \in H \times H$,
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 $h \in H$.

Pour tout groupe G, les sous-groupes $\{e\}$ et G sont toujours des sous-groupes distingués de G. Dans un groupe abélien, tous les sous-groupes sont distingués.

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, si bien 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 $h_1h_2 = h_1(h_2^{-1})^{-1}$ appartient à H. D'où le résultat. ∎

EXEMPLE. Soit F un corps, n un entier positif et $\mathrm{SL}(n,F)$ le sous-ensemble de $\mathrm{GL}(n,F)$ des matrices de déterminant 1. La matrice identité Id appartient à $\mathrm{SL}(n,F)$ et $\det(gh^{-1}) = \frac{\det(g)}{\det(h^{-1})} = 1$ pour tous g,h dans $\mathrm{SL}(n,F)$. D'après le lemme, le sous-ensemble $\mathrm{SL}(n,F)$ est donc un sous-groupe de $\mathrm{GL}(n,F)$. Pour tout g dans $\mathrm{GL}(n,F)$ et tout $h \in \mathrm{SL}(n,F)$, nous avons $\det(ghg^{-1}) = \det(h) = 1$, si bien que $\mathrm{SL}(n,F)$ est un sous-groupe distingué de $\mathrm{GL}(n,F)$. □

Lemme 1.5 Soit 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 $g_1g_2^{-1}$ aussi. Il en résulte que $g_1g_2^{-1}$ 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.
Soit $g \in G$ 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. ∎

L'intersection H de tous les sous-groupes de G qui contiennent un sous-ensemble $X \subset G$ 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 $\langle\{g_1, g_2, \ldots, g_n\}\rangle$ plus simplement $\langle g_1, g_2, \ldots, g_n\rangle$.

Définition 1.7 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. ∎

Exemple 1.8 L'ensemble $H = \langle i\rangle = \{1, i, i^2, i^3\} \subset (\mathbb{C}^*, \cdot)$ est un sous-groupe cyclique d'ordre 4. L'élément i^2 engendre un sous-groupe $K = \{1, i^2\}$ de H. Par une dénomination adéquate des éléments de H, par exemple $1 \rightsquigarrow e$, $i^2 \rightsquigarrow g_1$, $i \rightsquigarrow g_2$ et $i^3 \rightsquigarrow g_3$, nous obtenons que la table de multiplication du groupe H 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. □

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* formés par les $x_i \in X$ et leurs inverses x_i^{-1} (cf. chapitre A). Un exemple de mot est $x_2x_3^{-1}x_2x_3x_1^{-1}$. Cependant des « mots » distincts peuvent représenter les mêmes éléments de G. On convient que le mot vide est e.

Proposition 1.9 Soit 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 formés par les $x_i \in X$ et leurs inverses x_i^{-1}.
Si les générateurs $x_i \in X$ commutent entre eux, alors $\langle X\rangle$ est un sous-groupe abélien.
Si gx_ig^{-1} appartient à $\langle X\rangle$ pour tout x_i dans X et tout g dans G, alors $\langle X\rangle$ est un sous-groupe distingué de G.

DÉMONSTRATION. Notons $\mathcal{M}(X)$ le sous-ensemble de G des mots de longueur finie formés par 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 $\omega_i = \pm 1$, l'élément $zy^{-1} = z_1^{\epsilon_1}z_2^{\epsilon_2}\cdots z_n^{\epsilon_n}y_m^{-\omega_m}\cdots y_2^{-\omega_2}y_1^{-\omega_1}$ appartient à $\mathcal{M}(X)$, car c'est bien un mot formé par 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 formés par les $x_i \in X$ et leurs inverses x_i^{-1}, si bien que $\mathcal{M}(X) \subset \langle X\rangle$. Comme $\langle X\rangle$ est le plus petit sous-groupe qui contient X, nécessairement $\mathcal{M}(X) = \langle X\rangle$.
Si les $x_i \in X$ commutent entre eux, alors les x_i et les x_j^{-1} ainsi que les x_i^{-1} et les x_j^{-1}commutent entre eux. Dans le produit de deux mots de $\langle X\rangle$, il est donc

possible de faire passer toutes les lettres du mot de droite à gauche. Par conséquent, tous les mots commutent et le groupe $\langle X\rangle$ est abélien.
Soit $z = z_1^{\epsilon_1} z_2^{\epsilon_2} \cdots z_n^{\epsilon_n}$ dans $\langle X\rangle$ avec $z_i \in X$ et $\epsilon_i = \pm 1$. Si $gz_ig^{-1} \in \langle X\rangle$ pour tout $g \in G$, alors $(gz_ig^{-1})^{-1} = g^{-1}z_i^{-1}g \in \langle X\rangle$ pour tout $g \in G$. Il en résulte que $gz_i^{-1}g^{-1} \in \langle X\rangle$ pour tout $g \in G$. Si bien que

$$gzg^{-1} = gz_1^{\epsilon_1} z_2^{\epsilon_2} \cdots z_n^{\epsilon_n} g^{-1} = (gz_1^{\epsilon_1} g^{-1})(gz_2^{\epsilon_2} g^{-1})(g \cdots g^{-1})(gz_n^{\epsilon_n} g^{-1}) \in \langle X\rangle.$$

Par conséquent, $\langle X\rangle$ est un sous-groupe distingué de G. ∎

Corollaire 1.10 Soit G un groupe et $g \in G$ un élément d'ordre fini n. Alors, n est le plus petit entier strictement positif ayant la propriété $g^n = e$ et nous avons $\langle g\rangle = \{g, g^2, \ldots, g^n = e\}$. 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 formés par g et g^{-1} et donc ne contient que des éléments de la forme g^i avec $i \in \mathbb{Z}$. Comme le groupe $\langle g\rangle$ est fini, il existe $0 < i < j$ 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 $g^m = e$. Supposons qu'il existe $1 \leq i < j < m$ avec $g^j = g^i$. Il en résulterait que $g^{j-i} = e$ avec $0 \leq j-1 < m$, ce qui contredirait la minimalité de m. Par conséquent, les éléments $g, g^2, \ldots, g^m$ sont donc tous distincts. Puisque $\langle g\rangle$ est d'ordre n, nous avons $m \leq n$. 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 $\{g, g^2, \ldots, g^m\}$, si bien que $m = n$. 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.

Exemple 1.11 Pour n dans $(\mathbb{Z}, +)$, nous avons $\langle n\rangle = \{nk | k \in \mathbb{Z}\}$ et on note ce sous-groupe $n\mathbb{Z}$.

Proposition 1.12 Soit H un sous-groupe de $(\mathbb{Z}, +)$. 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 $a \neq 0$. Comme H contient a et $-a$, nous obtenons que H 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, r) dans $\mathbb{Z} \times \mathbb{Z}$ 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

Définition 1.13 Pour un entier $n \geq 1$ le ***groupe diédral*** D_n est le sous-groupe de $\mathrm{GL}(2,\mathbb{R})$ engendré par la symétrie axiale s et la rotation r d'angle $\theta = \frac{2\pi}{n}$ définies par $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $r = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. Le groupe C_n est le sous-groupe cyclique de D_n engendré par la rotation r.

Le groupe $D_1 = \langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle = \{e, s\}$ est un groupe cyclique d'ordre 2. Pour $n \geq 3$ le groupe diédral est le groupe des isométries du polygône régulier à n sommets (exemple 4.13). Cependant, nous allons utiliser une caractérisation par générateurs et relations qui sera utile plus tard.

Proposition 1.14 Pour un entier $n \geq 1$ le groupe $D_n \subset \mathrm{GL}(2,\mathbb{R})$ est un groupe d'ordre $2n$. Les générateurs r et s du groupe D_n satisfont aux relations $r^n = e$, $s^2 = e$ et $sr = r^{-1}s$ et les éléments de D_n sont donnés par la liste $\{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s \ldots, r^{n-1}s\}$. Le groupe D_2 est abélien non cyclique et pour $n \geq 3$ le groupe D_n est non abélien. Le sous-groupe $C_n = \langle r \rangle \subset D_n$ est un sous-groupe cyclique distingué de D_n d'ordre n.

DÉMONSTRATION. La vérification des relations entre r et s par le calcul est laissée au lecteur. Puisque n est le plus petit entier positif vérifiant $r^n = e$, le sous-groupe $\langle r \rangle$ de $\mathrm{GL}(2,\mathbb{R})$ est d'ordre n. Par conséquent, les éléments $e, r, r^2, \ldots, r^{n-1}$ sont tous distincts (corollaire 1.10). Comme $s^{-1} = s$ et $r^{-1} = r^{n-1}$, les mots formés par s, s^{-1}, r, r^{-1} s'écrivent comme des mots formés par r et s. À l'aide de la relation $sr = r^{-1}s = r^{n-1}s$, il est possible d'écrire tout mot en s, r sous la forme r^j ou $r^j s$ avec $j \in \{0, 1, \ldots, n-1\}$, montrant que le groupe D_n est un groupe fini d'ordre au plus $2n$. Comme $\det(s) = -1$, les éléments de la forme $r^j s$ ne sont pas dans $\langle r \rangle = \{e, r, r^2, \ldots, r^{n-1}\}$. Les éléments $s, rs, r^2s, \ldots, r^{n-1}s$ sont également distincts, car pour $i < j$, l'égalité $r^i s = r^j s$ entraînerait $r^{j-i} = e$ et contredirait le fait que r soit d'ordre n. Donc le sous-groupe $\langle r, s \rangle = D_n$ est d'ordre $2n$ et il en résulte que $D_n = \langle r, s \rangle = \{e, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$.
Pour tout $j \in \{1, \ldots, n\}$ et tout $i \in \{1, \ldots, n\}$, nous avons $r^j r^i r^{-j} = r^i \in \langle r \rangle$ et, puisque $rs = sr^{-1}$, $sr^i s = r^{-i} \in \langle r \rangle$. Si bien que

$$(r^j s) r^i (r^j s)^{-1} = r^j (s r^i s) r^{-j} = r^{-i} \in \langle r \rangle.$$

Par conséquent, le sous-groupe $\langle r \rangle$ est distingué dans D_n.
Pour $n = 2$ le groupe $D_2 = \{e, s, r, rs\}$ ne contient que des éléments d'ordre 2. Dans ce cas $sr = rs$, si bien que D_2 est non cyclique abélien avec comme table de multiplication la table $G_{4,1}$ (proposition 1.9). Pour $n \geq 3$, nous avons $sr = r^{-1}s \neq rs$ et dans ce cas, le groupe D_n est non abélien. ∎