Groupes (notes de cours)
Préparation à l'agrégation interne
Université Paris Diderot

Catherine Gille

1 Groupes, sous-groupes, morphismes

Définition 1.1 *Un groupe est un ensemble G non vide muni d'une loi de composition interne associative, possédant un élément neutre, et tel que tout élément de G admet un inverse (= un symétrique). Si la loi est commutative, on dit que le groupe est commutatif (ou abélien).*

Remarque : unicité de l'élément neutre, de l'inverse

Notations multiplicative et additive (celle-ci étant réservée aux groupes commutatifs).

Définition du produit cartésien de deux groupes.

Exemples :
1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de $+$.
2. $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ munis de $\times$.
3. $(\mathbb{Z}/n\mathbb{Z}, +)$.
4. $(\mathcal{M}_n(\mathbb{K}), +)$, $(GL_n(\mathbb{K}), \times)$.
5. $(\mathcal{S}(E), \circ)$ groupe des bijections d'un ensemble E. Groupe symétrique $(\mathcal{S}_n, \circ)$.

Proposition 1.2 *Soit $(G, \cdot)$ un groupe et H une partie de G. Alors les propriétés suivantes sont équivalentes :*

a. H est stable pour la loi $\cdot$ et $(H, \cdot)$ est un groupe,

b. H est non vide, stable pour la loi $\cdot$ et stable par passage à l'inverse,

c. H est non vide et vérifie : $\forall (x, y) \in H^2, x \cdot y^{-1} \in H$.

Si a, b ou c est vérifié, on dit que H est un *sous-groupe* de G.

Proposition 1.3 *Une intersection de sous-groupes est un sous-groupe.*

Exemples :
1. $]0, +\infty[$ est un sous-groupe de $(\mathbb{R}^*, \times)$.
2. $\mathbb{U}_n = \{z \in \mathbb{C} | z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$, et même de $(S^1, \times)$.

3. Les sous-groupes de $(\mathbb{Z},+)$ sont les $m\mathbb{Z}$, $m \in \mathbb{N}$.
4. Les sous-groupes de $(\mathbb{R},+)$ sont soit de la forme $\alpha\mathbb{Z}$ ($\alpha \in \mathbb{R}$), soit denses dans $\mathbb{R}$ (cf exercice ci-dessous).
5. Centre d'un groupe : $Z(G) = \{a \in G | \forall x \in G, ax = xa\}$

Exercice 1.4 (Sous-groupes de $\mathbb{R}$) *1. Soit G un sous groupe de $(\mathbb{R},+)$, non réduit à $\{0\}$.*

(a) Montrer que si $\inf(G \cap]0,+\infty[) > 0$, alors G est de la forme $\alpha\mathbb{Z}$, avec $\alpha > 0$. (G est alors discret)

(b) Montrer que si $\inf(G \cap]0,+\infty[) = 0$ alors G est dense dans $\mathbb{R}$.

2. Soit $\delta \in]0,+\infty[$. Montrer que $G = \{a + b\delta,\ (a,b) \in \mathbb{Z}^2\}$ est un sous-groupe additif de $\mathbb{R}$. Montrer que G est discret si et seulement si $\delta \in \mathbb{Q}$.

Exercice 1.5 *Montrer que le centre de $GL_n(\mathbb{K})$ est l'ensemble des matrices scalaires non nulles.*

Sous-groupe engendré par une partie

Soit $(G,\cdot)$ un groupe et soit A une partie non vide de G. on appelle *sous-groupe engendré par A* l'intersection de tous les sous-groupes de G qui contiennent A. C'est aussi le plus petit sous-groupe de G qui contient A. On le note $gr(A)$ ou $< A >$.

Proposition 1.6 *Soit $(G,\cdot)$ un groupe, A une partie non vide de G. Alors $gr(A)$ est l'ensemble des produits d'éléments de A et de leurs inverses.*

Exemples :
1. $n\mathbb{Z} = gr(\{n\})$ dans $(\mathbb{Z},+)$.
2. $\mathbb{U}_n = gr(\{e^{\frac{2i\pi}{n}}\})$ dans $(\mathbb{C}^*,\times)$.
3. $GL_n(\mathbb{K})$ est engendré par les matrices d'opérations élémentaires.

Morphismes de groupes (=homomorphismes)

Définition 1.7 *Soit $(G,*)$ et $(G',*')$ deux groupes. On dit qu'une application $f : G \to G'$ est un morphisme de groupes si : $\forall x,y \in G, f(x*y) = f(x) *' f(y)$.*

Remarque : on a alors $f(1_G) = 1'_G$ et $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G$.

Si f est un morphisme bijectif, on dit que c'est un *isomorphisme*, et on dit alors que G et G' sont *isomorphes*.

En utilisant que la composée de deux morphismes est encore un morphisme et que l'inverse d'un isomorphisme est un (iso-)morphisme, on définit le groupe des *automorphismes* du groupe G, que l'on note $(Aut(G),\circ)$.

Proposition 1.8 *L'image (respectivement l'image réciproque) d'un sous-groupe par un morphisme est un sous-groupe.*

En particulier, si $f : G \to G'$ est un morphisme de groupes, alors $Imf = f(G)$ est un sous-groupe de G' et $Kerf = \{x \in G | f(x) = 1_{G'}\}$ est un sous-groupe de G.

Proposition 1.9 *Soit $f : G \to G'$ un morphisme de groupes. Alors f est injective si et seulement si $Ker f = \{1_G\}$.*

Soit $f : G \to G'$ un morphisme de groupes. On remarque que si $x \in Ker f$ et $a \in G$, alors $axa^{-1} \in Ker f$. Ainsi $Ker f$ est stable par conjugaison.

Définition 1.10 *Soit G un groupe, H un sous-groupe de G. On dit que H est distingué dans G si : $\forall x \in G, \forall h \in H, xhx^{-1} \in H$.*

Remarque : dans un groupe commutatif, tout sous-groupe est distingué.

On vient de voir que le noyau d'un morphisme de groupes est distingué. Plus généralement on a :

Proposition 1.11 *L'image réciproque par un morphisme de groupes d'un sous-groupe distingué est un sous-groupe distingué.*

Exemples de morphisme :
0. Soit G un groupe et H un sous-groupe de G. Alors l'inclusion de H dans G est un morphisme de groupes injectif.
1. $\exp : (\mathbb{R}, +) \to (]0, +\infty[, \times)$ est un isomorphisme d'inverse ln.
2. $\det : (GL_n(\mathbb{R}), \times) \to (\mathbb{R}^*, \times)$ est un morphisme de groupes surjectif.
$SL_n(\mathbb{R}) = Ker \det$ est un sous-groupe distingué de $GL_n(\mathbb{R})$. L'ensemble des matrices $n \times n$ inversibles à déterminant positif est un sous-groupe distingué de $GL_n(\mathbb{R})$ (c'est $\det^{-1}(]0, +\infty[)$).
3. Signature des permutations : $\varepsilon : (\mathcal{S}_n, \circ) \to (\{-1, +1\}, \times)$ est un morphisme de groupes.

Exercice 1.12 *On note $\mathbb{Q}_+^* = \mathbb{Q} \cap]0, +\infty[$. Montrer que les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$ ne sont pas isomorphes (*indication: utiliser le fait que $\sqrt{2} \notin \mathbb{Q}$*).*

Exercice 1.13 (Automorphismes intérieurs) *Soit G un groupe. Pour tout $a \in G$, on définit une application $\psi_a : G \to G$ en posant $\psi_a(x) = axa^{-1}$ pour tout $x \in G$.*

1. *Montrer que pour tout $a \in G$, ψ_a est un automorphisme de G. Tout automorphisme de cette forme est appelé automorphisme intérieur.*
2. *Montrer que l'application $\Psi : G \to \mathrm{Aut(G)}$ qui à tout élément a de G associe ψ_a est un morphisme de groupes.*
3. *Montrer que l'ensemble* $\mathrm{Int(G)}$ *des automorphismes intérieurs forme un sous-groupe distingué de* $\mathrm{Aut(G)}$.
4. *Montrer que le centre $Z(G)$ de G est un sous-groupe distingué de G.*

2 Ordre d'un élément, ordre des sous-groupes, groupe quotient

2.1 Ordre d'un élément

Définition 2.1 *Soit $(G, \cdot)$ un groupe et soit x un élément de G. L'ordre de x est le plus petit entier $n \in \mathbb{N}^*$, s'il existe, tel que $x^n = 1$. Sinon, on dit que x est d'ordre infini.*

Autre définition : l'*ordre* de x est l'ordre du sous-groupe de G engendré par x.
(Rappel : l'*ordre* d'un groupe H est par définition son cardinal, on le note $|H|$).

Remarques : 0. Dans un groupe fini, tout élément est d'ordre fini.
1. Il existe des groupes infinis dans lesquels tout élément est d'ordre fini.
2. Il existe des groupes infinis engendrés par un nombre fini d'éléments d'ordre fini.
3. L'ordre des éléments est conservé par isomorphisme.

Proposition 2.2 *Soit $(G, \cdot)$ un groupe et soit x un élément de G. Alors pour tout $m \in \mathbb{Z}$ on a : $x^m = 1$ si et seulement si l'ordre de x divise m.*

2.2 Groupes monogènes, groupes cycliques

Définition 2.3 *Un groupe est monogène s'il est engendré par un seul élément. Si de plus il est d'ordre fini, on dit que le groupe est cyclique.*

Remarques :
1. Un groupe cyclique est commutatif.
2. Les générateurs d'un groupe cyclique d'ordre n sont exactement ses éléments d'ordre n.

Théorème 2.4 *Soit $(G, \cdot)$ un groupe monogène. Alors:*
i) soit G est infini et est isomorphe à $(\mathbb{Z}, +)$.
ii) soit G est fini et G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ où $n = |G|$.

Démonstration : Soit g un générateur de G. Si g est d'ordre infini, montrer que l'application $\varphi_g : (\mathbb{Z}, +) \to (G, \cdot)$ définie par $\varphi_g(k) = g^k$ est un isomorphisme. Si g est d'ordre fini n, montrer que l'application $\varphi_g : (\mathbb{Z}/n\mathbb{Z}, +) \to (G, \cdot)$ définie par $\varphi_g(\bar{k}) = g^k$ est bien définie et est un isomorphisme.

Les générateurs de $(\mathbb{Z}, +)$ sont 1 et -1.

Générateurs de $\mathbb{Z}/n\mathbb{Z}$

Proposition 2.5 *Soit $k \in \mathbb{Z}$. Alors $\bar{k}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ ssi $k \wedge n = 1$.*

Conséquence : il y a $\varphi(n)$ générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$, où φ désigne l'indicateur d'Euler.

Corollaire 2.6 *Soit $(G, \cdot)$ un groupe cyclique d'ordre n et g un générateur de G. Alors les générateurs de G sont les g^k avec $k \wedge n = 1$.*

Démonstration : L'isomorphisme φ_g défini plus haut envoie un générateur sur un générateur.

Exercice 2.7 *Soit $(G, \cdot)$ un groupe cyclique d'ordre n et g un générateur de G. Alors pour tout $k \in \mathbb{N}$, l'ordre de g^k est $\frac{n}{k \wedge n}$.*

Exercice 2.8 (Groupes d'ordre 4) *Montrer que tout groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

2.3 Classes, indice, théorème de Lagrange

Soit $(G, \cdot)$ un groupe et H un sous-groupe de G. La relation $\mathcal{R}_g$ définie sur G par :

$$x \mathcal{R}_g y \Leftrightarrow x^{-1} y \in H$$

est une relation d'équivalence.
Pour tout $x \in G$, $xH = \{xh, h \in H\}$ est la classe d'équivalence de x par $\mathcal{R}_g$ et s'appelle la *classe à gauche* de x. Toutes les classes à gauche ont même cardinal (celui de H) et elles forment une partition de G. On note $(G/H)_g$ l'ensemble des classes à gauche et $[G : H]$ le cardinal de cet ensemble (appelé *indice* de H dans G) quand il est fini. Si G est fini on a alors $|G| = [G : H] \times |H|$ et on en déduit le :

Théorème 2.9 (Théorème de Lagrange) *Soit G un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G. En particulier l'ordre de tout élément de G divise l'ordre de G.*

Corollaire 2.10 *Soit G un groupe d'ordre fini n. Alors pour tout $x \in G$, $x^n = 1$.*

Corollaire 2.11 *Tout groupe d'ordre premier est cyclique.*

De manière similaire, on peut définir sur G une relation d'équivalence $\mathcal{R}_d$ et les *classes à droite* associées Hx (pour tout $x \in G$). Il y en a autant que de classes à gauche mais elles ne définissent pas nécessairement la même partition de G. On note $(G/H)_d$ l'ensemble des classes à droite.

Exemple : Dans le groupe symétrique $\mathcal{S}_3$, déterminer les classes à gauche et à droite pour le sous-groupe $H =< (1, 2) >$ (engendré par la transposition $(1, 2)$).

Le cas où les deux partitions sont les mêmes correspond au cas où H est distingué dans G :

Proposition 2.12 *Soit G un groupe et H un sous-groupe.*
Alors H est distingué dans G ssi $(G/H)_g = (G/H)_d$ (ie les classes à gauche et à droite coïncident).

Corollaire 2.13 *Tout sous-groupe d'indice 2 est distingué.*

2.4 Groupe quotient

Théorème 2.14 *Soit $(G, \cdot)$ un groupe et soit H un sous-groupe de G.*
Alors les propositions suivantes sont équivalentes :

(i) H est distingué dans G,

(ii) La loi de composition sur G induit une loi de composition bien définie sur $(G/H)_g$.

Si H est un sous-groupe distingué de G, les classes à gauche et à droite coïncident et on peut donc définir $G/H = (G/H)_g = (G/H)_d$. D'après le théorème on peut munir G/H de la loi induite par la loi de G (définie par $xH \cdot yH = xyH$ pour tout $x, y \in G$). $(G/H, \cdot)$ est le *groupe quotient* de G par H.

Remarques : l'élément neutre est la classe de 1_G $(=H)$. On a $|G| = |G/H| \times |H|$ si G est fini.

On notera $\bar{x}$ plutôt que xH la classe de x. La projection canonique $\pi : G \to G/H$ définie par $\pi(x) = \bar{x}$ est un morphisme de groupes et son noyau est H. Ainsi on a la :

Proposition 2.15 *Soit G un groupe et soit H un sous-groupe de G.*
Alors H est distingué dans G ssi H est le noyau d'un morphisme de groupes défini sur G.

Exemples :
1. $(\mathbb{Z}/n\mathbb{Z}, +)$ est le groupe quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.
2. $]0, +\infty[$ est un sous-groupe (distingué) de $(\mathbb{R}^*, \times)$ et on a $\mathbb{R}^*/]0, +\infty[= \{\overline{1}, \overline{-1}\}$, $\overline{1} =]0, +\infty[$ et $\overline{-1} =]-\infty, 0[$.

Proposition 2.16 *Soit $f : G \to G'$ un morphisme de groupes. Alors f induit par passage au quotient un isomorphisme de groupes entre $G/\ker f$ et Imf. En particulier on a $|G| = |Imf| \times |\ker f|$ si G est fini.*

Exemples :
1. L'application $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ définie par $f(t) = e^{2i\pi t}$ est un morphisme de groupes, qui induit un isomorphisme $\mathbb{R}/\mathbb{Z} \simeq S^1$.
2. L'application $N : (\mathbb{C}^*, \times) \to (\mathbb{R}^*, \times)$ définie par $N(z) = |z|$ est un morphisme de groupes. On a $\ker N = S^1$, $ImN =]0, +\infty[$ et $\mathbb{C}^*/\ker N = \mathbb{C}^*/S^1 \simeq]0, +\infty[$.
3. Le morphisme det : $GL_n(\mathbb{R}) \to \mathbb{R}^*$ induit un isomorphisme $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$.
4. Pour tout groupe G, on a un isomorphisme Int(G) $\simeq$ G/Z(G) (cf exercice 1.13).

Exercice 2.17 *1. Soit G un groupe où pour tout x, $x^2 = e$. Montrer que G est abélien.*

2. *Pour cette question et la suivante, on suppose que G est de plus un groupe fini non trivial. Montrer qu'alors G est d'ordre pair.*

3. *En déduire que l'ordre d'un groupe G fini, vrifiant l'hypothse de la premire question, est une puissance de 2 (*indication: on raisonnera par récurrence sur l'ordre de G en considérant un quotient bien choisi*).*

Exercice 2.18 (Groupes d'ordre 6) *Le but de cet exercice est de montrer que les seuls groupes d'ordre 6 sont, à isomorphisme près, $\mathbb{Z}/6\mathbb{Z}$ et $\mathcal{S}_3$. Soit G un tel groupe.*

1. *Montrer que G admet des éléments d'ordre 2 et 3 (cf ex. 2.17).*
2. *Soit b un élément d'ordre 3 de G. Montrer que $\langle b \rangle$ est distingué.*
3. *Soit a un élément d'ordre 2 de G. Montrer que aba est égal à b ou b^2.*
4. *Si $aba = b$, montrer que ab est d'ordre 6 et conclure que $G \simeq \mathbb{Z}/6\mathbb{Z}$.*
5. *Si $aba = b^2$, on pose $c = ab$ et $d = ba$. Montrer que $G = \{e, a, b, b^2, c, d\}$ et écrire la table de G. Conclure que $G \simeq \mathcal{S}_3$.*

3 Le groupe symétrique

Soit $n \in \mathbb{N}^*$. $\mathcal{S}_n$ est par définition l'ensemble des bijections de l'ensemble $\{1, \ldots, n\}$. C'est un groupe pour la composition des applications, d'ordre $n!$, et non commutatif dès que $n \geq 3$. les éléments de $\mathcal{S}_n$ s'appellent des *permutations*.

Notation $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

Attention, on écrit souvent $\sigma\sigma'$ pour $\sigma \circ \sigma'$.

3.1 Décomposition en cycles

Définition 3.1 *Soit $\sigma \in \mathcal{S}_n$ et soit $x \in \{1, \ldots, n\}$.*
On appelle orbite de x pour σ l'ensemble $\mathcal{O}_x = \{\sigma^k(x), k \in \mathbb{Z}\}$.

Lemme 3.2 *Soit $\sigma \in \mathcal{S}_n$. Les orbites pour σ forment une partition de $\{1, \ldots, n\}$.*

Démonstration : les orbites sont les classes d'équivalence pour la relation d'équivalence $\mathcal{R}$ sur $\{1, \ldots, n\}$ définie par : $x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z}, y = \sigma^k(x)$.

Définition 3.3 *Une permutation est un cycle si elle possède exactement une orbite non réduite à un élément. Cette orbite s'appelle le support du cycle. Son cardinal est la longueur du cycle.*
Un cycle de longueur 2 s'appelle une transposition.

Notation $(a_1 a_2 \ldots a_l)$ pour un cycle.

Lemme 3.4 *Deux cycles à supports disjoints commutent.*

Théorème 3.5 *Toute permutation ($\neq id$) se décompose en produit de cycles à supports disjoints et cette décomposition est unique à l'ordre des facteurs près.*

Application : calcul des puissances d'une permutation, de son ordre.

Exercice 3.6 *Quel est le plus petit n tel que $\mathcal{S}_n$ contienne un élément d'ordre 14?*

3.2 Conjugaison

Soit $c = (a_1 a_2 \ldots a_l)$ un cycle et σ une permutation quelconque de $\mathcal{S}_n$. Alors on a :

$$\sigma c \sigma^{-1} = (\sigma(a_1)\sigma(a_2)\ldots\sigma(a_l)).$$

Le conjugué d'un cycle est donc un cycle de même longueur.

Pour un produit de cycles $C = c_1 c_2 \ldots c_k$ on a :

$$\sigma C \sigma^{-1} = (\sigma c_1 \sigma^{-1})(\sigma c_2 \sigma^{-1}) \ldots (\sigma c_k \sigma^{-1}).$$

Ceci permet de montrer le théorème qui va suivre en ayant auparavant établi la notation suivante : pour $\sigma \in \mathcal{S}_n \setminus \{id\}$, on note $l(\sigma) = (l_1, \cdots, l_k)$, $l_1 \geq \ldots \geq l_k > 1$ les longueurs des cycles dans sa décomposition en cycles à supports disjoints. On pose $l(id) = 1$.

Théorème 3.7 *Soit $\sigma, \sigma' \in \mathcal{S}_n$. Alors σ et σ' sont conjugués dans $\mathcal{S}_n$ ssi $l(\sigma) = l(\sigma')$.*

Applications :

1) Parties génératrices de $\mathcal{S}_n$

Proposition 3.8 *1. $\mathcal{S}_n$ est engendré par les transpositions.*

2. $\mathcal{S}_n$ est engendré par les transpositions de type $(i, i+1)$.

3. $\mathcal{S}_n$ est engendré par les permutations (12) et $(12 \ldots n)$.

2) Centre de $\mathcal{S}_n$

Exercice 3.9 *1. Soit $\sigma \in \mathcal{S}_n$ et c un cycle de $\mathcal{S}_n$. Calculer $\sigma c \sigma^{-1}$.*

2. Soit σ un élément du centre de $\mathcal{S}_n$. Montrer que pour tous $1 \leq i \neq j \leq n$, σ préserve $\{i, j\}$.

3. En déduire le centre de $\mathcal{S}_n$, pour $n \geq 2$.

3.3 Signature

Définition 3.10 *Soit $\sigma \in \mathcal{S}_n$. On appelle signature de σ le nombre $\varepsilon(\sigma) = (-1)^{n-k}$ où k est le nombre d'orbites suivant σ. Si $\varepsilon(\sigma) = 1$, on dit que σ est paire, si $\varepsilon(\sigma) = -1$, on dit que σ est impaire.*

Proposition 3.11 (Signature d'un cycle) *Soit $c \in \mathcal{S}_n$ un cycle de longueur l. Alors $\varepsilon(c) = (-1)^{l-1}$. En particulier, toute transposition est impaire.*

Théorème 3.12 *$\varepsilon : \mathcal{S}_n \to \{-1, +1\}$ est un morphisme de groupes.*

Le *groupe alterné* $\mathcal{A}_n$ est le noyau de ε, c'est-à-dire l'ensemble des permutations paires de $\mathcal{S}_n$. C'est un sous-groupe distingué de $\mathcal{S}_n$ d'ordre $n!/2$.

Exemple : déterminer $\mathcal{A}_4$.

Exercice 3.13 *Dans le groupe $\mathcal{S}_7$ des permutations de $\{1, \ldots, 7\}$, considérons les éléments*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 1 & 7 & 3 & 4 & 2 \end{pmatrix} \text{ et } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 4 & 1 & 7 & 2 \end{pmatrix}$$

1. Décomposer σ et τ en produits de cycles à supports disjoints.

2. Ces deux éléments sont-ils conjugués ?

3. Quel est l'ordre de σ ? Quel est l'élément σ^{145} ?

4 Groupe des isométries affines

4.1 Groupe affine

Soit E un espace vectoriel sur $\mathbb{R}$ de dimension finie n et $\mathcal{E}$ un espace affine sur E. On s'intéresse à $(GA(\mathcal{E}), \circ)$, le groupe des bijections affines de $\mathcal{E}$, appelé *groupe affine* de $\mathcal{E}$.

Rappels : Pour toute application affine $f : \mathcal{E} \to \mathcal{E}$, on note $\overrightarrow{f} \in L(E)$ son application linéaire associée.
1. Une application affine est déterminée par son application linéaire associée et par l'image d'un point.
2. Si f et g sont affines, alors $f \circ g$ est affine d'application linéaire associée $\overrightarrow{f} \circ \overrightarrow{g}$.
3. Soit $f : \mathcal{E} \to \mathcal{E}$ affine. Si f est bijective, alors f^{-1} est affine.
4. Soit $f : \mathcal{E} \to \mathcal{E}$ affine. Alors f est bijective ssi $\overrightarrow{f}$ l'est.
5. L'application
$$\begin{array}{ccc} \Phi : (GA(\mathcal{E}), \circ) & \longrightarrow & (GL(E), \circ) \\ f & \longmapsto & \overrightarrow{f} \end{array}$$
est un morphisme de groupes surjectif.

Vocabulaire : une application affine bijective est souvent appelée *transformation affine*.

Quelques sous-groupes particuliers de $GA(\mathcal{E})$

1. $T(\mathcal{E}) = \ker \phi = \{f \in GA(\mathcal{E}), \overrightarrow{f} = id_E\} = \{t_v, v \in E\}$ est le sous-groupe des translations de $\mathcal{E}$ (on note t_v la translation de vecteur v). C'est un sous-groupe distingué (car noyau d'un morphisme de groupes). Ainsi le conjugué d'une translation par une bijection affine est une translation. Plus précisément : soit $g \in GA(\mathcal{E})$, soit $v \in E$, alors $g \circ t_v \circ g^{-1} = t_{\overrightarrow{g}(v)}$.

2. $HT(\mathcal{E}) = \phi^{-1}(\{\lambda id_E, \lambda \in \mathbb{R}^*\})$ est le sous-groupe des homothéties-translations.
(*Rappel* : Soit $f \in GA(\mathcal{E})$ tel que $\overrightarrow{f} = \lambda id_E$ avec $\lambda \in \mathbb{R} \setminus \{0, 1\}$. Alors f est une homothétie de rapport λ.)
C'est un sous-groupe distingué (car $\{\lambda id_E, \lambda \in \mathbb{R}^*\}$ est distingué dans $GL(E)$).
Soit $g \in GA(\mathcal{E})$, soit $h \in HT(\mathcal{E})$. On suppose que $h = hom(C, \lambda)$ (homothétie de centre C et de rapport λ). Alors on a : $g \circ h \circ g^{-1} = hom(g(C), \lambda)$.

3. $\phi^{-1}(\{id_E, -id_E\})$ est le sous groupe distingué des translations et symétries centrales.

4. $GA^+(\mathcal{E}) = \{f \in GA(\mathcal{E}), \det(\overrightarrow{f}) > 0\}$ est le sous-groupe des bijections affines positives. Il est distingué d'indice 2 dans $GA(\mathcal{E})$.

5. Soit X une partie de $\mathcal{E}$. $G_X = \{f \in GA(\mathcal{E}), f(X) = X\}$ est le groupe des transformations affines qui conservent X.
Cas particulier : $X = \{P\}$ où P est un point de $\mathcal{E}$. $G_{\{P\}}$ est le groupe des bijections affines qui laissent fixes P et il est isomorphe à $GL(E)$.
Remarque : si tous les éléments de G ont un point fixe en commun (ce qui arrive dès que X est fini: considérer l'isobarycentre des éléments de X), alors le problème, affine au départ, devient vectoriel (il revient au même d'étudier les éléments de G et leurs applications linéaires associées).

Exercice 4.1 (Groupe du triangle) *Soit $\mathcal{E}$ un plan affine et A_1, A_2, A_3 trois points non alignés de $\mathcal{E}$. On considère le triangle $T = \{A_1, A_2, A_3\}$. Alors G_T est isomorphe au groupe symétrique $\mathcal{S}_3$.*

Exercice 4.2 (Groupe du parallèlogramme) *Soit $\mathcal{E}$ un plan affine et $ABCD$ un parallèlogramme de $\mathcal{E}$. On note $X = \{A, B, C, D\}$ et Ω son isobarycentre.*

1. *Montrer que pour tout $f \in G_X$, $f(\Omega) = \Omega$.*
2. *En déduire que l'homomorphisme* $\left\{ \begin{array}{ccc} \Phi : G_X & \longrightarrow & GL(E) \\ f & \longmapsto & \overrightarrow{f} \end{array} \right.$ *est injectif. Ainsi G_X est isomorphe à $\Phi(G_X)$.*
3. *Montrer que pour tout $f \in GA(\mathcal{E})$, on a l'équivalence :*
   $f \in G_X$ si et seulement si $f(\Omega) = \Omega$ et la matrice de $\overrightarrow{f}$ dans la base $(\overrightarrow{\Omega A}, \overrightarrow{\Omega B})$ appartient à $\left\{ \begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix} \mid e, f \in \{+1, -1\} \right\} \bigcup \left\{ \begin{pmatrix} 0 & e \\ f & 0 \end{pmatrix} \mid e, f \in \{+1, -1\} \right\}$.
4. *Décrire géométriquement tous les éléments de G_X.*

4.2 Rappel : le groupe orthogonal

Soit E un espace vectoriel euclidien, c'est-à-dire un espace vectoriel sur $\mathbb{R}$ de dimension finie muni d'un produit scalaire. On note $< \cdot, \cdot >$ le produit scalaire et $\| \cdot \|$ la norme associée.

Proposition 4.3 *Pour tout $f \in GL(E)$, les propositions suivantes sont équivalentes :*

1. $\forall v \in E, \|f(v)\| = \|v\|$
2. $\forall v, w \in E, < f(v), f(w) >=< v, w >$
3. $f^* = f^{-1}$
4. *L'image par f d'une base orthonormée de E est une base orthonormée de E.*
5. *La matrice de f dans une base orthonormée de E est orthogonale.*

Si l'une des propriétés *1.* à *5.* est vérifiée, on dit que l'endomorphisme f est *orthogonal* (ou que f est une *isométrie vectorielle*).

On note $O(E)$ l'ensemble des isométries vectorielles de E. La propriété *1.* (par exemple) montre que les isométries vectorielles forment un sous-groupe de $GL(E)$.

Pour tout $f \in O(E)$, on a $\det f = \pm 1$. Si $\det f = +1$ (respectivement -1) on dit que f est *directe* (respectivement *indirecte*). L'ensemble des isométries vectorielles directes de E est noté $SO(E)$. C'est un sous-groupe distingué de $O(E)$.

4.3 Isométries affines

Soit $\mathcal{E}$ un espace affine euclidien, et E l'espace vectoriel (euclidien) associé. Rappelons que la norme sur E définit une distance sur $\mathcal{E}$.

Définition 4.4 *Une isométrie affine de $\mathcal{E}$ est une application affine de $\mathcal{E}$ dans $\mathcal{E}$ qui conserve les distances.*

Remarque : Soit $f \in GA(\mathcal{E})$. Alors f est une isométrie affine si et seulement si $\overrightarrow{f}$ est une isométrie vectorielle. En particulier toute isométrie affine est bijective.

On note :
- $Isom(\mathcal{E})$ l'ensemble des isométrie affines de $\mathcal{E}$. C'est un sous-groupe de $GA(\mathcal{E})$ (image réciproque de $O(E)$ par $\Phi : GA(\mathcal{E}) \to GL(E)$).
- $Isom^+(\mathcal{E}) = \{f \in Isom(\mathcal{E}), \det(\overrightarrow{f}) = 1\}$ le sous-groupe (distingué) des *déplacements* de $\mathcal{E}$.
- $Isom^-(\mathcal{E}) = \{f \in Isom(\mathcal{E}), \det(\overrightarrow{f}) = -1\}$ l'ensemble des *anti-déplacements* de $\mathcal{E}$.

Comme dans le cas plus général des transformations affines, on peut étudier les sous-groupe d'isométries laissant stables une partie de $\mathcal{E}$.

Rappel : la classification des isométries du plan et de l'espace
Les déplacements du plan sont (entre parenthèse l'ensemble des points fixes):

1. L'identité ($\mathcal{E}$)
2. Les rotations (1 point)
3. Les translations ($\emptyset$)

et les antidéplacements :

1. Les symétries orthogonales par rapport à une droite (1 droite)
2. Les symétries glissées ($\emptyset$)

Les déplacements de l'espace sont :

1. L'identité ($\mathcal{E}$)
2. Les rotations (1 droite)
3. Les vissages ($\emptyset$)
4. Les translations ($\emptyset$)

et les antidéplacements :

1. Les symétries orthogonales par rapport à un plan (1 plan)
2. Les symétries-rotations (1 point)
3. Les symétries glissées ($\emptyset$)

Exemples :

1. Le groupe du triangle (équilatéral) est isomorphe à $\mathcal{S}_3$.
2. Le groupe du tétraèdre (régulier) est isomorphe à $\mathcal{S}_4$.

Exercice 4.5 (Groupe diédral) *Soit $\mathcal{E}$ un plan affine euclidien orienté muni d'un repère orthonormé direct (O, u, v). Soit ρ la rotation de centre O d'angle $2\pi/n$, et soit σ la symétrie orthogonale par rapport à l'axe (O, u). On pose $P_0 = O + u$ et pour tout $i \in \{1, \dots, n-1\}$, $P_i = \rho^i(P_0)$. On appelle D_n le groupe des isométries qui envoient le polygone régulier $P_0P_1 \dots P_{n-1}$ sur lui-même.*

1. *Montrer que les isométries directes de D_n forment un sous-groupe cyclique engendré par ρ. Quel est l'ordre de ce sous-groupe ?*

2. *Montrer que tout élément de D_n est de la forme ρ^i ou $\rho^i \circ \sigma$ pour un $i \in \{0, \dots n-1\}$. Quel est l'ordre de D_n ?*

3. *Caractériser géométriquement les éléments de D_n (distinguer suivant la parité de n).*

4. *Montrer que $\sigma \circ \rho = \rho^{-1} \circ \sigma$ puis déterminer le produit de deux éléments quelconques de D_n.*

Exercice 4.6 (Groupe du cube) *Dans l'espace $\mathbb{R}^3$, on considère le cube $\mathcal{C}$ dont les sommets ont des coordonnées égales à ± 1. On appelle A_1, B_1, C_1 et D_1 les quatre sommets d'une face du cube et A_2, B_2, C_2 et D_2 les sommets opposés (symétriques par rapport a 0). On appelle H le groupe des isométries vectorielles de $\mathbb{R}^3$ qui envoient le cube $\mathcal{C}$ sur lui-même*

1. *Pourquoi le groupe des isométries affines qui conserve $\mathcal{C}$ est-il isomorphe à H ?*

2. *Montrer que tout élément de H permute les paires de sommets opposés. En déduire un homomorphisme Φ de H dans $\mathcal{S}_4$.*

3. *Déterminer le noyau de Φ.*

4. *Soit H^+ le sous-ensemble des déplacements de H. Montrer que H^+ est un sous-groupe de H. Quelle est l'image par Φ des retournements d'axe passant par les milieux des côtés opposés du cube? En déduire que la restriction de Φ à H^+ est surjective, puis montrer que c'est un isomorphisme.*

5. *Quel est l'ordre de H^+ ? Décrire tous ses éléments.*

6. *On considère l'application $\lambda : H^+ \times \mathbb{Z}/2\mathbb{Z} \to H$ définie par $\begin{cases} \lambda(f,0) = f \\ \lambda(f,1) = -id \circ f \end{cases}$ Montrer que λ est un isomorphisme de groupes. En déduire que H est isomorphe à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.*

4.4 Sous-groupes finis de $Isom(\mathcal{E})$

Proposition 4.7 *Soit $\mathcal{E}$ un espace affine euclidien (E l'espace vectoriel associé). Soit G un sous-groupe fini de $Isom(\mathcal{E})$. Alors il existe un point $\Omega \in \mathcal{E}$ qui est fixe pour tout élément de G.*

D'après cette proposition, l'étude des sous-groupes finis de $Isom(\mathcal{E})$ se ramène à l'étude des sous-groupes finis de $O(E)$.

On se place maintenant en dimension 2.

Théorème 4.8 *Soit E un espace vectoriel euclidien de dimension 2. Soit G un sous-groupe fini de $O(E)$. Alors soit G est un groupe cyclique soit G est isomorphe à un groupe diédral.*

5 Groupe opérant sur un ensemble

Définition 5.1 *Soit $(G, \cdot)$ un groupe et E un ensemble. On dit que G opère (ou agit) sur E s'il existe une application*

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

telle que :

1. $\forall g_1, g_2 \in G, \forall x \in E, g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$,
2. $\forall x \in E, 1_G \cdot x = x$.

Si on a une action de G sur E, alors pour tout $g \in G$, l'application $m_g : E \to E$ définie par $m_g(x) = g \cdot x$ est bijective : ainsi m_g appartient à $\mathcal{S}_E$ le groupe des bijections de E. En outre, l'application qui à $g \in G$ associe m_g est un morphisme de groupes de G dans $\mathcal{S}_E$.

Réciproquement, si on a un morphisme $\varphi : G \to \mathcal{S}_E$, on peut définir une action de G sur E par : $\forall x \in E, \forall g \in G, g \cdot x = \varphi(g)(x)$.

Ainsi, se donner une action de G sur E, c'est se donner un morphisme de groupes de $(G, \cdot)$ dans $(\mathcal{S}_E, \circ)$. De plus, si ce morphisme est injectif, on dit que l'action est *fidèle* (ce qui signifie que seul l'élément neutre du groupe agit trivialement).

Définition 5.2 *Soit $x \in E$. On appelle orbite de x l'ensemble $\mathcal{O}_x = \{g \cdot x, g \in G\}$.*
Lorsqu'il n'y a qu'une seule orbite, on dit que l'action est transitive.

Remarque : l'ensemble des orbites forme une partition de E.

Exemples :

1. (Extrait du livre de F.Combes "Algèbre et géométrie", Bréal, p44) On se demande combien on peut fabriquer de colliers différents avec 4 perles vertes, 3 blanches et 2 jaunes. On peut représenter un collier par une coloration des sommets d'un polygone régulier à 9 côtés en utilisant 4 fois la couleur verte, 3 fois la blanche et 2 fois la jaune et on appelle X l'ensemble de ces colorations. Le groupe diédral D_9 agit sur X, et deux colorations représentent le même collier si et seulement si elles sont dans la même orbite pour cette action. Le nombre de colliers est donc le nombre d'orbites, cardinal que l'on calculera un peu plus loin grâce à la formule de Burnside.
2. Le groupe symétrique $\mathcal{S}_n$ agit naturellement sur l'ensemble $\{1, \ldots, n\}$ et cette action est transitive et fidèle. Maintenant si on fixe $\sigma \in \mathcal{S}_n$ on peut restreindre cette action au sous-groupe $< \sigma >$. Elle reste fidèle mais elle n'est plus transitive en général : les orbites sont les orbites de σ... On en déduit que l'action est transitive si et seulement si σ est un n-cycle.
3. Soit G un groupe et E l'ensemble des sous-groupes de G. Alors l'application

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (g, H) & \longmapsto & gHg^{-1} \end{array}$$

définit une action de G sur E. L'orbite d'un sous-groupe H est l'ensemble des sous-groupes conjugués de H. Remarquons que H est distingué si et seulement si son orbite est le singleton $\{H\}$.

4. Si $\mathcal{E}$ est un espace affine, l'application

$$\begin{array}{ccc} GA(\mathcal{E}) \times \mathcal{E} & \longrightarrow & \mathcal{E} \\ (f, M) & \longmapsto & f(M) \end{array}$$

définit une action transitive et fidèle du groupe affine $GA(\mathcal{E})$ sur $\mathcal{E}$.

5. Si E est un espace vectoriel euclidien, l'application

$$\begin{array}{ccc} O(E) \times E & \longrightarrow & E \\ (f, u) & \longmapsto & f(u) \end{array}$$

définit une action fidèle du groupe orthogonal $O(E)$ sur E. Les orbites sont les sphères de E centrées en 0.

6. Soit $\mathcal{E}$ un plan affine euclidien. Alors $Isom(\mathcal{E})$ agit sur l'ensemble des triangles de $\mathcal{E}$. L'orbite d'un triangle t est l'ensemble des triangles isométriques à t. Cette action n'est pas transitive. En revanche, $Isom(\mathcal{E})$ agit transitivement sur l'ensemble des droites de $\mathcal{E}$ ou sur l'ensemble des points de $\mathcal{E}$.

Définition 5.3 *Soit $G \times E \to E$ une action de groupe. Soit $x \in E$. L'ensemble $G_x = \{g \in G, g \cdot x = x\}$ est un sous-groupe de G appelé stabilisateur de x.*
Lorsque tous les stabilisateurs sont triviaux, on dit que l'action est libre.

Remarque : une action libre est fidèle.

Dans l'exemple 6. ci-dessus, le stabilisateur d'un triangle équilatéral est le sous-groupe des isométries qui préservent le triangle (globalement). C'est le groupe diédral D_3 (isomorphe à $\mathcal{S}_3$). Ainsi cette action n'est pas libre.

Proposition 5.4 *On suppose que le groupe G agit sur l'ensemble E. Soit $x \in E$. Alors*

$$\begin{array}{ccc} \varphi : (G/G_x)_g & \longrightarrow & \mathcal{O}_x \\ gG_x & \longmapsto & g \cdot x \end{array}$$

définit une application bijective de l'ensemble des classes à gauches pour le stabilisateur de x dans l'orbite de x.

Conséquence : pour $x \in E$, on a $Card(\mathcal{O}_x) = [G : G_x]$. De plus, si E est fini, les orbites formant une partition de E, on a la :

Proposition 5.5 (Formule des classes) *Soit $G \times E \to E$ une action de groupe où l'ensemble E est fini soit $\mathcal{A}$ un ensemble de représentants des orbites. Alors*

$$Card(E) = \sum_{x \in \mathcal{A}} Card(\mathcal{O}_x) = \sum_{x \in \mathcal{A}} \frac{|G|}{|G_x|}$$

la deuxième égalité étant valable dans le cas où G est fini.

Enfin si le groupe G est également fini on a la :

Proposition 5.6 (Formule de Burnside) *Soit $G \times E \to E$ une action de groupe où l'ensemble E et le groupe G sont finis. Pour tout $g \in G$, on note $fix(g)$ l'ensemble des points fixes de E sous l'action de g. Alors le nombre d'orbites est donné par la formule :*

$$\frac{1}{|G|} \sum_{g \in G} Card(fix(g))$$

Démonstration : calculer le cardinal de l'ensemble $\{(g, x) \in G \times E, g \cdot x = x\}$ de deux façons différentes.

Application : en appliquant la formule de Burnside dans l'exemple 1. ci-dessus, on trouve qu'il y a 76 colliers différents réalisables avec 4 perles vertes, 3 blanches et 2 jaunes.

Opérations d'un groupe G sur lui-même

1. *Multiplication à gauche* : l'application

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & gx \end{array}$$

définit une action libre et transitive. En particulier l'action est fidèle ce qui signifie que le morphisme de groupes associé de G dans $\mathcal{S}_G$ est injectif. En conséquence on a le :

Théorème 5.7 (Théorème de Cayley) *Soit G un groupe fini d'ordre n.*
Alors G est isomorphe à un sous-groupe de $\mathcal{S}_n$.

2. *Conjugaison* : l'application

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & gxg^{-1} \end{array}$$

définit une action.
Soit $x \in G$. Le stabilisateur de x est le sous groupe de G des éléments qui commutent avec x: on l'appelle le *centralisateur* de x et on le note $Z(x)$. L'orbite de x est l'ensemble des conjugués de x (c'est la *classe de conjugaison* de x). On remarque que pour tout $x \in G$, on a l'équivalence : $x \in Z(G) \Leftrightarrow \mathcal{O}_x = \{x\}$. Cela permet de préciser la formule des classes :

Proposition 5.8 (Formule des classes pour l'action de conjugaison) *Soit G un groupe fini. Soit $\mathcal{A}$ un ensemble de représentants des classes de conjugaisons non réduites à un élément. Alors on a*

$$|G| = |Z(G)| + \sum_{x \in \mathcal{A}} \frac{|G|}{|Z(x)|}$$

Applications :

(a) Soit G un groupe d'ordre p^n (p premier, $n \in \mathbb{N}^*$). Alors $Z(G)$ est non trivial.

(b) Soit p un nombre premier. Alors tout groupe d'ordre p^2 est abélien.
Indication : montrer qu'un groupe G est abélien revient à montrer que $G = Z(G)$.

Contents