Cours

Groupes et actions de groupes

Le saviez-vous ?

La notion de *Groupe* émergea progressivement au cours du XIX^{eme} siècle. Evariste Galois et Niels Henrik Abel sont les premiers à l'avoir dégagée, dans leurs travaux respectifs sur la résolution par radicaux des équations polynômiales sur $\mathbb{Q}$. Les équations de degré 2, 3 et 4 avaient été résolues par des méthodes n'utilisant, outre les opérations élémentaires, que des extractions successives de racines n-ièmes. Abel, puis Galois ont montré que ce procédé (résolution par radicaux de l'équation) devenait insuffisant pour les équations de degré 5 ou plus.

Galois alla plus loin en introduisant ce qui deviendrait plus tard la notion de groupe afin de donner une condition nécessaire pour la résolution par radicaux d'une équation. Le principe de sa théorie est d'associer un groupe à l'équation étudiée, le Groupe de Galois de l'équation. Il s'agit, en termes vagues, de l'ensemble des permutations des racines qui laissent invariantes toutes les expressions algébriques de ces racines. Ce groupe exprime le degré d'indiscernabilité des racines. Le génie de Galois consiste à avoir trouvé une condition opératoire sur ce groupe qui est nécessaire pour que l'équation de départ soit résoluble par radicaux.

Dès lors, le concept moderne et abstrait de groupe se développa à travers différents champs des mathématiques (géométrie, théorie des nombres,...) de part son lien étroit avec la notion de symétrie. Il joue également un rôle important dans de nombreuses sciences. Les groupes généraux linéaires, par exemple, sont utilisés en physique fondamentale pour comprendre les lois de la relativité restreinte et les phénomènes liés à la symétrie des molécules en chimie.

Mathieu Mansuy
Professeur de Mathématiques en deuxième année de CPGE filière ECS au Lycée Louis Pergaud (Besançon)
Page personnelle : `http://mathieu-mansuy.fr/`
E-mail : `mansuy.mathieu@hotmail.fr`

1 Relations d'équivalences

1.1 Définitions et exemples

Définition.

Soit E un ensemble. On appelle *relation binaire* $\mathcal{R}$ sur E la donnée d'une partie

$$\Gamma \subset E \times E = \{(x, y),\ x, y \in E\}.$$

On dira qu'un élément $x \in E$ est *en relation* avec un autre élément $y \in E$ si $(x, y) \in \Gamma$. On notera alors $x\mathcal{R}y$.

Exemple. Pour $\Gamma = \{(x, x),\ x \in E\}$, on a $x\mathcal{R}y$ si et seulement si $x = y$.

Définition.

Une *relation d'équivalence* sur un ensemble E est une relation binaire $\mathcal{R}$ sur E qui est :

- *réflexive* : $\forall x \in E,\ x\mathcal{R}x$,
- *symétrique* : $\forall x, y \in E,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$,
- *transitive* : $\forall x, y, z \in E,\ x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

On définit la *classe d'équivalence modulo* $\mathcal{R}$ *d'un élément* $x \in E$, notée $\overline{x}$ ou $\mathcal{C}_{\mathcal{R}}(x)$, comme la partie de E donnée par :

$$\overline{x} = \mathcal{C}_{\mathcal{R}}(x) = \{y \in E,\ y\mathcal{R}x\} \in \mathcal{P}(E).$$

On appelle *représentant de la classe de* x tout élément de $\mathcal{C}_{\mathcal{R}}(x)$.

Exemples.

- La relation binaire $\mathcal{R}$ définie précédemment par $x\mathcal{R}y$ si et seulement si $x = y$, est une relation d'équivalence. La classe d'équivalence d'un élément x de E est donnée par le singleton $\{x\}$.
- On note $\overrightarrow{\mathcal{P}}$ l'ensemble des vecteurs du plan. On rappelle que deux vecteurs $\overrightarrow{e_1}$ et $\overrightarrow{e_2}$ sont colinéaires si et seulement s'il existe un réel k tel que $\overrightarrow{e_2} = k\overrightarrow{e_1}$ ou $\overrightarrow{e_1} = k\overrightarrow{e_1}$. La relation de colinéarité n'est pas une relation d'équivalence sur $\overrightarrow{\mathcal{P}}$ (elle est réflexive et transitive, mais elle n'est pas symétrique). Cependant la relation de colinéarité est bien une relation d'équivalence si on se restreint à l'ensemble $\overrightarrow{\mathcal{P}} \setminus \{\overrightarrow{0}\}$ des vecteurs non nuls du plan.
- Soit $n \in \mathbb{N}^*$. La relation de congruence modulo n est une relation d'équivalence. Il y a n classes d'équivalences distinctes, qui sont :
$$\overline{0}, \overline{1}, \cdots, \overline{n-1} \in \mathcal{P}(\mathbb{Z})$$
avec pour tout $0 \leq p \leq n-1$:
$$\overline{p} = \{q \in \mathbb{Z} \mid q \equiv p[n]\} = \{p + kn \mid k \in \mathbb{Z}\} = p + n\mathbb{Z}.$$

1.2 Ensemble quotient $E/\mathcal{R}$

Propriété 1

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E.

(1) $\overline{x} = \overline{y}$ si et seulement si $x\mathcal{R}y$.

(2) L'ensemble des classes d'équivalences constitue une partition de E, c'est-à-dire :

(a) pour tout $x \in E$, $\overline{x} \neq \emptyset$,

(b) pour tout $x, y \in E$ tels que $\overline{x} \neq \overline{y}$, on a : $\overline{x} \cap \overline{y} = \emptyset$,

(c) $E = \bigcup_{x \in E} \overline{x}$.

Preuve.

(1) Supposons que $\overline{x} = \overline{y}$. Puisque $\mathcal{R}$ est réflexive, on a $x \in \overline{x} = \overline{y}$. Ainsi $x \in \overline{y}$ et donc $x\mathcal{R}y$ par définition.

Réciproquement, on suppose que $x\mathcal{R}y$. Montrons que $\overline{x} = \overline{y}$. On procède par double inclusion : soit $z \in \overline{x}$, on a $z\mathcal{R}x$. Comme de plus $x\mathcal{R}y$, on obtient par transitivité de $\mathcal{R}$ que $z\mathcal{R}y$. Ainsi $z \in \overline{y}$ et on a montré que $\overline{x} \subset \overline{y}$. On montre de la même manière l'inclusion réciproque.

(2) Tout d'abord puisque $\mathcal{R}$ est réflexive, $x \in \overline{x}$ pour tout $x \in E$.

En particulier, $\overline{x} \neq \emptyset$.

On obtient également que $x \in \bigcup_{x\in E} \overline{x}$ et donc que $E = \bigcup_{x\in E} \overline{x}$.

Reste à montrer le deuxième point. On procède par contraposition : supposons que $\overline{x} \cap \overline{y} \neq \emptyset$ et soit $z \in \overline{x} \cap \overline{y}$. Alors $z\mathcal{R}x$ et $z\mathcal{R}y$. Par (1), on obtient donc :

$$\overline{x} = \overline{z} = \overline{y}.$$

□

Définition.

On appelle *ensemble quotient*, et on note $E/\mathcal{R}$, la partition de E formée de toutes les classes d'équivalence :

$$E/\mathcal{R} = \{\mathcal{C}_{\mathcal{R}}(x),\ x \in E\} \subset \mathcal{P}(E).$$

On appelle *système de représentants des classes* de E pour la relation d'équivalence $\mathcal{R}$ toute partie de E qui contient **exactement** un représentant par classe.

Exemples.

- On définit la relation binaire « être de la même classe » sur l'ensemble des étudiants de l'Université de Franche-Comté. C'est une relation d'équivalence dont les classes d'équivalence sont paramétrées par le nom de chaque section, un système de représentants des classes étant donné par exemple par la désignation d'un délégué par section.
- On définit la relation binaire suivante sur $\mathcal{M}_n(\mathbb{K})$:

$$M\mathcal{R}N \quad \Leftrightarrow \quad \exists P, Q \in GL_n(\mathbb{K}), \quad M = PNQ^{-1}$$

On vérifie que c'est une relation d'équivalence, deux matrices étant équivalentes si et seulement si elles sont de même rang. Et on montre qu'il y a $n+1$ classes d'équivalences, et qu'un système de représentants des classes d'équivalences est donné par l'ensemble des matrices $J_r = \begin{pmatrix} I_r & 0_{r,n-r} \\ 0_{n-r,r} & 0_{n-r,n-r} \end{pmatrix}$ pour $r \in \{0, \dots, n\}$.

Remarque. Supposons que E soit un ensemble fini, muni d'une relation d'équivalence $\mathcal{R}$, et notons $\mathcal{S}$ un système de représentants des classes d'équivalences. Puisque $E/\mathcal{R}$ est une partition de E, on a :

$$\mathrm{Card}(E) = \sum_{x\in\mathcal{S}} \mathrm{Card}(\mathcal{C}_{\mathcal{R}}(x)).$$

2 Groupes, sous-groupes

2.1 Groupes

Soit G un ensemble non vide muni d'une *loi de composition interne* notée $*$, c'est-à-dire d'une application de $G \times G$ dans G :

$$* : (x, y) \in G \times G \mapsto x * y \in G$$

Définition.

On dit que $(G, *)$ est un *groupe pour la loi* $*$ si :

- cette loi est *associative* : $\forall\ x, y, z \in G,\ x * (y * z) = (x * y) * z$,
- cette loi possède un *élément neutre* : $\exists\ e \in G,\ \forall\ x \in G,\ x * e = e * x = x$,
- tout élément admet un *symétrique* par cette loi : $\forall\ x \in G,\ \exists\ y \in G,\ x * y = y * x = e$.

Si de plus $*$ est *commutative*, c'est-à-dire : $\forall\ x, y \in G,\ x * y = y * x$, on dira que $(G, *)$ est un *groupe commutatif* ou *abélien*. Si G est fini, son cardinal $\mathrm{Card}(G)$ s'appelle *l'ordre* de G.

Remarque. On montre que :

- l'élément neutre e est unique, noté aussi 1_G. En effet, si e, e' sont des éléments neutres pour $(G, *)$, on a :
$$e = e * e' = e'.$$
- pour tout élément $x \in G$, le symétrique de x est unique. On l'appelle aussi *l'inverse* de x et on le note x^{-1}. En effet, si $x \in G$ et si y, y' sont des symétriques de x dans $(G, *)$, on a :
$$y = y * e = y * (x * y') = (y * x) * y' = e * y' = y'.$$

Lorsque le groupe est commutatif, on pourra préférer une notation additive : $+$ pour désigner la loi de G, 0_G pour l'élément neutre, et $-x$ pour le symétrique de x aussi appelé *opposé* de x dans ce cas.

Premiers exemples.

- $(\mathbb{Z}, +)$ est un groupe commutatif d'élément neutre $e = 0$. $(\mathbb{N}, +)$ n'est pas un groupe.
- Si $\mathbb{K}$ est un corps commutatif, alors $(\mathbb{K}^*, \times)$ est un groupe commutatif d'élément neutre $e = 1_{\mathbb{K}}$.
- Plus généralement pour tout anneau $(A, +, \times)$ unitaire, l'ensemble $\mathcal{U}(A)$ des éléments inversibles est un groupe pour la loi $\times$ d'élément neutre $e = 1_A$. Par exemple $(GL_n(\mathbb{K}), \times)$ est un groupe, non commutatif dès que $n \geq 2$, d'élément neutre $e = I_n$.
- Soit X un ensemble. Notons $\mathcal{S}(X)$ l'ensemble des *permutations* de X, c'est-à-dire des bijections de X dans lui-même. Alors $\mathcal{S}(X)$ est un groupe pour la loi de composition $\circ$ d'élément neutre l'application identité $e = \mathrm{Id}_X$. On l'appelle *groupe symétrique de* X. Ce groupe est non commutatif dès que X possède plus de 3 éléments.

  Si $X = \{1, 2, \ldots, n\}$ avec $n \geq 1$, on le notera plus simplement $\mathcal{S}_n$, et on l'appellera *groupe symétrique d'indice* n. Il est d'ordre $n!$. Un élément $\sigma \in \mathcal{S}_n$ se représente communément sous forme d'un tableau :
$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Exercice. Montrer que $\mathcal{S}_n$ n'est pas commutatif dès que $n \geq 3$.

On considère pour cela les deux permutations suivantes :
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 1 & 3 & 4 & \ldots & n \end{pmatrix} \quad \text{et} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 1 & 3 & 2 & 4 & \ldots & n \end{pmatrix}.$$
Alors on a :
$$\tau \circ \sigma(1) = \tau(2) = 3 \quad \text{et} \quad \sigma \circ \tau(1) = \sigma(1) = 2.$$
Ainsi $\tau \circ \sigma \neq \sigma \circ \tau$, et $\mathcal{S}_n$ n'est pas commutatif.

Exemple. Soient $(N, *)$ et $(H, *')$ deux groupes. Le produit cartésien $N \times H$ est muni d'une structure de groupe avec la loi produit $\star$ suivante :
$$(n, h) \star (n', h') = (n * n', h *' h').$$
On l'appelle le *produit direct des groupes* N *et* H. On vérifie que $e_{N \times H} = (e_N, e_H)$ et $(n, h)^{-1} = (n^{-1}, h^{-1})$. $N \times H$ est commutatif si et seulement si N et H sont commutatifs.

2.2 Sous-groupes

Définition.

Soit $(G, *)$ un groupe. On dit que $H \subset G$ est *un sous-groupe de* G, ce qu'on note $H < G$, si la restriction de la loi $*$ à H lui confère une structure de groupe.

Propriété 2 (Caractérisation des sous-groupes)

Soit G un groupe, et $H \subset G$. H est un sous-groupe de G si et seulement si

$$\begin{cases} e \in H \\ \forall\, x, y \in H,\ x * y^{-1} \in H \end{cases}$$

Exemples.

- L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est un sous-groupe de $(\mathbb{C}^*, \times)$. Pour tout $n \geq 2$, l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est lui-même un sous-groupe de $(\mathbb{C}^*, \times)$ (et de $(\mathbb{U}, \times)$ aussi). On a de plus les inclusions :
$$\mathbb{U}_m \subset \mathbb{U}_n \quad \Leftrightarrow \quad m \text{ divise } n.$$
En effet, si m divise n, alors il existe $k \in \mathbb{Z}$ tel que $n = km$, et alors pour tout $\xi \in \mathbb{U}_m$, on a :
$$\xi^n = \xi^{km} = (\xi^m)^k = 1^k = 1.$$
Réciproquement, si $\mathbb{U}_m \subset \mathbb{U}_n$ alors on aurait :
$$1 = (e^{\frac{2i\pi}{m}})^n = e^{\frac{2ni\pi}{m}} \Rightarrow \frac{n}{m} \in \mathbb{Z} \Rightarrow n \in m\mathbb{Z}.$$
- Notons $\mathcal{D}_n^*(\mathbb{K})$ (resp. $(\mathcal{T}_n^{\pm})^*(\mathbb{K})$) l'ensemble des matrices diagonales inversibles (resp. triangulaires supérieures/inférieures inversibles). Alors $D_n^*(\mathbb{K}), (\mathcal{T}_n^{\pm})^*(\mathbb{K})$ sont des sous-groupes de $GL_n(\mathbb{K})$.

Exercice. Le but de cet exercice est de montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les ensembles de la forme $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\}$ avec $n \geq 0$.

1. Montrer que pour tout $n \geq 0$, nZ est un sous-groupe de Z.
2. Soit H un sous-groupe de $(\mathbb{Z}, +)$, $H \neq \{0\}$.
   (a) Montrer que la partie $H \cap \mathbb{N}^*$ possède un plus petit élément. On note a cet élément.
   (b) Montrer que $a\mathbb{Z} \subset H$.
   (c) Montrer que $H \subset a\mathbb{Z}$ (penser à utiliser la division euclidienne).

1. On montre les différents points définissant un sous-groupe de $(\mathbb{Z}, +)$:
   - $0 = 0 \times n \in n\mathbb{Z}$;
   - Soient $a, b \in n\mathbb{Z}$, il existe $k, l \in \mathbb{Z}$ tels que $a = kn$ et $b = ln$. Alors $a+b = kn+ln = (k+l)n \in n\mathbb{Z}$;
   - Soit $a \in n\mathbb{Z}$, il existe $k \in \mathbb{Z}$ tel que $a = kn$. Alors $sym(a) = -a = -kn = (-k)n \in n\mathbb{Z}$.

   Ainsi $n\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$.
2. (a) Par hypothèse $H \neq \{0\}$, donc il existe $h \in H$ tel que $h \neq 0$. Si $h > 0$, c'est bon. Sinon, comme H est un groupe, on a $sym(h) = -h \in H$ et $-h > 0$. Dans tous les cas on a donc que $H \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}^*$. Elle possède donc un plus petit élément a.
   (b) Puisque $a \in H$ et que H est un sous-groupe, on a aussi $sym(a) = -a \in H$. On montre alors par une récurrence (à faire) que pour tout $k \in \mathbb{N}$, ka et $-ka$ appartiennent à H. Ainsi $a\mathbb{Z} \subset H$.
   (c) Soit $h \in H$. Montrons que $h \in a\mathbb{Z}$. Faisons la division euclidienne de h par a : il existe $q, r \in \mathbb{Z}$ tels que :
$$h = qa + r \text{ et } 0 \leq r < a.$$

On a $h \in H$, $qa \in a\mathbb{Z} \subset H$. Puisque H est un sous-groupe, on en déduit que $r = h - qa$ appartient à H. Par minimalité de a, on en déduit que $r = 0$. Ainsi on a bien $h = qa$, et donc $h \in a\mathbb{Z}$.

On a ainsi montré que tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ avec $n \geq 0$ (résultat à retenir).

Propriété 3

Soit $\{H_i\}_{i\in I}$ une famille de sous-groupes d'un groupe G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Preuve.

- Pour tout $i \in I$, $e \in H_i$ car H_i est un sous-groupe de G. Donc $e \in \bigcap_{i\in I} H_i$ et $\bigcap_{i\in I} H_i \neq \emptyset$.
- Soient $x, y \in \bigcap_{i\in I} H_i$. Alors pour tout $i \in I$, $x, y \in H_i$. H_i étant un sous-groupe de G, $x * y^{-1}$ appartient à H_i. Ceci étant vrai pour tout $i \in I$, on conclut que $x * y^{-1} \in \bigcap_{i\in I} H_i$.

□

2.3 sous-groupes engendrés par une partie

Définition.

Soit $(G, *)$ un groupe, et A un sous-ensemble non vide de G. Le *sous-groupe* $\langle A\rangle$ *de* G *engendré par* A est l'intersection de tous les sous-groupes de G qui contiennent A. On dit alors que A est une *partie génératrice* de $\langle A\rangle$.

Propriété 4

L'ensemble $\langle A\rangle$ coïncide avec l'ensemble des produits $x_1 \dots x_m$ où m est un entier positif non nul, et où pour tout $1 \leq i \leq m$, on a $x_i \in A$ ou $x_i^{-1} \in A$.

Exemple. Pour tout $x \in G$, on a $\langle x\rangle = \{x^m, m \in \mathbb{Z}\}$. On notera en particulier que $\langle x\rangle$ est un groupe commutatif.

Définition.

Un élément x de G est dit *d'ordre* $p \in \mathbb{N}^*$ si $\langle x\rangle$ est fini d'ordre p. L'ordre de x est aussi le plus petit entier naturel non nul p tel que $x^p = e$. On le note $o(x)$. On a :

$$\langle x\rangle = \{e, x, \dots, x^{p-1}\}.$$

Exemples.

- Soit $n \geq 2$. $\xi = e^{\frac{2i\pi}{n}}$ est un élément d'ordre n de $(\mathbb{C}^*, \times)$.
- Dans $\mathcal{S}_n$, on appelle *transposition* toute permutation de la forme

$$\tau_{i,j} = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$$

  où $1 \leq i < j \leq n$. Les transpositions sont des éléments d'ordre 2 dans $\mathcal{S}_n$.

Exercice. Montrer les assertions suivantes :

- Si x est d'ordre p, alors : $x^q = e \quad \Leftrightarrow \quad p|q$.
- Si x est d'ordre p, alors pour tout $k \in \mathbb{Z}$, x^k est d'ordre $\dfrac{p}{p \wedge k}$.

- Si p divise q, il existe $k \in \mathbb{Z}$ tel que $q = kp$. Dès lors, on a :
$$x^q = (x^p)^k = e^k = e.$$
Réciproquement supposons que $x^q = e$. On effectue la division euclidienne de q par p : il existe (r, s) un couple d'entiers tel que :
$$\begin{cases} q = pr + s \\ 0 \leq s < p \end{cases}$$
On a alors :
$$e = x^q = x^{pr+s} = (x^p)^r x^s = x^s.$$
Or $0 \leq s < p$. Par minimalité de p, on en déduit que $s = 0$, et donc que $q = pr$.
- Soit donc $k \in \mathbb{Z}$. Déterminons l'ordre q de x^k. On a :
$$e = (x^k)^q = x^{kq} \quad \text{d'où} \quad p \text{ divise } kq \quad \Leftrightarrow \quad \exists r \in \mathbb{Z}, kq = pr.$$
Soient $p', k' \in \mathbb{Z}$ tels que $\begin{cases} p = (p \wedge k)p' \\ k = (p \wedge k)k' \\ k' \wedge p' = 1 \end{cases}$. En substituant dans l'égalité précédente, on obtient $k'q = p'r$. On en déduit que :
$$\begin{cases} p' \text{ divise } k'q \\ p' \wedge k' = 1 \end{cases} \overset{\text{Gauss}}{\Rightarrow} \quad p' = \frac{p}{p \wedge k} \text{ divise } q.$$
D'autre part, on a $k \times \dfrac{p}{p \wedge k} = p \times \underbrace{\dfrac{k}{p \wedge k}}_{\in \mathbb{Z}}$ et donc $(x^k)^{\frac{p}{p \wedge k}} = (x^p)^{\frac{k}{p \wedge k}} = (e)^{\frac{k}{p \wedge k}} = e$. Ainsi q divise $\dfrac{p}{p \wedge k}$. Comme on a aussi montré que $\dfrac{p}{p \wedge k}$ divise q, on conclut que $q = \dfrac{p}{p \wedge k}$.

Définition.

- On dit qu'un groupe G est *monogène* s'il existe $x \in G$ tel que $G = \langle x \rangle$. Si de plus G est fini, on dit que G est cyclique.
- On dit qu'un groupe G est *de type fini* s'il existe un nombre fini d'éléments $x_1, \ldots, x_m$ de G tels que $G = \langle x_1, \ldots, x_n \rangle$. Un tel n-uplet $(x_1, \ldots, x_n)$ est appelé *système de générateurs de* G.

Exemples.

- $\mathbb{Z}$ et ses sous-groupes sont monogènes.
- Pour tout $n \geq 1$, $\mathbb{U}_n$ est un groupe cyclique engendré par $\xi = e^{\frac{2i\pi}{n}}$. D'autres générateurs sont possibles, précisés par l'équivalence suivante :
$$\mathbb{U}_n = \langle \xi^k \rangle \quad \Leftrightarrow \quad (k \wedge n = 1).$$
En effet on a les équivalences suivantes :
$$\mathbb{U}_n = \langle \xi^k \rangle \quad \Leftrightarrow \quad \xi^k \text{ est d'ordre } n \quad \Leftrightarrow \quad \frac{n}{n \wedge k} = n \quad \Leftrightarrow \quad n \wedge k = 1.$$
- $\mathbb{Z}^2$ est de type fini, engendré par les éléments $u_1 = (1, 0)$ et $u_2 = (0, 1)$. Il n'est pas monogène.

Exercice.

1. Montrer par récurrence sur $n \geq 2$ que le groupe symétrique $\mathcal{S}_n$ est de type fini, engendré par les transpositions.
2. Décomposer la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$ de $\mathcal{S}_5$ comme produits de transpositions.

1. On le montre par récurrence sur $n \geq 2$.

   Init. $\mathcal{S}_2 = \{Id, \tau_{1,2}\}$, donc $\mathcal{S}_2$ est bien engendré par les transpositions.

   Hér. Soit $n \geq 3$. Supposons la propriété au rang $n-1$. Soit $\sigma \in \mathcal{S}_n$. On a deux cas possibles :

   – $\sigma(n) = n$. Dans ce cas, σ peut-être vue comme une permutation $\tilde{\sigma}$ de $\{1, 2, \ldots, n-1\}$. Par hypothèse de récurrence, il existe $k \geq 0$ et $\tilde{\tau_1}, \ldots, \tilde{\tau_k}$ des transpositions de $\{1, 2, \ldots, n-1\}$ tels que :
   $$\tilde{\sigma} = \tilde{\tau_1} \circ \cdots \circ \tilde{\tau_k}.$$
   Pour tout $1 \leq i \leq k$, on définit alors la transposition $\tau_i \in \mathcal{S}_n$ par $\tau_i(j) = \begin{cases} \tilde{\tau_i}(j) & \text{si } j \neq n \\ n & \text{si } j = n \end{cases}$, et on vérifie qu'on a :
   $$\sigma = \tau_1 \circ \cdots \circ \tau_k.$$

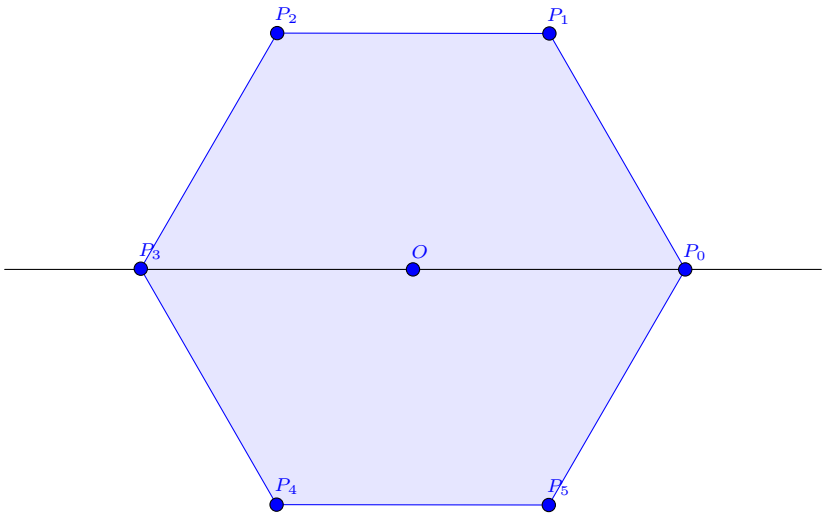
   – $\sigma(n) \neq n$. On note τ_0 la transposition permutant les entiers $\sigma(n)$ et n. On a $\tau_0 \circ \sigma(n) = n$. On est ramené ainsi au cas précédent : il existe $k \geq 0$ et des transpositions $\tau_i \in \mathcal{S}_n$ tels que :
   $$\tau_0 \circ \sigma = \tau_1 \circ \cdots \circ \tau_k$$
   soit encore :
   $$\sigma = \tau_0 \circ \tau_1 \circ \cdots \circ \tau_k.$$

   D'où la propriété au rang n.

   On conclut par principe de récurrence. On a d'ailleurs montré plus précisément que toute permutation de $\mathcal{S}_n$ est produit d'au plus $n-1$ transpositions.

2. Faisons un exemple. On considère la permutation suivante $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$ de $\mathcal{S}_5$. On s'inspire pour cela de la preuve précédente :
   $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \\ 3 & 2 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \begin{matrix} \\ \sigma \\ \tau_{2,5} \circ \sigma \\ \tau_{1,3} \circ \tau_{2,5} \circ \sigma \end{matrix}$$
   Ainsi on a $\tau_{1,3} \circ \tau_{2,5} \circ \sigma = \mathrm{Id}$, d'où :
   $$\sigma = (\tau_{1,3} \circ \tau_{2,5})^{-1} = \tau_{2,5}^{-1} \circ \tau_{1,3}^{-1} = \tau_{2,5} \circ \tau_{1,3}.$$

Exemple. Soit $n \geq 3$, et $P_0 P_1 \ldots P_{n-1}$ un polygone régulier à n côtés de centre O. On note $\mathcal{D}_{2n}$ l'ensemble des isométries du plan qui conservent ce polygone régulier. On montre facilement que c'est un sous-groupe du groupe des isométries du plan, appelé *le groupe diédral d'ordre* $2n$.



On note r la rotation de centre O envoyant P_0 sur P_1, et s la symétrie d'axe OP_0. Montrons que :

$$\mathcal{D}_{2n} = \{Id, r, \dots, r^{n-1}, s, r \circ s, \dots, r^{n-1} \circ s\}.$$

On a bien l'inclusion $\{Id, r, \dots, r^{n-1}, s, r \circ s, \dots, r^{n-1} \circ s\} \subset \mathcal{D}_{2n}$.
Réciproquement, soit f une isométrie conservant le polygone régulier. On sait que $f(O) = O$ (f conserve l'isobarycentre des sommets du polygone). On a alors plusieurs cas :

- Supposons que $f(P_0) = P_0$. On discute alors de $f(P_1)$, il s'agit d'un des sommets du polygone satisfaisant l'égalité des longueurs $P_0f(P_1) = P_0P_1$. On a donc deux cas possibles :
  - soit $f(P_1) = P_1$. Alors $f = Id$ car ces deux isométries coïncident en trois points non alignés du plan.
  - soit $f(P_1) = P_5$. Dans ce cas $f = s$ pour les mêmes raisons.
- Si $f(P_0) = P_k$ avec $1 \leq k \leq n-1$, alors $r^{-k} \circ f$ est une isométrie conservant le polygone et envoyant P_0 sur lui-même. On est donc dans le cas précédent :
  - soit $r^{-k} \circ f = Id$, et alors $f = r^k$;
  - soit $r^{-k} \circ f = s$, et alors $f = r^k \circ s$.

Ainsi $\mathcal{D}_{2n} = \langle r, s \rangle$, et $\{r, s\}$ est un système de générateurs du groupe $\mathcal{D}_{2n}$. On retiendra que $\mathcal{D}_{2n}$ est un groupe d'ordre $2n$, non commutatif (on vérifiera que $r \circ s \neq s \circ r$), ayant un sous-groupe cyclique $\langle r \rangle = \{Id, r, \dots, r^{n-1}\}$ d'ordre n.

3 Morphismes et actions de groupes

3.1 Morphismes de groupes

Définition.

Soient $(G, *)$ et $(G', *')$ deux groupes et une application $\varphi : G \to G'$. On dit que φ est un *morphisme de groupes* si

$$\forall\, x, y \in G, \quad \varphi(x * y) = \varphi(x) *' \varphi(y)$$

Remarque. Un morphisme de groupes $\varphi : G \to G'$ envoie l'élément neutre e de G sur l'élément neutre e' de G', et l'élément x^{-1} de G sur $f(x)^{-1}$ pour tout $x \in G$. En effet, on a :

$$\varphi(e) = \varphi(e * e) = \varphi(e) *' \varphi(e).$$

D'où en multipliant à gauche par $\varphi(e)^{-1}$, on obtient bien $\varphi(e) = e'$. Et pour tout $x \in G$, on a :

$$\varphi(x) *' \varphi(x^{-1}) = \varphi(x * x^{-1}) = \varphi(e) = e'.$$

De même on montre que $\varphi(x^{-1}) *' \varphi(x) = e'$, et donc $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Exemples.

- Le logarithme ln : $(\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ et l'exponentielle exp : $(\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ sont des morphismes de groupes.
- L'application déterminant det : $(GL_n(\mathbb{K}), \times) \to (\mathbb{K}^*, \times)$ est un morphisme de groupes.

Définition.

Soit $\sigma \in \mathcal{S}_n$. On appelle *signature* de σ le produit :

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Remarque. $\varepsilon(\sigma)$ vaut 1 si le nombre d'inversions (i.e. le nombre de paires $\{i, j\}$ $(1 \leq i < j \leq n)$ telles que $\sigma(j) - \sigma(i) < 0$) est paire, -1 sinon.

Propriété 5

La signature ε est un morphisme de groupes de $\mathcal{S}_n$ dans $\{-1, 1\}$

Preuve. Soient $\sigma_1, \sigma_2 \in \mathcal{S}_n$. On a :

$$\begin{aligned}
\varepsilon(\sigma_1 \circ \sigma_2) &= \prod_{1\leq i<j\leq n} \frac{\sigma_1\circ\sigma_2(j) - \sigma_1\circ\sigma_2(i)}{j-i} = \prod_{1\leq i<j\leq n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j)-\sigma_2(i)} \frac{\sigma_2(j)-\sigma_2(i)}{j-i} \\
&= \prod_{1\leq i<j\leq n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j)-\sigma_2(i)} \prod_{1\leq i<j\leq n} \frac{\sigma_2(j)-\sigma_2(i)}{j-i} \\
&= \prod_{1\leq \sigma_2(i)<\sigma_2(j)\leq n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j)-\sigma_2(i)} \prod_{1\leq i<j\leq n} \frac{\sigma_2(j)-\sigma_2(i)}{j-i} \\
&= \prod_{1\leq k<l\leq n} \frac{\sigma_1(l) - \sigma_1(k)}{l-k} \prod_{1\leq i<j\leq n} \frac{\sigma_2(j)-\sigma_2(i)}{j-i} = \varepsilon(\sigma_1)\varepsilon(\sigma_2)
\end{aligned}$$

□

Remarque. On vérifie que la signature d'une transposition vaut -1. Pour calculer la signature d'une permutation quelconque, on commence par la décomposer en un produit de k transpositions. La signature est alors $(-1)^k$.

Propriété 6

Soit $\varphi : G \to G'$ un morphisme de groupes.

- Pour tout sous-groupe H de G, $\varphi(H) := \{\varphi(h),\ h \in H\}$ est un sous-groupe de G'
- Pour tout sous-groupe H' de G', $\varphi^{-1}(H') := \{h \in G,\ \varphi(h) \in H'\}$ est un sous-groupe de G.

Preuve.

- $e' = \varphi(e) \in \varphi(H)$ (car e appartient à H sous-groupe). De plus pour tout $x', y' \in \varphi(H)$, il existe $x, y \in H$ tels que $x' = \varphi(x)$ et $y' = \varphi(y)$. On a alors :

  $$x' *' y'^{-1} = \varphi(x) *' \varphi(y)^{-1} = \varphi(x) *' \varphi(y^{-1}) = \varphi(x * y^{-1})$$

  qui appartient bien à $\varphi(H)$ car $x * y^{-1} \in H$ (H sous-groupe de G). Ainsi $\varphi(H)$ est bien un sous-groupe de G.

- $e \in \varphi^{-1}(H')$ car $\varphi(e) = e'$ appartient à H' sous-groupe. Soient à présent $x, y \in \varphi^{-1}(H')$, on a :

  $$\varphi(x * y^{-1}) = \underbrace{\varphi(x)}_{\in H'} *' \underbrace{\varphi(y)^{-1}}_{\in H'} \in H'$$

  car H' est un sous-groupe de G'. Ainsi $\varphi^{-1}(H')$ est bien un sous-groupe de G'.

□

On déduit de cette propriété que :

- $\mathrm{Im}(\varphi) = \varphi(G)$ est un sous-groupe de G' appelé *l'image* de φ. De plus, on a $\mathrm{Im}(\varphi) = G'$ si et seulement si φ est surjective.
- $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{e'\})$ est un sous-groupe de G appelé *le noyau* de φ. De plus, on a $\mathrm{Ker}(\varphi) = \{e\}$ si et seulement si φ est injective.

Exemple. $\mathcal{A}_n = \mathrm{Ker}(\varepsilon)$ est un sous-groupe de $\mathcal{S}_n$ de cardinal $\dfrac{n!}{2}$, appelé *groupe alterné*. Une permutation $\sigma \in \mathcal{S}_n$ est dite *paire* si $\sigma \in \mathcal{A}_n$, *impaire* sinon.

Si un morphisme de groupe $\varphi : G \to G'$ est bijectif, on dit que φ est un *isomorphisme*. Si $\varphi : G \to G$ est un isomorphisme de G dans G, on dit que f est un *automorphisme*. On vérifie que l'ensemble $\mathrm{Aut}(G)$ des automorphismes du groupe G est un groupe pour la composition.

Un classe importante d'automorphismes de G est donnée par la propriété suivante.

Propriété 7

Soit G un groupe, et a un élément de G. L'application $\varphi_a : G \to G, x \mapsto a * x * a^{-1}$ est un automorphisme de G appelé *automorphisme intérieur associé à* a. De plus, l'ensemble $\mathrm{Int}(G)$ des automorphismes intérieurs de G est un sous-groupe de $\mathrm{Aut}(G)$.

Preuve. Soit $a \in G$. Montrons que φ_a est un morphisme de groupes de G dans G. Pour tout $x, y \in G$, on a :

$$\varphi_a(x * y) = a * (x * y) * a^{-1} = a * x * a * a^{-1} * y * a^{-1} = \varphi(x) * \varphi(y).$$

Donc φ_a est un morphisme de groupes. De plus, pour tout $a, b \in G$, on a :

$$\forall x \in G, \quad \varphi_a \circ \varphi_b(x) = \varphi_a(b * x * b^{-1}) = a * b * x * b^{-1} * a^{-1} = (a * b) * x * (a * b)^{-1} = \varphi_{a*b}(x).$$

et

$$\forall x \in G, \quad \varphi_e(x) = e * x * e^{-1} = Id(x)$$

On en déduit en particulier que pour tout $a \in G$, on a :

$$\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a*a^{-1}} = \varphi_e = Id = \varphi_{a^{-1}} * \varphi_a.$$

Ainsi on a bien que pour tout $a \in G$, $\varphi_a \in \mathrm{Aut}(G)$.
Finalement, on a montré que :

- $\mathrm{Int}(G) \subset \mathrm{Aut}(G)$;
- $\mathrm{Id} = \varphi_e \in \mathrm{Int}(G)$;
- $\forall a, b \in G$, $\varphi_a \circ \varphi_b^{-1} = \varphi_{a*b^{-1}} \in \mathrm{Int}(G)$.

Donc $\mathrm{Int}(G)$ est un sous-groupe de $\mathrm{Aut}(G)$. □

3.2 Actions de groupes

Si on veut avoir une image « géométrique » d'un groupe G, on peut tenter de « réaliser » G comme sous-groupe du groupe des permutations d'un ensemble X, c'est-à-dire de trouver un morphisme injectif de G dans $\mathcal{S}(X)$. Une représentation moins « fidèle » est fournie par un morphisme quelconque de G dans $\mathcal{S}(X)$. On obtient les définitions suivantes.

Définition.

Une opération (ou action) de $(G, *)$ sur X est la donnée d'un morphisme ρ de G dans $\mathcal{S}(X)$.

Remarque. L'action de $(G, *)$ sur X se note plus simplement $g \cdot x = \rho(g)(x)$ pour tout $g \in G$ et $x \in X$. On notera que :

$$(1) \quad \forall (g, g') \in G^2, \ \forall x \in X, \ g \cdot (g' \cdot x) = (g * g') \cdot x \qquad (2) \quad \forall x \in X, \ e \cdot x = x.$$

Réciproquement, toute application $G \times X \to X$ vérifiant ces deux points définit une action de G sur X.

Définition.

On dit que l'action est *fidèle* si $\rho : G \to \mathcal{S}(X)$ est injective, c'est-à-dire si :

$$\forall x \in X, \quad g \cdot x = x \quad \Rightarrow \quad g = e.$$

L'action est *transitive* si :

$$\forall (x, x') \in X, \quad \exists g \in G, \quad g \cdot x = x'.$$

Quelques exemples classiques.

- Un groupe G opère sur lui-même de deux manières fondamentales :
  - par translation à gauche (resp. à droite) :
$$G \times G \to G, \quad (g,x) \mapsto g * x \quad (resp.\ G \times G \to G, \quad (g,x) \mapsto x * g^{-1}).$$
    Cette action est fidèle et transitive.
  - par conjugaison :
$$G \times G \to G, \quad (g,x) \mapsto g * x * g^{-1}.$$
- Si X est une partie d'un espace affine euclidien E, l'ensemble G des isométries de E qui laissent X globalement invariant est un sous-groupe de $\mathrm{Is}(E)$ qui opère naturellement sur X. L'opération est fidèle si et seulement si X engendre E, c'est-à-dire n'est contenue dans aucun sous-espace affine strict. On a définit ainsi le groupe diédral $\mathcal{D}_{2n}$ comme étant l'ensemble des isométries du plan laissant stable un polygone régulier à n côtés. On définit de même le groupe du tétraèdre, le groupe du cube, etc.
- Citons encore l'action du groupe linéaire $GL_n(\mathbb{K})$ sur $\mathbb{K}^n$, de $O_n(\mathbb{R})$ sur la sphère unité de $\mathbb{R}^n$. Ces actions sont fidèles et transitives.

Définition.

Soit G un groupe agissant sur un ensemble X. Pour tout $x \in X$, on appelle :

- *orbite de x* (ou *trajectoire*) le sous-ensemble $\mathcal{O}_x = \{g \cdot x, g \in G\}$ de X ;
- *stabilisateur de x* le sous-ensemble $G_x = \{g \in G, g \cdot x = x\}$.

Remarque. On notera que l'action de G sur X est transitive si et seulement si il n'y a qu'une seule orbite.

Propriété 8

(1) Les orbites pour l'action de G sur X forment une partition de X.

(2) Pour tout $x \in X$, G_x est un sous-groupe de G.

(3) Si $y = g \cdot x$ est dans l'orbite de x, alors $g * G_y * g^{-1} = G_x$, et donc les sous-groupes G_y et G_x sont isomorphes via un automorphisme intérieur de G.

Preuve. Démontrons (1). Pour cela on introduit la relation binaire $\sim$ sur X suivante, dont on vérifie qu'il s'agit d'une relation d'équivalence :

$$x \sim y \quad \Leftrightarrow \quad \exists g \in G,\ y = g \cdot x.$$

Pour cette relation d'équivalence, on note que la classe d'équivalence d'un élément $x \in X$ n'est autre que son orbite $\mathcal{O}_x$ sous l'action de G. Ces classes d'équivalences formant une partition de X, on en déduit le résultat.
Montrons (2). On a $e.x = x$ donc $e \in G_x$. De plus pour tout $g, g' \in G_x$, on a :

$$g \cdot x = x \text{ et } g' \cdot x = x \quad \Leftrightarrow \quad x = g'^{-1} \cdot x.$$

On en déduit que :

$$g * g'^{-1} \cdot x = g \cdot (g'^{-1} \cdot x) = g \cdot x = x$$

et donc $g * g'^{-1}$ appartient à G_x. G_x est donc bien un sous-groupe de G.
On montre enfin (3). On a :

$$\begin{aligned} g' \in G_y &\Leftrightarrow g' \cdot y = y \Leftrightarrow g' \cdot (g \cdot x) = g \cdot x \\ &\Leftrightarrow (g^{-1} * g' * g) \cdot x = x \Leftrightarrow g^{-1} * g' * g \in G_x \end{aligned}$$

□

Exemple. Les orbites du groupe orthogonal $O_n(\mathbb{R})$ dans son action naturelle sur $\mathbb{R}^n$ sont les sphères de centre l'origine.

Considérons l'action naturelle de $\mathcal{S}_n$ sur $X = \{1, 2, \dots, n\}$:

$$\mathcal{S}_n \times X \to X, \quad (\sigma, i) \to \sigma(i).$$

Cette action est fidèle et transitive. Soit $\gamma \in \mathcal{S}_n$. Alors le groupe cyclique $\langle\gamma\rangle$ agit aussi sur X.

Définition.

Soit $\gamma \in \mathcal{S}_n$. On dit que γ est un *cycle* si parmi les orbites de X sous l'action de $\langle\gamma\rangle$, il n'existe qu'une seule orbite non réduite à un élément, autrement dit s'il existe $p \geq 2$ et $i \in \{1, \dots, n\}$ tels que :

$$\mathcal{O}_i = \{i, \gamma(i), \dots, \gamma^{p-1}(i)\} \quad \text{et} \quad \forall j \notin \mathcal{O}_i,\ \gamma(j) = j.$$

L'orbite $\mathcal{O}_i$ s'appelle le *support* du cycle, son cardinal est la *longueur* du cycle, et on note $\gamma = (i, \gamma(i), \dots, \gamma^{p-1}(i))$.

Exemples.

- Une transposition est un cycle de longueur 2.
- $\gamma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 4 & \dots & 1 \end{pmatrix} \in \mathcal{S}_n$ est un cycle de longueur n, qu'on notera donc $\gamma = (1, 2, 3, \dots, n)$.
- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in \mathcal{S}_4$ n'est pas un cycle puisque $\mathcal{O}_1 = \{1, 2\}$ et $\mathcal{O}_3 = \{3, 4\}$.

Remarques.

- Des cycles à supports disjoints commutent.
- L'ordre d'un cycle est sa longueur.
- La signature d'un cycle de longueur p est $(-1)^{p-1}$. En effet, si $\gamma = (a_1, a_2, \dots, a_p)$ est un cycle de longueur p, alors on vérifie que :

$$\gamma = (a_1, a_p)(a_1, a_{p-1}) \dots (a_1, a_3)(a_1, a_2) \quad \text{produit de } p-1 \text{ transpositions}$$

et donc $\varepsilon(\gamma) = (-1)^{p-1}$.

Théorème 9

Toute permutation $\sigma \neq Id$ se décompose de manière unique à l'ordre près en un produit de cycles dont les supports sont deux à deux disjoints.

Preuve. Soient $\mathcal{O}_{i_1}, \dots, \mathcal{O}_{i_r}$ les orbites de X sous l'action de $\langle\sigma\rangle$. Alors les permutations σ_j définies par :

$$\sigma_j(x) = \begin{cases} x & \text{si } x \notin \mathcal{O}_{i_j} \\ \sigma(x) & \text{si } x \in \mathcal{O}_{i_j} \end{cases}$$

sont des cycles d'ordre $\text{Card}(\mathcal{O}_{i_j})$, deux à deux permutables car de supports disjoints, et on a $\sigma = \sigma_1 \circ \dots \circ \sigma_r$. □

Exemple. Considérons $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix} \in \mathcal{S}_8$. On a $\mathcal{O}_1 = \{1, 3, 4, 5\}$, $\mathcal{O}_2 = \{2, 6, 8\}$ et $\mathcal{O}_7 = \{7\}$, et $\sigma = (1, 3, 4, 5)(2, 6, 8)(7) = (1, 3, 4, 5)(2, 6, 8)$ (inutile d'écrire les cycles d'ordre 1).

4 Classes à gauche, groupes quotients

4.1 Classes à droite, classes à gauche

Soit G un groupe, H un sous-groupe de G. Le sous-groupe H agit sur G par translation à gauche comme suit :

$$H \times G \to G, \quad (h, g) \mapsto h * g.$$

Les orbites pour cette action sont de la forme $Hg = \{h * g,\ h \in H\}$. Elles sont appelées *classes à droites* de G. Elles forment une partition de G, et on note $H\backslash G$ l'ensemble des classes à droite.

On définit de même les *classes à gauches* de G par $gH = \{g * h, h \in H\}$ pour tout $g \in G$, notée dans la suite $[g]$. Elles forment aussi une partition de G (en faisant cette fois agir H sur G par translation à droite), et on note G/H l'ensemble des classes à gauche.

Les classes à gauches ont un lien important avec les orbites.

Propriété 10

L'application $G/G_x \to \mathcal{O}_x, [g] \mapsto g \cdot x$ est bien définie et établit une bijection (ensembliste).

Preuve. Montrons tout d'abord que cette application est bien définie. Soit pour cela g' pris dans la classe à gauche de g. On peut donc écrire $g' = g * h$ avec $h \in G_x$. On a :

$$g' \cdot x = (g * h) \cdot x = g \cdot (h \cdot x) = g \cdot x.$$

D'où la bonne définition de cette application : l'image de $[g]$ ne dépend pas du représentant de la classe de g choisi.
Montrons à présent son injectivité : soient pour cela g_1 et g_2 tels que $g_1 \cdot x = g_2 \cdot x$. Alors on a :

$$(g_2^{-1} g_1) \cdot x = g_2^{-1} \cdot (g_1 \cdot x) = g_2^{-1} \cdot (g_2 \cdot x) = (g_2^{-1} g_2) \cdot x = e \cdot x = x.$$

Ceci nous montre que $g_2^{-1} g_1$ appartient à G_x, soit encore que $g_1 \in g_2 G_x$. On a donc bien $[g_1] = [g_2]$.

□

4.2 Groupes quotients

On souhaite munir l'ensemble G/H des classes à gauche d'une structure naturelle de groupe, pour laquelle la *projection canonique* $\pi : G \to G/H, g \mapsto [g]$ soit un morphisme de groupes. Cela revient à définir si possible une loi sur G/H, encore notée $*$, satisfaisant :

$$\forall g_1, g_2 \in G, \quad [g_1] * [g_2] = [g_1 * g_2].$$

Une telle loi n'existe pas toujours. Le résultat suivant nous donne les propriétés que le sous-groupe H doit satisfaire pour cela.

Propriété 11

Soit G un groupe et H un sous-groupe. Les conditions suivantes sont équivalentes.

(1) G/H est muni d'une structure naturelle de groupe ;

(1') $H\backslash G$ est muni d'une structure naturelle de groupe ;

(2) Toute classe à droite est aussi une classe à gauche, i.e. $x * H = H * x$ pour tout $x \in G$;

(3) Pour tout $x \in G$, $x * H * x^{-1} \subset H$.

Preuve.

(1) ⇒ (3) (1) implique en particulier que $[e] * [g^{-1}] = [e * g^{-1}] = [g^{-1}]$ et donc que $H * (g^{-1} * H) = g^{-1} H$. Et comme $e \in H$, on obtient que :

$$H * g^{-1} = H * g^{-1} * e \subset g^{-1} * H$$

Il vient donc que $g * H * g^{-1} \subset H$, d'où la stabilité.

(3) $\Rightarrow$ (2) On a donc $g*H*g^{-1} \subset H$, mais aussi en changeant g en g^{-1}, $g^{-1}*H*g \subset H$, c'est à dire $H \subset g*H*g^{-1}$. D'où l'égalité $g*H*g^{-1} = H$ et donc $g*H = H*g$.

(2) $\Rightarrow$ (1) Comme (2) est vrai, on a :

$$\begin{aligned}[g_1]*[g_2] &= (g_1*H)*(g_2*H) = g_1*(H*g_2)*H = g_1*(g_2*H)*H \\ &= (g_1*g_2)*(H*H) = (g_1*g_2)*H = [g_1*g_2].\end{aligned}$$

Comme (1) et (1′) jouent des rôles similaires, on a bouclé la propriété. □

Définition.

Un sous-groupe H vérifiant une de ces conditions est appelé *sous-groupe distingué* de G, ce qu'on note $H \lhd G$. $(G/H, *)$ est alors *le groupe quotient G sur H*.

Remarque. $\{e\}$ et G sont des sous-groupes distingués dans G. Tout sous-groupe d'un groupe abélien G est distingué dans G.

Exemple. Soit G un groupe. On appelle centre du groupe l'ensemble $\mathcal{Z}(G)$ des éléments qui commutent avec tous les autres éléments de G, soit :

$$\mathcal{Z}(G) = \{x \in G,\ \forall y \in G,\ x*y = y*x\}.$$

On vérifie facilement que $\mathcal{Z}(G)$ est un sous-groupe distingué de G.

Exemple fondamental. Soit $n \geq 1$, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$, distingué puisque $(\mathbb{Z}, +)$ est commutatif. On définit alors le groupe quotient $\mathbb{Z}/n\mathbb{Z}$, cyclique d'ordre n.

Propriété 12

Soit $\varphi : G \to G'$ un morphisme de groupes, et H' un sous-groupe distingué de G'. Alors $\varphi^{-1}(H')$ est un sous-groupe distingué de G.

Preuve. On a déjà établi que $\varphi^{-1}(H')$ est un sous-groupe de G. Montrons que ce sous-groupe est distingué. Soient $h \in \varphi^{-1}(H')$ et $g \in G$, on a :

$$\varphi(g*h*g^{-1}) = \varphi(g) *' \underbrace{\varphi(h)}_{\in H'} *' \varphi(g)^{-1} \in H' \text{ car } H' \text{ distingué dans } G'$$

Ainsi $g*h*g^{-1} \in \varphi^{-1}(H')$, et $\varphi^{-1}(H')$ est un sous-groupe distingué de G. □

Remarque. Ce n'est pas vrai en général pour l'image direct $\varphi(H)$ d'un sous-groupe distingué de G.

Remarque. Le sous-groupe trivial $\{e'\}$ étant distingué dans G', on déduit de la propriété précédente que $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{e'\})$ est distingué dans G. Par exemple, le groupe alterné $\mathcal{A}_n$ est un sous-groupe distingué de $\mathcal{S}_n$.

Théorème 13

Soit $\varphi : G \to G'$ un homomorphisme de groupes. L'application $\overline{\varphi} : [x] \mapsto \varphi(x)$ définit un isomorphisme entre les groupes $G/\mathrm{Ker}(\varphi)$ et $\mathrm{Im}(\varphi)$.

Preuve. Vérifions tout d'abord que $\overline{\varphi}$ est bien définie. Soit pour cela $x' \in [x]$. Il existe donc $h \in \mathrm{Ker}(\varphi)$ tel que $x' = x*h$, et on a :

$$\varphi(x') = \varphi(x*h) = \varphi(x) *' \varphi(h) = \varphi(x) *' e' = \varphi(x).$$

Donc l'application $\overline{\varphi}$ est bien définie. Elle définit donc un morphisme de groupes de $G/\mathrm{Ker}(\varphi)$ à valeurs dans $\mathrm{Im}(\varphi)$ par définition. Elle est par définition surjective, et injective car :

$$\overline{\varphi}(x) = e' \Leftrightarrow \varphi(x) = e' \Leftrightarrow x \in \mathrm{Ker}(\varphi) \Leftrightarrow [x] = [e].$$

Donc φ définit bien un isomorphisme entre les groupes $G/\mathrm{Ker}(\varphi)$ et $\mathrm{Im}(\varphi)$. □

Comme application de ce résultat, on a la propriété suivante.

Propriété 14

Tout groupe monogène est isomorphe à $\mathbb{Z}$ s'il est infini, à $(\mathbb{Z}/n\mathbb{Z})$ s'il est fini d'ordre $n \geq 1$.

Preuve. Soit $G = \langle a \rangle$ un groupe monogène. On définit l'application :

$$\varphi : \mathbb{Z} \to G, \quad k \mapsto a^k.$$

On vérifie facilement que φ est un morphisme surjectif. On a alors deux cas possibles :

- soit φ est injectif, alors G est infini et φ est un isomorphisme de $\mathbb{Z}$ sur G ;
- soit $\mathrm{Ker}(\varphi) \neq \{0\}$ et c'est un sous-groupe de $\mathbb{Z}$, alors il existe $n > 1$ tel que $\mathrm{Ker}(\varphi) = n\mathbb{Z}$. Par le résultat précédent, on en déduit que G est fini, isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

□

Le saviez-vous ?

L'intérêt des sous-groupes distingués est de permettre le « dévissage » des groupes : si G est un groupe et si on a un sous-groupe distingué H dans G, on peut essayer de ramener l'étude de G à celles de H et G/H censées être plus aisé[a], en montrant par exemple que G est isomorphe au produit direct $G/H \times H$. Pour des exemples de dévissages (produits directs et semi-directs), voir [8].
Certains groupes G sont cependant « indévissables » car ils ne possèdent pas de sous-groupes distingués autres que $\{e\}$ et G. On les appelle des *groupes simples*. Ce sont les « briques fondamentales » dans le dévissage des groupes. Donnons deux exemples de groupes simples :

- On pourra montrer à titre d'exercice que $\mathbb{Z}/p\mathbb{Z}$ est un groupe simple si et seulement si p est premier (utilise le théorème de Lagrange).
- Le groupe alterné $\mathcal{A}_n$ est simple pour $n \geq 5$ (voir [8] pour une démonstration).

La classification des groupes simples finis a été achevée en 1981. C'est en fait un ensemble de travaux, comprenant des dizaines de milliers de pages publiées dans 500 articles par plus de 100 auteurs. Les groupes finis simples se répartissent ainsi :

1. les groupes cycliques $\mathbb{Z}/p\mathbb{Z}$ avec p premier ;
2. les groupes alternés $\mathcal{A}_n$ pour $n \geq 5$;
3. les groupes finis du type de Lie ;
4. les 26 groupes sporadiques, nommés ainsi car ils ne correspondent pas à une répartition en "familles" cohérentes comme les autres.

Parmi les groupes sporadiques, citons comme exemple le Monstre (de Fischer), le plus gros des groupes sporadiques, de cardinal :

$$2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71 (\simeq 8 \times 10^{53} ...).$$

[a] si G est fini par exemple, ces groupes sont de cardinal plus petit comme on va le voir à la section suivante.

5 Groupes finis

5.1 Théorème de Lagrange

Soit G un groupe fini, H un sous-groupe de G. Faisons encore agir H sur G par translation à droite. Les orbites sont les classes à gauches $[g] = gH$, toutes de cardinal $\mathrm{Card}(H)$ ($h \mapsto gh$ définissant une bijection de H sur gH). Puisqu'elles forment une partition de G, on obtient ainsi que :

$$\mathrm{Card}(G) = \sum_{[g]\in G/H} \mathrm{Card}([g]) = \sum_{[g]\in G/H} \mathrm{Card}(H) = \mathrm{Card}(G/H)\mathrm{Card}(H).$$

D'où le résultat suivant.

Théorème 15 (Lagrange)

Soit G un groupe fini. L'ordre de tout sous-groupe H de G divise l'ordre du groupe.

Remarque. L'entier $\mathrm{Card}(G/H)$ est appelé *indice de H dans G*, et noté $[G : H]$. On retiendra :

$$\mathrm{Card}(G) = [G : H] \times \mathrm{Card}(H).$$

Par exemple, $[\mathcal{S}_n : \mathcal{A}_n] = 2$.

En appliquant le résultat précédent à $H = \langle a\rangle$ pour $a \in G$, on obtient le

Théorème 16

Si G est fini d'ordre n, alors l'ordre de tout élément de G divise n. En particulier, tout élément a de G vérifie $a^n = e$.

Comme application directe, on a la propriété suivante.

Propriété 17

Soit G un groupe d'ordre p premier. Alors $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Preuve. Soit $a \in G$, $a \neq e$. Alors l'ordre de a divise l'ordre de G, c'est à dire p. C'est donc 1 ou p. Comme $a \neq e$, l'ordre de a est donc p. On en déduit donc que $G = \langle a\rangle$ est cyclique d'ordre p, et par une proposition précédente que $G \simeq \mathbb{Z}/p\mathbb{Z}$. □

5.2 Équation aux classes

Soit toujours G un groupe fini agissant sur un ensemble X lui aussi supposé fini.

Pour tout $x \in X$, nous avons établi une bijection entre les ensembles G/G_x et $\mathcal{O}_x$. On en déduit une première égalité sur les cardinaux de ces ensembles :

$$\mathrm{Card}\,(G/G_x) = \mathrm{Card}(\mathcal{O}_x), \quad \text{soit encore} \quad \frac{\mathrm{Card}(G)}{\mathrm{Card}(G_x)} = \mathrm{Card}(O_x).$$

De plus, puisque les orbites sous l'action de G forment une partition de X, on obtient :

$$\mathrm{Card}(X) = \sum_{x\in\mathcal{S}} \mathrm{Card}(\mathcal{O}_x) = \sum_{x\in\mathcal{S}} \frac{\mathrm{Card}(G)}{\mathrm{Card}(G_x)}$$

où $\mathcal{S}$ désigne un système de représentants des orbites pour l'action de G sur X. On note en passant que si le sous-groupe G_x dépend du choix de x dans son orbite, son ordre, lui, n'en dépend pas. Cette égalité est appelée l'équation aux classes.

5.3 Application aux automorphismes intérieurs

Soit G un groupe fini. On applique l'équation aux classes dans le cas particulier de l'action de G sur lui-même par conjugaison :

$$(G,G) \to G, \quad (g,x) \mapsto g*x*g^{-1}.$$

On obtient :

$$\mathrm{Card}(G) = \sum_{\mathcal{O}} \mathrm{Card}(\mathcal{O}).$$

Or on a pour tout $x \in G$:

$$\mathrm{Card}(O_x) = 1 \quad \Leftrightarrow \quad \forall g \in G, g*x = x*g \quad \Leftrightarrow \quad x \in \mathcal{Z}(G).$$

Et si $\mathrm{Card}(\mathcal{O}_x) > 1$, alors on sait que $\mathrm{Card}(O_x) = \dfrac{\mathrm{Card}(G)}{\mathrm{Card}(G_x)}$ avec $G_x \neq G, \{e\}$ car $x \notin \mathcal{Z}(G)$ et car $\{e,x\} \subset G_x$.
On en déduit l'existence d'une famille finie $(H_i)_{i\in I}$ de sous-groupes stricts de G (i.e. $\neq G, \{e\}$) telle que :

$$\begin{aligned}\mathrm{Card}(G) &= \sum_{\mathrm{Card}(\mathcal{O})=1} \mathrm{Card}(\mathcal{O}) + \sum_{\mathrm{Card}(\mathcal{O})>1} \mathrm{Card}(\mathcal{O}) \\ &= \mathrm{Card}(\mathcal{Z}(G)) + \sum_{i\in I} \frac{\mathrm{Card}(G)}{\mathrm{Card}(H_i)}.\end{aligned}$$

Donnons ici une application classique à l'étude des p-groupes. Un p-groupe est un groupe dont l'ordre est une puissance de p.

Propriété 18

Le centre d'un p-groupe est non trivial.

Preuve. On utilise la formule obtenue précédemment : il existe une famille finie $(H_i)_{i\in I}$ de sous-groupes stricts de G telle que :

$$\mathrm{Card}(G) = \mathrm{Card}(\mathcal{Z}(G)) + \sum_{i\in I} \frac{\mathrm{Card}(G)}{\mathrm{Card}(H_i)}.$$

Les entiers $\mathrm{Card}(G)$ et $\dfrac{\mathrm{Card}(G)}{\mathrm{Card}(H_i)}$ sont divisibles par p. Donc p divise $\mathrm{Card}(Z(G))$. Comme $\mathrm{Card}(Z(G)) \geq 1$, on en déduit que $Z(G)$ n'est pas réduit à $\{e\}$. □

5.4 Formule de Burnside

On cherche à dénombrer le nombre d'orbites $\mathrm{Card}(X/G)$.

Théorème 19 (Burnside)

On a :

$$\mathrm{Card}(X/G) = \frac{1}{\mathrm{Card}(G)} \sum_{g\in G} \mathrm{Card}(X_g)$$

où $X_g = \{x \in X,\ g\cdot x = x\}$.

Preuve. On va calculer de deux façon le cardinal de l'ensemble $R = \{(g,x),\ g\cdot x = x\}$.

- Si on fixe $x \in X$, on a $\mathrm{Card}(G_x)$ possibilités pour g, soit :

$$\mathrm{Card}(R) = \sum_{x\in X} \mathrm{Card}(G_x).$$

On peut alors regrouper tous les x d'une même orbite puisque leurs stabilisateurs étant conjugués, sont de même cardinal. Cela donne :

$$\begin{aligned}\mathrm{Card}(R) &= \sum_{[x]\in X/G} \mathrm{Card}(G_x) \times \mathrm{Card}(\mathcal{O}_x) = \sum_{[x]\in X/G} \mathrm{Card}(G_x)\frac{\mathrm{Card}(G)}{\mathrm{Card}(G_x)} = \sum_{[x]\in X/G} \mathrm{Card}(G) \\ &= \mathrm{Card}(X/G)\mathrm{Card}(G).\end{aligned}$$

- Si on fixe à présent $g \in G$, alors on a $\mathrm{Card}(X_g)$ possibilités pour x, d'où :

$$\mathrm{Card}(R) = \sum_{g \in G} \mathrm{Card}(X_g).$$

D'où le résultat avec les deux formules obtenues. □

Les exemples d'applications de cette formules sont nombreux, en particulier en dénombrement, par exemple dans les problèmes de coloriage ou de colliers de perles.

Prolongements possibles

On indique ici quelques thèmes d'études éventuels pour approfondir les notions introduites dans ce cours.

- Les théorèmes de Sylow. Voir par exemple [2, 8, 6].
- La simplicité de $\mathcal{A}_n$ pour $n \geq 5$. Voir par exemple [2, 8, 9].
- Produits direct et semi-direct de groupes. Voir par exemple [8].
- Groupes d'isométries des polyèdres réguliers de l'espace. Groupes de frises. Sous-groupes finis des isométries de l'espace. Voir par exemple [3, 6].

Cette liste est bien sûr non exhaustive.

References

[1] Boucekkine, F. Introduction à la Théorie des Groupes. Polycopié, `http://culturemath.ens.fr/`.

[2] Calais, J. Éléments de théorie des groupes. Cours et exercices.

[3] Caldero, P. Carnet de voyage en Algébrie. Exercices corrigés.

[4] Caldero, P. Groupes et Actions de groupes. Polycopié, `http://math.univ-lyon1.fr/ caldero/Agreginterne.html`.

[5] Debeaumarché, G. Manuel de Mathématiques, Volumes 2 et 4, Algèbre et géométrie. Cours et exercices.

[6] Francinou, S., Gianella, H. et Nicolas, S. Exercices de mathématiques, oraux x-ens. Exercices corrigés.

[7] Gourdon, X. Les maths en tête, Algèbre. Résumé de cours et exercices corrigés.

[8] Perrin, D. Cours d'algèbre. Cours et exercices.

[9] Tauvel, P. Algèbre pour l'agrégation interne. Cours.