Théorie des groupes

Pourquoi les groupes ?

Il est bien clair pour le géomètre que si l'on démontre une propriété pour tous les cercles centrés en un point O du plan, alors cette propriété est valable pour tous les cercles, quelle que soit la place de leur centre.

Il est bien clair aussi que parmi les entiers n entre 0 et 99, dénombrer les pairs ou les impairs donne le même résultat.

On sait qu'en algèbre linéaire, pour calculer certains invariants d'un endomorphisme f (comme son déterminant) ou comparer des endomorphismes (comme dans le théorème de Cayley-Hamilton, où l'on prouve qu'un certain polynôme en f est nul), on peut se placer dans la base que l'on souhaite. Par exemple, une base de trigonalisation, ou une base formée des itérés sous f d'un vecteur.

L'idée mathématique qui suggère ces remarques est la même dans les trois cas. Dans ces situations comme dans de nombreuses autres en mathématiques, ce que l'on souhaite étudier n'est pas vraiment un objet particulier mais des propriétés de cet objet indépendantes de sa position particulière dans l'espace ; ou de sa position dans un ensemble particulier qui le contient ; ou du nom qui a été donné de manière temporaire à cet objet. Dans ce cas-là, on peut utiliser des transformations de l'espace pour déplacer l'objet, ou l'envoyer sur un autre objet qui lui ressemble (nous dirons *isomorphe* : qui a la même forme). Les ensembles de transformations que l'on est amené à considérer possèdent à chaque fois les propriétés d'un *groupe*. Voici le « pourquoi » des groupes.

Les nombreux exemples à notre disposition illustreront ces propos un peu abstraits dans une profusion de situations très concrètes.

Table des matières

1 Groupes, sous-groupes

Définition 1.1 Un *groupe* est un triplet (G, m, e) composé d'un ensemble G, d'une application $m : G \times G \to G$ (aussi appelée loi de composition interne) et d'un élément $e \in G$ tels que :

i) la loi m est *associative* : $\forall (g_1, g_2, g_3) \in G^3$, $m(m(g_1, g_2), g_3) = m(g_1, m(g_2, g_3))$,

ii) l'élément e est *neutre* : $\forall g \in G$, $m(e, g) = m(g, e) = g$,

iii) tout élément possède un *symétrique* : $\forall g \in G$, $\exists \widetilde{g} \in G$, $m(g, \widetilde{g}) = m(\widetilde{g}, g) = e$.

Remarques 1.2 1) La plupart du temps, pour simplifier l'écriture, on emprunte en général la notation usuelle de la multiplication et on note $g_1 g_2$ au lieu de $m(g_1, g_2)$, la loi m étant sous-entendue. Alors, les axiomes ci-dessus deviennent :

i) $\forall (g_1, g_2, g_3) \in G^3$, $(g_1, g_2)g_3 = g_1(g_2, g_3)$,

ii) $\forall g \in G$, $eg = ge = g$,

iii) $\forall g \in G$, $\exists \widetilde{g} \in G$, $g\widetilde{g} = \widetilde{g}g = e$.

Conformément à cette notation multiplicative, le symétrique est en général appelé l'inverse et noté g^{-1}. Enfin, le neutre e est souvent noté 1.

2) Dans le même souci de simplifier les notations, on note en général simplement G au lieu de (G, m, e). C'est un abus d'écriture, car pour un même ensemble G, il peut y avoir plusieurs lois m, m' qui en font un groupe de manière différente. Par exemple, les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont deux groupes différents avec le même ensemble sous-jacent, un ensemble à quatre éléments. Néanmoins, cet abus sera inoffensif lorsque la loi du groupe est claire d'après le contexte.

Propriétés 1.3 *L'élément neutre e d'un groupe G est forcément unique. L'inverse g^{-1} d'un élément g est nécessairement unique. De plus, l'inverse vérifie les propriétés suivantes :*

- pour tout $g \in G$, on a $(g^{-1})^{-1} = g$.

- pour tout $(g_1, g_2) \in G^2$, on a $(g_1 g_2)^{-1} = (g_2)^{-1}(g_1)^{-1}$.

Démonstration : Il s'agit de manipulations avec les axiomes de la définition d'un groupe.

Si e et e' vérifient la propriété de l'élément neutre, alors comme e est neutre on a $ee' = e'$ et comme e' est neutre on a $ee' = e$, donc $e = e'$. Donc le neutre est unique.

Si $\widetilde{g}$ et $\overline{g}$ vérifient la propriété de symétrique (ou d'inverse) de g, alors $\widetilde{g} = \widetilde{g}e = \widetilde{g}g\overline{g} = e\overline{g} = \overline{g}$. Donc l'inverse de g est unique.

Les égalités $gg^{-1} = g^{-1}g = e$ disent que g est l'inverse de g^{-1}, c'est-à-dire $(g^{-1})^{-1} = g$.

Enfin, pour voir que $(g_2)^{-1}(g_1)^{-1}$ est l'inverse de $g_1 g_2$ il faut voir que $(g_1 g_2)((g_2)^{-1}(g_1)^{-1}) = e$ et $((g_2)^{-1}(g_1)^{-1})(g_1 g_2) = e$, ce qui est clair. □

Exemples 1.4 - Le groupe des bijections d'un ensemble E, muni de la loi donnée par la composition des bijections, et de l'application identité comme élément neutre. Ce groupe est noté $(S_E, \circ, \mathrm{id}_E)$ ou simplement S_E. On trouve aussi les notations $S(E)$, $\mathfrak{S}_E$, $\mathfrak{S}(E)$ [1].

- $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$.
- $(\mathbb{Q}^*, \times, 1)$, $(\mathbb{R}^*, \times, 1)$, $(\mathbb{R}^{+*}, \times, 1)$, $(\mathbb{C}^*, \times, 1)$.
- $(\mathbb{U}, \times, 1)$ où $\mathbb{U}$ est l'ensemble des nombres complexes de module 1.
- groupes cycliques, groupes diédraux, groupes symétriques, groupes alternés,
- espaces vectoriels sur un corps k,
- ensembles de polynômes ou de fonctions (continues, dérivables...),

[1] La lettre '$\mathfrak{S}$' est le 'S' gothique.

- $\mathrm{GL}_n(K)$, $\mathrm{SL}_n(K)$, $\mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$,
- groupe des translations d'un espace affine, des isométries affines, homothéties, similitudes,
- groupe des homographies $h : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$.

Définitions 1.5 Soit $G = (G, m, e)$ un groupe. Un *sous-groupe H de G* est un sous-ensemble $H \subset G$ tel que :

i) H contient e,

ii) H est *stable par produit* : $\forall (h_1, h_2) \in G^2$, $h_1 h_2 \in H$,

iii) H est *stable par inversion* : $\forall h \in H$, $h^{-1} \in H$.

Un sous-groupe est un groupe à part entière, lorsqu'on oublie qu'il est sous-ensemble d'un plus gros groupe.

Proposition 1.6 *Soit $\{H_i\}_{i\in I}$ une famille de sous-groupes de G. Alors l'intersection des H_i est un sous-groupe.*

Démonstration : Notons $H = \cap_{i\in I} H_i$. L'élément e est dans tous les H_i, donc il est dans leur intersection H. Soient h_1, h_2 deux éléments de H. Alors, pour chaque $i \in H$ ils sont dans H_i, donc $h_1 h_2 \in H_i$ puisque H_i est un sous-groupe. Il s'ensuit que $h_1 h_2$ est dans tous les H_i, donc dans H. Pour finir, si $h \in H$, alors $h \in H_i$ pour tout i, donc $h^{-1} \in H_i$ puisque H_i est un sous-groupe, et ainsi $h^{-1} \in H$. On a bien montré que H est un sous-groupe de G. □

Proposition 1.7 *Soit G un groupe et soit A une partie de G. Alors, il existe un plus petit sous-groupe de G contenant A. Ce sous-groupe est noté $\langle A \rangle$ et peut être décrit des deux manières suivantes :*

i) c'est l'ensemble des produits $a_1 \dots a_n \in G$ où $n \geq 0$ est entier et pour tout $i \geq 1$, $a_i \in A$ ou $a_i^{-1} \in A$ (on considère que le produit vide est égal à e et fait partie de cet ensemble).

ii) c'est l'intersection des sous-groupes de G contenant A.

Démonstration : Notons $\{H_i\}_{i\in I}$ la famille des sous-groupes de G contenant A. D'après la proposition précédente, l'intersection $H = \cap_{i\in I} H_i$ est un sous-groupe de G. Il est clair que H contient A ; et par ailleurs tout sous-groupe K contenant A est l'un des H_i et donc contient H, qui est leur intersection. Ceci montre que H est le plus petit des sous-groupes de G contenant A.

Considérons maintenant l'ensemble E des produits $a_1 \dots a_n \in G$ avec n entier et pour tout i, $a_i \in A$ ou $a_i^{-1} \in A$. Cet ensemble contient e. De plus, étant donnés deux éléments $a_1 \dots a_n$ et $b_1 \dots b_m$, il est clair que le produit $a_1 \dots a_n b_1 \dots b_m$ est encore dans E, puisque c'est un produit d'un certain nombre d'éléments appartenant, eux ou leur inverse, à A. Enfin, l'inverse de $a_1 \dots a_n$ est $(a_n)^{-1} \dots (a_1)^{-1}$ (voir la remarque 5 ci-dessus), c'est encore un élément de E. Il s'ensuit que E est un sous-groupe de G contenant A. Par ailleurs, si un sous-groupe quelconque H de G contient A, alors d'après les propriétés de sous-groupe, il contient tous les inverses des éléments de A, et aussi tous les produits d'un certain nombre (fini) d'éléments de A et d'inverses d'éléments de A. Donc H contient E. Finalement E est le plus petit des sous-groupes de G contenant A. □

Définition 1.8 Le sous-groupe $\langle A \rangle$ est appelé *sous-groupe de G engendré par A.*

Exemple 1.9 Toujours en cohérence avec la notation multiplicative, pour tout entier $k \geq 1$, le produit d'un élément $g \in G$ par lui-même k fois est noté g^k, et le produit de g^{-1} par lui-même k fois est noté g^{-k}. On convient que $g^0 = e$. Alors, il est facile de vérifier que le sous-groupe de G engendré par le singleton $A = \{g\}$ est l'ensemble $\{g^k,\ k \in \mathbb{Z}\}$.

2 Morphismes de groupes

Définition 2.1 Soient G et G' deux groupes. Un *morphisme (de groupes)* de G dans G' est une application $f : G \to G'$ telle que pour tous g_1, g_2 dans G on a $f(g_1 g_2) = f(g_1)f(g_2)$.

Exemples 2.2 - Si H est un sous-groupe de G, alors l'inclusion $i : H \to G$ définie par $i(h) = h$ est un morphisme de groupes. Par exemple, les inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des morphismes de groupes.

- le déterminant $\mathrm{GL}_n(k) \to k^*$.
- l'exponentielle $\exp : \mathbb{R} \to \mathbb{R}^{+*}$.
- toute application linéaire entre deux k-espaces vectoriels.

Remarque 2.3 Pour tout morphisme de groupes $f : G \to G'$, on a $f(e)f(e) = f(ee) = f(e)$ ce qui montre, en composant à droite par $f(e)^{-1}$, que $f(e) = e'$.

De plus, pour tout $g \in G$, on a $f(g)f(g^{-1}) = f(gg^{-1}) = f(e) = e'$ et $f(g)^{-1}f(g) = f(g^{-1}g) = f(e) = e'$, ce qui montre que $f(g^{-1}) = f(g)^{-1}$.

En résumé, un morphisme de groupes envoie le neutre sur le neutre et l'inverse sur l'inverse.

En général, il y a d'autres éléments que e qui s'envoient sur e', et l'ensemble de ces éléments est suffisamment important dans la théorie pour mériter un nom. Nous l'introduisons maintenant.

Définition 2.4 Soit $f : G \to G'$ un morphisme de groupes.

Le *noyau* de f, noté $\ker(f)$, est l'ensemble des $g \in G$ tels que $f(g) = e'$.

L'*image* de f, notée $\mathrm{im}(f)$, est l'ensemble des $g' \in G'$ tels qu'il existe $g \in G$ vérifiant $g' = f(g)$.

Proposition 2.5 *Pour tout morphisme de groupes $f : G \to G'$, le noyau $\ker(f)$ est un sous-groupe de G et l'image $\mathrm{im}(f)$ est un sous-groupe de G'.*

Démonstration : La vérification est facile et laissée comme un bon exercice d'entraînement pour la lectrice. □

Proposition 2.6 *Un morphisme de groupes $f : G \to G'$ est injectif ssi $\ker(f) = \{e\}$.*

Lorsqu'on a un morphisme injectif $f : G \to G'$, on dit parfois que G *se plonge* dans G' via f.

Démonstration : On sait que $\{e\} \subset \ker(f)$, on doit donc montrer que f est injectif ssi $\ker(f) \subset \{e\}$. Supposons que f est injectif, alors pour tout élément $g \in \ker(f)$, on a $f(g) = e' = f(e)$ donc $g = e$ par injection ; ainsi $\ker(f) \subset \{e\}$. Réciproquement, supposons que $\ker(f) \subset \{e\}$ et soient g_1, g_2 tels que $f(g_1) = f(g_2)$. Alors $f(g_1(g_2)^{-1}) = f(g_1)f(g_2)^{-1} = e'$ donc $g_1(g_2)^{-1} \in \ker(f)$. D'après l'hypothèse, on trouve $g_1(g_2)^{-1} = e$ donc $g_1 = g_2$. Ainsi, f est injectif. □

Définition 2.7 Si un morphisme de groupes $f : G \to G'$ est bijectif, on dit que c'est un *isomorphisme*. Si de plus $G' = G$, on dit que f est un *automorphisme* de G. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

Il est facile de vérifier que la bijection réciproque d'un isomorphisme ou d'un automorphisme est encore un morphisme de groupes.

On définit maintenant des automorphismes extrêmement importants d'un groupe G : les *automorphismes intérieurs* ou *conjugaisons*. Pour $g \in G$, la conjugaison par g est l'application :

$$\begin{array}{rccc} c_g : & G & \to & G \\ & h & \mapsto & ghg^{-1} \ . \end{array}$$

Il est facile de voir que c_g est un morphisme de groupes : pour x, y dans G on a $c_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = c_g(x)c_g(y)$. On note $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs. L'énoncé suivant indique le lien précis entre G et ses automorphismes intérieurs ; pour donner un énoncé complet, nous utilisons la notion de sous-groupe distingué introduite plus bas, dans la définition 4.1.

Proposition 2.8 *Soit G un groupe.*

1) L'ensemble $\mathrm{Aut}(G)$ est un sous-groupe du groupe des bijections de G.

2) L'application $c : G \to \mathrm{Aut}(G)$ qui envoie g sur c_g est un morphisme de groupes.

3) L'image de c, c'est-à-dire $\mathrm{Int}(G)$, est un sous-groupe distingué de $\mathrm{Aut}(G)$.

4) Le noyau de c est égal au centre $Z(G)$ de G.

Démonstration : 1) Il est clair que l'identité id_G est un automorphisme de groupes de G. Vérifions que le composé $f = f_1 \circ f_2$ de deux automorphismes $f_1, f_2 : G \to G$ est un automorphisme. Soient g, g' deux éléments de G, on a alors $f(gg') = f_1(f_2(gg')) = f_1(f_2(g)f_2(g')) = f_1(f_2(g))f_1(f_2(g')) = f(g)f(g')$, comme on le voulait. Il n'est pas plus difficile de vérifier que la bijection réciproque f^{-1} d'un automorphisme $f : G \to G$ est un automorphisme.

2) Pour tout $h \in G$, on a $c_{gg'}(h) = (gg')h(gg')^{-1} = gg'h(g')^{-1}g^{-1} = c_g(c_{g'}(h))$ ce qui montre que $c_{gg'} = c_g \circ c_{g'}$, donc c est un morphisme de groupes.

3) Comme c est un morphisme, son image est un sous-groupe. Il n'y a qu'à voir qu'il est distingué dans $\mathrm{Aut}(G)$. Pour cela, on doit vérifier que pour tout automorphisme φ de G, l'automorphisme $\varphi \circ c_g \circ \varphi^{-1}$ de G est intérieur. Or

$$(\varphi c_g \varphi^{-1})(h) = \varphi(g\varphi^{-1}(h)g^{-1}) = \varphi(g)\varphi(\varphi^{-1}(h))\varphi(g^{-1}) = \varphi(g)h\varphi(g)^{-1} = c_{\varphi(g)}(h) \ .$$

On voit donc que $\varphi c_g \varphi^{-1} = c_{\varphi(g)}$ qui est bien un automorphisme intérieur.

4) Un élément $g \in \ker(c)$ est tel que pour tout $h \in G$, on a $ghg^{-1} = h$. Ceci signifie que $gh = hg$, c'est-à-dire que g commute avec tous les $h \in G$ donc g est dans le centre de G. □

3 Classes à gauche et à droite modulo un sous-groupe

Définition 3.1 Soit G un groupe. Pour tout $g \in G$, on définit des applications :

- translation à gauche $\gamma_g : G \to G$, $\gamma_g(x) = gx$.
- translation à droite $\delta_g : G \to G$, $\delta_g(x) = xg$.

Proposition 3.2 *Ces applications sont bijectives et les γ_g donnent lieu à un morphisme injectif de groupes $\gamma : G \to S_G$ qui envoie g sur γ_g.*

Démonstration : Le fait que γ_g est bijective est clair car on vérifie aussitôt que $\gamma_{g^{-1}}$ en est une bijection réciproque. Une remarque similaire vaut pour δ_g. Il s'ensuit que $\gamma_g \in S_G$. Pour voir

que $g \mapsto \gamma_g$ soit un morphisme de groupes, il suffit de constater que pour tout $x \in G$, on a $\gamma_{gh}(x) = (gh)x = g(hx) = (\gamma_g\gamma_h)(x)$. Il ne nous reste qu'à voir que γ est injectif. Or si $\gamma_g = \gamma_{g'}$, pour tout $x \in G$ on $gx = g'x$ donc $g = g'$. □

Remarques 3.3 1) Les γ_g et δ_g sont bijectives mais *ne sont pas* des morphismes de groupes : si $g \neq 1$, elles n'envoient même pas e sur e. En revanche, on a vu qu'en combinant translation à gauche (par g) et à droite (par g^{-1}), on obtenait un morphisme : la conjugaison c_g.

2) Pour fabriquer un morphisme de groupes $G \to S_G$ avec les δ_g, il faut considérer l'application $g \mapsto \delta_{g^{-1}}$. Si on omet l'inverse, on obtient une application δ qui vérifie $\delta(gh) = \delta(h)\delta(g)$ ce qui ne donne pas un morphisme.

3) la proposition 3.2 montre que les groupes de bijections S_X ont un rôle fondamental dans la théorie : tout groupe peut être vu comme un sous-groupe d'un tel groupe S_X, précisément pour $X = G$.

Proposition 3.4 *Soit $H \subset G$ un sous-groupe. La relation définie par $x \backsim y$ ssi $x^{-1}y \in H$ est une relation d'équivalence sur G. La classe d'équivalence de x est l'ensemble $xH = \gamma_x(H)$. Les classes d'équivalence sont toutes en bijection.*

Démonstration : La démonstration est un exercice facile. Notons simplement qu'en ce qui concerne la dernière affirmation, la bijection γ_x met en bijection la classe H avec la classe $xH = \gamma_x(H)$. Donc toutes les classes sont en bijection. □

Définitions 3.5 La classe d'équivalence de x est appelée *classe à gauche de x modulo H*. L'ensemble des classes à gauche modulo H est noté G/H et la surjection $\pi : G \to G/H$ qui à x associe sa classe xH est appelée *surjection canonique*. Un *système de représentants des classes à gauche* est une partie $S \subset G$ contenant un élément de chaque classe.

La *partition de G en classes à gauche* $G = \bigsqcup_{x \in S} xH$ est indépendante du choix de S.

Remarque 3.6 On a les mêmes notions à droite : la relation définie par $x \backsim y$ ssi $yx^{-1} \in H$ est une relation d'équivalence sur G, la *classe à droite de x modulo H* est l'ensemble $Hx = \delta_x(H)$, l'ensemble des classes à droite modulo H est noté $H\backslash G$, etc.

4 Sous-groupes distingués et quotients

On a vu que les noyaux de morphismes $f : G \to G'$ et les images de morphismes $f' : G' \to G$ fournissent des exemples de sous-groupes de G. On peut se demander si on obtient ainsi tous les sous-groupes de G. En fait, il se trouve que tout sous-groupe $H \subset G$ est l'image d'un morphisme $f' : G' \to G$. Il suffit pour cela de considérer le groupe $G' = H$ et le morphisme $f' : H \to G$ donné par $f(h) = h$ (ce n'est rien d'autre que l'inclusion de H dans G). Le fait que H soit un sous-groupe montre que f est en effet un morphisme, et il est clair que son image est H !

On pourrait s'attendre à ce que, de manière analogue, « tout sous-groupe $H \subset G$ est le noyau d'un morphisme $f : G \to G'$ », mais ceci n'est pas vrai en général. La raison est que les noyaux de morphismes vérifient une certaine propriété qui en fait des sous-groupes très particuliers.

Définition 4.1 Un sous-groupe H d'un groupe G est dit *distingué*, ou *normal*, si pour tout $h \in H$ et tout $g \in G$, on a $ghg^{-1} \in H$. Lorsqu'un sous-groupe H de G est distingué, on note $H \lhd G$.

Il est donc équivalent de dire qu'un sous-groupe H est distingué, ou qu'il est invariant par tout automorphisme intérieur : $\forall g \in G$, $c_g(H) \subset H$.

Proposition 4.2 *Soit $f : G \to G'$ un morphisme de groupes. Alors, le noyau $\ker(f)$ est un sous-groupe distingué.*

Démonstration : Soit $h \in \ker(f)$ et $g \in G$, on doit montrer que $ghg^{-1} \in \ker(f)$. C'est clair, puisque $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e$. □

Exemples 4.3 Le lecteur est invité à détailler les exemples suivants (par exemple dans le cas $n = 2$ pour les exemples matriciels) : le sous-groupe de $\mathrm{GL}_n(K)$ formé des homothéties est distingué ; le sous-groupe formé des matrices triangulaires supérieures n'est pas distingué ; tous les sous-groupes de $\mathbb{Z}$ sont distingués.

Les noyaux des morphismes $f : G \to G'$ sont des sous-groupes distingués. Réciproquement, tout sous-groupe distingué de G est-il noyau d'un morphisme $f : G \to G'$? La réponse est oui, et la manière de le voir est l'une des constructions les plus importantes de ces notes sur la théorie des groupes. Nous énonçons le théorème correspondant après une petite observation faite sous la forme d'un lemme.

Lemme 4.4 *Soit G un groupe et $H \lhd G$un sous-groupe distingué. Alors les classes à gauche et à droite modulo H coïncident : $xH = Hx$ pour tout $x \in G$, donc $G/H = H\backslash G$. Réciproquement, si classes à gauche et classes à droite coïncident, le sous-groupe H est distingué.*

Démonstration : En effet, pour tout $h \in H$, comme $xhx^{-1} \in H$ alors $xh = xhx^{-1}x \in Hx$. Ceci montre que $xH \subset Hx$, et on montre de la même manière que $Hx \subset xH$. Il est également facile de montrer la réciproque. □

Théorème 4.5 *Considérons un groupe G et un sous-groupe distingué $H \lhd G$.*

1) Il existe une unique structure de groupe sur l'ensemble quotient $G/H = H\backslash G$ telle que l'application canonique $\pi : G \to G/H$ soit un morphisme de groupes.

2) Pour tout morphisme $f : G \to G'$ tel que $H \subset \ker(f)$, il existe un unique morphisme $\widetilde{f} : G/H \to G'$ tel que $f = \widetilde{f} \circ \pi$. Le noyau de $\widetilde{f}$ est l'image de $\ker(f)$ dans G/H, qui s'identifie á $\ker(f)/H$. En particulier $\widetilde{f}$ est injectif ssi $H = \ker(f)$.

Démonstration : 1) Il nous faut définir une multiplication sur G/H. Comme l'application canonique π est surjective, deux éléments quelconques x, x' de G/H peuvent s'écrire $x = \pi(g)$ et $x' = \pi(g')$. Si l'on veut que π soit un morphisme de groupes, on doit avoir $xx' = \pi(g)\pi(g') = \pi(gg')$ ce qui montre qu'on n'a pas le choix pour définir le produit. Le point qui n'est pas évident est que ce produit est indépendant des choix de g et g' comme antécédents de x et x'. Or, si l'on choisit d'autres d'antécédents u, u', il existe des éléments h, h' de H tels que $u = gh$ et $u' = g'h'$. Comme $g'^{-1}hg' \in H$, on a $g'^{-1}hg'h' \in H$ et donc $\pi(uu') = \pi(ghg'h') = \pi(gg'g'^{-1}hg'h') = \pi(gg')$. Ceci montre que le produit xx' défini en choisissant des antécédents pour x et x' est indépendant de ces choix. Il est alors clair, par construction, que π est un morphisme de groupes.

2) Soit $f : G \to G'$ un morphisme tel que $H \subset \ker(f)$. Utilisant cette hypothèse, on voit que pour $x = \pi(g) \in G/H$, l'élément de G' égal à $f(g)$ ne dépend pas du choix de l'antécédent g choisi pour x. On peut donc poser $\widetilde{f}(x) := f(g)$. Ceci définit une application $\widetilde{f} : G/H \to G'$. Pour voir que c'est un morphisme de groupes, soient $x = \pi(g)$ et $x' = \pi(g')$ dans G/H, alors gg' est un antécédent de xx' dans G et donc $\widetilde{f}(xx') = f(gg') = f(g)f(g') = \widetilde{f}(x)\widetilde{f}(x')$. Ceci montre que $\widetilde{f}$ est un morphisme de groupes. Intéressons-nous à son noyau : soit $x = \pi(g) \in \ker(\widetilde{f})$. Ceci veut dire que $\widetilde{f}(x) = f(g) = e'$ donc $g \in \ker(f)$ et x appartient à l'image de $\ker(f)$ dans G/H. Le fait que, réciproquement, l'image de $\ker(f)$ dans G/H soit incluse dans le noyau de $\widetilde{f}$ est évident. □

Exemples 4.6 - Soit $n \geq 1$ entier. Le quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$ des multiples de n est le groupe bien connu $\mathbb{Z}/n\mathbb{Z}$.

- Soit $\mathbb{U}$ le groupe multiplicatif des nombres complexes de module 1. L'application $e : \mathbb{R} \to \mathbb{U}$ qui associe à x le complexe e^{ix} est un morphisme surjectif de groupes commutatifs, de noyau égal au sous-groupe $2\pi\mathbb{Z}$ engendré par 2π dans $\mathbb{R}$. Elle se factorise en un morphisme $\widetilde{e} : \mathbb{R}/2\pi\mathbb{Z} \to \mathbb{U}$ qui est injectif, donc est un isomorphisme. L'isomorphisme inverse est l'application *argument*, qui à un nombre complexe z de module 1 associe la classe modulo 2π d'un réel θ tel que $z = e^{i\theta}$.

5 Groupes abéliens

Définitions 5.1 On dit qu'un groupe G est *commutatif*, ou *abélien*, si sa multiplication vérifie la propriété suivante : $\forall (g_1, g_2) \in G^2$, $g_1 g_2 = g_2 g_1$.

Exemples 5.2 Le groupe $\mathbb{Z}$ est abélien. Le sous-groupe d'un groupe G engendré par un élément g est abélien. Le groupe $\mathrm{GL}_n(K)$ n'est pas abélien si $n \geq 2$.

Définition 5.3 Dans un groupe G, on dit que deux éléments g_1, g_2 *commutent* si et seulement si $g_1 g_2 = g_2 g_1$. Le *centre* de G est l'ensemble des $g \in G$ qui commutent avec tous les éléments de G. On le note $Z(G)$.

Proposition 5.4 *Soit G un groupe. Son centre $Z(G)$ est un groupe abélien ; c'est un sous-groupe distingué de G. De plus, G est abélien ssi $Z(G) = G$.*

Démonstration : La vérification est facile et laissée comme un bon exercice d'entraînement pour la lectrice. Le fait que $Z(G)$ est distingué peut se justifier en disant que c'est le noyau du morphisme de conjugaison $c : G \to \mathrm{Aut}(G)$, voir proposition 2.8. □

Remarque 5.5 Le lecteur pourra montrer en exercice qu'un groupe G est abélien si et seulement si l'application d'inversion $i : G \to G$ telle que $i(g) = g^{-1}$ est un morphisme de groupes.

Remarque 5.6 Nous terminons ces remarques sur les groupes abéliens par une question de notation. Comme nous l'avons déjà dit, en théorie des groupes, on utilise généralement la notation multiplicative pour la loi interne d'un groupe. Cependant, il est d'usage de réserver un traitement à part aux groupes abéliens dont la loi est notée additivement, c'est-à-dire avec le signe '+'. En accord avec ce choix, l'inverse est alors appelé l'*opposé* et le neutre est noté 0.

6 Groupes monogènes

Définition 6.1 Un groupe G est dit *monogène* s'il peut être engendré par un seul élément. Si de plus G est fini, on préfère souvent le qualificatif *cyclique*.

Lemme 6.2 *Soit H un sous-groupe de $\mathbb{Z}$. Alors, il existe un entier $n \geq 0$ tel que $H = n\mathbb{Z}$.*

Démonstration : Si $H = \{0\}$, on a le résultat annoncé avec $n = 0$. Sinon, H possède des éléments strictement positifs et on peut considérer le plus petit de ces éléments, noté n. Montrons que $H = n\mathbb{Z}$. Pour cela, soit $a \in H$. Si $a > 0$ on peut faire sa division euclidienne par n qui s'écrit $a = qn + r$ avec $0 \leq r < n$. Ainsi $r = a - qn$ est dans H et strictement inférieur à n. Le choix de n impose que l'on ait $r = 0$, de sorte que $a = qn \in n\mathbb{Z}$ comme on le voulait. Si $a < 0$, on peut faire exactement le même raisonnement avec $-a$ à la place de a, et l'on obtient encore $a \in n\mathbb{Z}$. Finalement $H = n\mathbb{Z}$. □

Proposition 6.3 *Soit G un groupe monogène. Alors G est isomorphe à $\mathbb{Z}$ s'il est infini, et à $\mathbb{Z}/n\mathbb{Z}$ s'il est fini.*

Démonstration : Par hypothèse, il existe un élément $x \in G$ qui l'engendre. Considérons l'application $f : \mathbb{Z} \to G$ qui envoie l'entier k sur x^k. Il est clair que c'est un morphisme de groupes, qui est de plus surjectif puisque x engendre G, voir l'exemple 1.9. Si f est injectif, c'est un isomorphisme entre $\mathbb{Z}$ et G. Si f n'est pas injectif, d'après le lemme 6.2 il existe $n > 0$ tel que $\ker(f) = n\mathbb{Z}$. Alors f induit un isomorphisme $\widetilde{f} : \mathbb{Z}/n\mathbb{Z} \to G$. En remettant ces remarques dans l'ordre, on obtient l'énoncé proposé. □

7 Groupes finis

Définitions 7.1 On dit qu'un groupe G est *fini* si son ensemble sous-jacent est fini. L'*ordre* ou *cardinal* d'un groupe G est le nombre de ses éléments s'il est fini, et est égal à l'infini sinon. On le note $|G|$, $\mathrm{card}(G)$ ou $\mathrm{ord}(G)$. L'*ordre* d'un élément g est l'ordre du sous-groupe de G qu'il engendre, on le note $\mathrm{ord}(g)$.

Dire que g est d'ordre fini $n > 0$ revient à dire que $g^n = e$ et que n est le plus petit entier > 0 avec cette propriété.

Remarque 7.2 Il existe des groupes infinis dans lesquels tout élément est d'ordre fini. Par exemple, l'ensemble des suites $u = \{u_i\}_{i\in\mathbb{N}}$ à valeurs dans $\mathbb{Z}/n\mathbb{Z}$ est un groupe G pour l'addition, le neutre étant la suite nulle. Il est clair que pour toute suite u, on a $nu = \{nu_i\}_{i\in\mathbb{N}} = 0$ alors que G est infini.

Exemple 7.3 Le groupe des bijections de l'ensemble $\{1, \ldots, n\}$ est en général noté $\mathfrak{S}_n$ ou S_n, plutôt que $S_{\{1,\ldots,n\}}$. Il est appelé *groupe symétrique*. C'est un groupe fini d'ordre $n!$, car une bijection $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ est entièrement déterminée par le uplet d'images $(f(1), \ldots, f(n))$, or on a n choix pour $f(1)$, puis $n - 1$ choix pour $f(2)$, etc.

Théorème 7.4 (Cayley) *Tout groupe fini G d'ordre n se plonge dans le groupe symétrique $\mathfrak{S}_n$.*

Démonstration : On a vu dans la proposition 3.2 que les translations à gauche donnent un morphisme injectif $\gamma : G \hookrightarrow S_G$. Or comme G est d'ordre n, il existe une bijection $f : G \to \{1, \ldots, n\}$ et il est clair que celle-ci induit une bijection

$$\begin{array}{rcl} S_G & \to & \mathfrak{S}_n \\ u & \mapsto & fuf^{-1} \ . \end{array}$$

En composant, on obtient l'injection $G \hookrightarrow S_G \simeq \mathfrak{S}_n$. □

Définition 7.5 Soit G un groupe et H un sous-groupe. On appelle *indice* de H dans G le cardinal (éventuellement infini) de l'ensemble quotient G/H. On le note $(G : H)$ ou $[G : H]$.

Théorème 7.6 (Lagrange) *Soit G un groupe fini et H un sous-groupe. Alors, on a :*

$$|G| = (G : H)\,|H| \ .$$

En particulier, le cardinal d'un sous-groupe divise le cardinal du groupe. Plus généralement, si on a des sous-groupes $K \subset H \subset G$ alors $(G : K) = (G : H)(H : K)$.

Démonstration : Nous avons vu dans la section 3 qu'à tout sous-groupe H est associé une partition de G en classes à gauche xH qui sont toutes en bijection, donc possèdent toutes le même cardinal égal à $|H|$. Le nombre de classes est égal à $(G : H)$ par définition de l'indice. Il s'ensuit que le cardinal de G est égal au produit du nombre de classes par le cardinal d'une classe, ce qui donne : $|G| = (G : H)\,|H|$. Dans la situation de sous-groupes $K \subset H \subset G$, on a

$$|G| = (G : H)\,|H| \quad , \quad |G| = (G : K)\,|K| \quad \text{et} \quad |H| = (H : K)\,|K|$$

donc $(G : K) = \frac{|G|}{|K|} = \frac{|G|}{|H|}\,\frac{|H|}{|K|} = (G : H)(H : K)$. □

Corollaire 7.7 *Dans un groupe G fini d'ordre n on a, pour tout $x \in G$, $x^n = 1$.*

Démonstration : Notons $H = \langle x \rangle$ le sous-groupe engendré par x et m son ordre, donc $x^m = 1$. Par le théorème de Lagrange, on a $n = md$ où $d = (G : H)$, donc $x^n = (x^m)^d = 1$. □

8 Actions de groupes

Comme nous l'avons dit dans l'introduction de ces notes, la raison de l'apparition de la notion théorique de *groupe* est l'observation que de nombreuses structures mathématiques (ensembles, espaces vectoriels, objets géométriques divers) possèdent des transformations naturelles et que dont la bonne connaissance est précieuse. Ainsi, presque par définition, *les groupes sont des êtres qui agissent (comme nous dirons) sur des ensembles, des formes, des espaces, etc.* Pour cette raison, il est souvent utile, même pour leur étude abstraite, de faire intervenir des ensembles sur lesquels ils agissent. Par exemple, le vocabulaire des actions de groupes sera nécessaire pour étudier les groupes symétriques, dans la section 9.

Nous voici à pied d'œuvre pour introduire quelques notions.

Définition 8.1 Soit G un groupe et X un ensemble. Une *action* de G sur X est un morphisme de groupes $\rho : G \to S_X$ du groupe G vers le groupe des bijections de X. C'est la même chose de se donner, pour tout élément $g \in G$, une bijection $\rho_g : X \to X$, de telle façon que

(i) $\rho_1 = \mathrm{id_X}$.

(ii) $\rho_{gg'} = \rho_g \circ \rho_{g'}$ pour tous g, g' dans G.

Par souci de concision, en général on note g au lieu de ρ_g, et gx ou $g.x$ au lieu de $\rho_g(x)$.

Pour exploiter l'intuition de la géométrie, on appelle souvent les éléments de X des *points*.

Exemples 8.2 Les translations à gauche dans G donnent lieu à un morphisme injectif $G \hookrightarrow S_G$ qui est une action de G sur lui-même (c'est-à-dire qu'ici $X = G$).

Le groupe $G = \mathrm{GL}_k(E)$ des automorphismes linéaires d'un k-espace vectoriel E agit sur E ; sur l'ensemble des droites d de E par $\rho_g(d) = g(d)$; sur l'ensemble des endomorphismes linéaires f de E par $\rho_g(f) = g \circ f$; etc.

Le groupe des isométries d'un espace vectoriel euclidien agit sur l'espace lui-même, ou sur l'ensemble de ses triangles, ou sur l'ensemble de ses droites, ou sur l'ensemble des cercles...

Définition 8.3 Soit G un groupe agissant sur X. Une partie $Y \subset X$ est dite *stable*, ou *invariante*, sous G, si pour tout $g \in G$ on a $g(Y) \subset Y$.

Remarque 8.4 Partant d'une action de G sur X, on peut souvent en fabriquer de nouvelles en considérant des groupes reliés à G ou des ensembles reliés à X. Par exemple :
1) pour tout sous-groupe $H \subset G$ il y a une *action restreinte* de H sur X obtenue par la composition $H \subset G \to S_X$.
2) si une partie $Y \subset X$ est stable sous G, il y a une action induite de G sur Y. On prendra garde néanmoins qu'en général, l'ensemble des $g \in G$ tels que $g(Y) \subset Y$ n'est pas un sous-groupe, le problème éventuel venant du défaut de surjectivité de $g : Y \to Y$. Nous verrons des exemples de ceci dans les exercices.

Définition 8.5 Soit G un groupe agissant sur un ensemble X. L'*orbite d'un point $x \in X$ sous le groupe G*, ou *G-orbite de x*, est la partie de X définie par $\mathcal{O}_G(x) = \{gx\,, g \in G\}$.

Si Y est une partie de X, le *stabilisateur* de Y dans G est le sous-groupe de G composé des $g \in G$ tels que $g(Y) = Y$. En particulier, le stabilisateur d'un point $x \in X$ est le sous-groupe de G défini par $G_x = \{g \in G\,, gx = x\}$. (La vérification du fait qu'il s'agit d'un sous-groupe est un exercice facile.)

Remarque 8.6 Il y a aussi une notion de *fixateur* de Y : c'est le sous-groupe composé des $g \in G$ tels que pour tout $y \in Y$, on a $g(y) = y$. C'est donc aussi l'intersection des stabilisateurs G_y des points $y \in Y$. (Lorsque Y est un point, les notions de stabilisateur et de fixateur coïncident !)

Pour $x \in X$, nous introduisons maintenant l'application $ev_x : G \to X$ qui envoie $g \in G$ sur $g(x)$. Nous l'appellerons l'*application d'évaluation en x*.

Théorème 8.7 *L'application d'évaluation en x induit une bijection $G/G_x \to \mathcal{O}_G(x)$.*

Démonstration : Par définition de l'orbite, l'image de ev_x est l'orbite $\mathcal{O}_G(x)$ donc ev_x est une application surjective $G \to \mathcal{O}_G(x)$. Pour cette application, deux éléments g, h ont la même image ssi $g^{-1}h \in G_x$. Il s'ensuit, d'après la définition de l'ensemble quotient G/G_x, ensemble des classes à gauche de G modulo G_x, que ev_x induit une application bijective $\widetilde{ev}_x : G/G_x \to \mathcal{O}_G(x)$. □

Corollaire 8.8 *Si un groupe fini G agit sur un ensemble X, les orbites de X sous G sont finies et le cardinal de l'orbite de x est égal à l'indice de son stabilisateur.*

Démonstration : Le théorème précédent nous dit que $|\mathcal{O}_G(x)| = (G : G_x)$. □

Proposition 8.9 *La relation binaire sur X définie par $x \sim y$ ssi il existe $g \in G$ tel que $y = gx$ est une relation d'équivalence. On a évidemment :*

$$x \sim y \iff y \in \mathcal{O}_G(x) \iff \mathcal{O}_G(x) = \mathcal{O}_G(y) \ .$$

Les classes d'équivalence pour cette relation sont les orbites de l'action de G sur X.

Démonstration : C'est un exercice facile. □

La partition en classes pour la relation d'équivalence introduite dans la proposition ci-dessus est appelée la *partition en orbites* de X.

Exemple 8.10 Les classes à gauche modulo un sous-groupe $H \subset G$ peuvent être vues comme les orbites d'une action de H sur G. En effet, considérons l'action donnée par les translations à droite : $\rho : H \to S_G$ telle que $\rho_h(g) = gh^{-1}$. Alors, l'orbite de g est la classe gH.

Il faut cependant prendre garde au fait que pour une action générale, les classes de la partition en orbites n'ont pas toutes le même nombre d'éléments.

Les dernières notions importantes que nous mentionnons sont reliées à la taille des orbites : nous introduisons des qualificatifs utiles lorsqu'il existe des orbites très grosses ou très petites.

Définition 8.11 On dit que l'action d'un groupe G sur un ensemble X est *transitive* s'il n'y a qu'une orbite.

Ceci signifie que pour tous x, y dans X il existe $g \in G$ tel que $y = gx$, ou encore, que l'application d'évaluation $ev_x : G \to X$ est surjective. Par exemple, partant d'une action quelconque de G sur un ensemble X, et d'un point $x \in X$, il y a une action de G sur l'orbite $Y := O_G(x)$ et cette action est transitive, par définition de l'orbite.

Définition 8.12 Soit G un groupe agissant sur un ensemble X, et $x \in X$ un point. Si $\mathcal{O}_G(x) = \{x\}$, on dit que l'orbite de x est *ponctuelle*, ou *réduite à un point*, ou parfois *triviale*. On dit aussi que x est un *point fixe* sous G.

Par exemple, x est toujours un point fixe sous son stabilisateur G_x, c'est-à-dire $O_{G_x}(x) = \{x\}$. Ceci provient juste de la définition du stabilisateur.

9 Groupes symétriques et alternés

9.1 Groupes symétriques

Définition 9.1 Soit E un ensemble. On appelle *groupe symétrique de E* le groupe des bijections de E. On le note $S(E)$ ou $\mathfrak{S}(E)$. Si $E = \{1, \ldots, n\}$, on le note simplement S_n ou $\mathfrak{S}_n$. Les éléments du groupe symétrique $\mathfrak{S}_n$ sont traditionnellement appelés des *permutations*.

Exemple 9.2 On a $\mathfrak{S}_1 = \{1\}$, $\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathfrak{S}_3$ est isomorphe au groupe diédral $\mathbb{D}_3$, groupe des isométries du triangle équilatéral. Pour $n \geq 4$, il n'y a pas en général d'identification de $\mathfrak{S}_n$ avec un groupe plus simple connu (cyclique, diédral,...). Pour $n \geq 3$, le groupe $\mathfrak{S}_n$ n'est pas abélien.

Remarque 9.3 Une façon de représenter une permutation σ est d'indiquer sur une ligne tous les entiers de 1 à n, et sur une ligne située en-dessous, les images de ces entiers par σ. Par exemple, la permutation $\sigma \in \mathfrak{S}_3$ qui envoie 1 sur 1, 2 sur 3 et 3 sur 2 sera représentée ainsi :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} .$$

Mais nous verrons plus loin une représentation plus commode, qui aura entre autres avantages celui de permettre de calculer facilement des compositions de permutations.

Le groupe symétrique agit naturellement (par sa définition même) sur l'ensemble des n premiers entiers $\{1, \ldots, n\}$. Lorsqu'on l'étudie, cette action est toujours en toile de fond et on utilise naturellement le vocabulaire des actions de groupes. Par exemple, chaque permutation σ a des orbites (les σ-orbites), qui sont les orbites de $\{1, \ldots, n\}$ sous $G = \langle \sigma \rangle$.

Définition 9.4 Une permutation σ qui possède une et une seule orbite non ponctuelle dans son action sur $\{1, \ldots, n\}$ est appelée un *cycle*. Si r est le cardinal de l'orbite non ponctuelle, on dit aussi que σ est un *r-cycle*. Un 2-cycle est aussi appelé une *transposition*.

Définition 9.5 Soit $\sigma \in \mathfrak{S}_n$ une permutation et $i \in \{1, \ldots, n\}$.

On dit que $i \in \{1, \ldots, n\}$ est un *point fixe* pour σ si et seulement si $\sigma(i) = i$. On note $\mathrm{Fix}(\sigma)$ l'ensemble des points fixes de σ dans $\{1, \ldots, n\}$.

On appelle *support* de σ et on note $\mathrm{Supp}(\sigma)$ le complémentaire de l'ensemble des points fixes de σ, c'est-à-dire l'ensemble des $i \in \{1, \ldots, n\}$ tels que $\sigma(i) \neq i$.

Remarques 9.6 - Un cycle est donc une permutation dont le support est non vide et est une orbite. Notez que, d'après la définition, l'identité n'est pas un cycle.

- L'ensemble des permutations qui fixent le point i est le stabilisateur de i pour l'action de $\mathfrak{S}_n$ sur $\{1, \ldots, n\}$. C'est donc un sous-groupe ; il est facile de voir qu'il s'identifie au sous-groupe des permutations de $\{1, \ldots, i-1, i+1, \ldots, n\}$ qui est un groupe isomorphe à $\mathfrak{S}_{n-1}$.

Proposition 9.7 *Deux permutations σ et τ à supports disjoints commutent : $\sigma\tau = \tau\sigma$.*

Démonstration : Il s'agit de démontrer que pour tout $i \in \{1, \ldots, n\}$ on a $(\sigma\tau)(i) = (\tau\sigma)(i)$. Si i n'est ni dans le support de σ ni dans celui de τ, on a $\sigma(i) = \tau(i) = i$ donc $(\sigma\tau)(i) = (\tau\sigma)(i) = i$ et on a fini. Il reste à traiter les cas où $i \in \mathrm{Supp}(\sigma)$ et $i \in \mathrm{Supp}(\tau)$. Clairement le raisonnement sera le même dans les deux cas, en changeant σ en τ, donc il suffit de regarder le premier cas : $i \in \mathrm{Supp}(\sigma)$. Nous faisons l'observation que comme $\mathrm{Fix}(\sigma)$ est stable sous σ, son complémentaire $\mathrm{Supp}(\sigma)$ l'est aussi. Ainsi i et $\sigma(i)$ sont dans le support de σ. Comme σ et τ sont à supports disjoints, i et $\sigma(i)$ ne sont pas dans le support de τ, en d'autres termes $\tau(i) = i$ et $\tau(\sigma(i)) = \sigma(i)$. Donc $\tau(\sigma(i)) = \sigma(i) = \sigma(\tau(i))$ et on a fini. □

Théorème 9.8 (Décomposition en cycles à supports disjoints) *Toute permutation s'écrit de manière unique, à l'ordre près des facteurs, comme un produit de cycles à supports disjoints.*

Démonstration : Existence : soient $\mathcal{O}_1, \ldots, \mathcal{O}_s$ les orbites non ponctuelles de σ. Pour chaque i tel que $1 \leq i \leq s$, on note $\tau_i : \{1, \ldots, n\} \to \{1, \ldots, n\}$ l'application définie par

$$\tau_i(x) = \begin{cases} \sigma(x) & \text{si } x \in \mathcal{O}_i \ , \\ x & \text{si } x \notin \mathcal{O}_i \ . \end{cases} \qquad (\star)$$

Il est clair que c'est une permutation et que $\mathcal{O}_i$ est une orbite de τ_i. En d'autres termes, τ_i est un cycle. Par ailleurs, les supports des τ_i sont les orbites $\mathcal{O}_i$ donc sont disjoints. On a ainsi démontré l'existence de la décomposition annoncée.

Unicité : supposons que $\sigma = \tau_1 \ldots \tau_s$ est un produit de cycles à supports disjoints et notons $\mathcal{O}_i = \mathrm{Supp}(\tau_i)$. Puisque les τ_i commutent entre eux d'après la proposition 9.7 et puisque $\tau_j(x) = x$ si $x \in \mathcal{O}_i$, $i \neq j$, on obtient :

- si $x \in \mathcal{O}_i$: $\tau_i(x) = \tau_i(\tau_i\tau_1 \ldots \tau_{i-1}\tau_{i+1} \ldots \tau_s(x)) = (\tau_1 \ldots \tau_s)(x) = \sigma(x)$,
- si $x \notin \mathcal{O}_i$: $\tau_i(x) = x$.

Donc τ_i est la permutation décrite en $(\star)$ ci-dessus, ce qui montre l'unicité. □

Exemple 9.9 La permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} .$$

a pour seule orbite non ponctuelle l'ensemble $\{2, 3\}$. Le seul cycle qui entre dans sa décomposition en cycles à supports disjoints est la transposition qui échange 2 et 3.

Notation 9.10 Ceci mène à une nouvelle manière d'écrire les permutations. Un cycle est noté en indiquant entre des parenthèses les images successives d'un point de son orbite non ponctuelle, par exemple la notation $\tau = (134)$ désigne le 3-cycle tel que $\tau(1) = 3$, $\tau(3) = 4$ et $\tau(4) = 1$. On note que dans cette notation, *les points fixes par la permutation* (ici un cycle) *n'apparaissent pas*. Ceci n'est évidemment pas gênant, puisqu'on sait quelle doit être leur image par τ : eux-mêmes ! Une permutation est notée en juxtaposant les écritures des différents cycles de sa décomposition en cycles à supports disjoints, par exemple la notation $\sigma = (134)(25)$ désigne le produit du 3-cycle $\tau = (134)$ par la transposition $\tau' = (25)$. Nous verrons lors des exercices comment cette notation permet, par exemple, de calculer très rapidement la composée de deux permutations.

Théorème 9.11 *Pour tout $n \geq 2$, le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions. Plus précisément, toute permutation peut s'écrire comme un produit d'au plus n transpositions.*

Démonstration : Faisons une démontronstration par récurrence sur n. Si $n = 2$, le groupe $\mathfrak{S}_2$ est composé de 1 et d'une transposition donc il n'y a rien à démontrer. Supposons maintenant que $\mathfrak{S}_n$ est engendré par les transpositions, et montrons que $\mathfrak{S}_{n+1}$ l'est aussi. Il s'agit de montrer que toute permutation σ est un produit de transpositions. Notons H le sous-groupe de $\mathfrak{S}_{n+1}$ constitué des permutations qui fixent $n + 1$ (voir remarque 9.6), c'est un sous-groupe isomorphe à $\mathfrak{S}_n$. Si $\sigma(n + 1) = n + 1$ alors $\sigma \in H$ et l'hypothèse de récurrence nous dit que σ est un produit d'au plus n transpositions de $H \simeq \mathfrak{S}_n$. Si $\sigma(n + 1) = i \neq n + 1$, considérons la transposition $\tau = (i, n + 1)$. Il est clair que $\tau\sigma$ fixe $n + 1$, de sorte que par l'hypothèse de récurrence $\tau\sigma \in H$ est un produit d'au plus n transpositions : $\tau\sigma = \tau_1 \ldots \tau_s$ avec $s \leq n$. Il s'ensuit que $\sigma = \tau\tau_1 \ldots \tau_s$ est produit d'au plus $n + 1$ transpositions. □

9.2 Groupes alternés

Soit $n \geq 2$ et S_n le groupe symétrique. Dans cette sous-section, nous allons démontrer le théorème suivant :

Théorème 9.12 *Il existe un unique morphisme de groupes surjectif* $\epsilon : \mathfrak{S}_n \to \{\pm 1\}$.

Définition 9.13 Le morphisme du théorème 9.12 est appelé la *signature*. Son noyau est appelé le *groupe alterné* et noté A_n ou $\mathfrak{A}_n$. Une permutation de signature $+1$ est dite *paire*, et une permutation de signature -1 est dite *impaire*.

L'existence de la signature et du groupe alterné, sous-groupe distingué d'indice 2 de $\mathfrak{S}_n$, est un phénomène tout à fait remarquable.

Noter que le groupe à 2 éléments, qui est unique à isomorphisme près, peut être représenté par le groupe additif $\mathbb{Z}/2\mathbb{Z}$ (quotient de $\mathbb{Z}$) mais aussi par le groupe multiplicatif $\{\pm 1\}$ (sous-groupe de $\mathbb{Q}^*$).

Dans la démonstration, deux concepts que nous introduisons au préalable vont jouer un rôle important : l'action du groupe symétrique $\mathfrak{S}_n$ sur les polynômes en n indéterminées (exemple 9.14 ci-dessous) et le nombre d'inversions d'une permutation (définition 9.15).

Exemple 9.14 Soit $\mathbb{C}[X_1, \ldots, X_n]$ le $\mathbb{C}$-espace vectoriel des polynômes en les n indéterminées $X_1, \ldots, X_n$. Nous aurons besoin de très peu de choses sur cet espace vectoriel. Pour $n = 3$, des exemples de polynômes dans $\mathbb{C}[X, Y, Z]$ sont : $X^2 + Y$, $XYZ + Z^7 - 1$ ou $(X - Y)(X^2 + Z^2)$.

Le groupe $\mathfrak{S}_n$ agit sur $\mathbb{C}[X_1, \ldots, X_n]$ par permutation des indéterminées de la façon suivante : pour un polynôme $P = P(X_1, \ldots, X_n)$ et une permutation $\sigma \in \mathfrak{S}_n$, on note σP le polynôme

$$(\sigma P)(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \ .$$

La variable X_i se trouve donc à la place d'indice $\sigma^{-1}(i)$. Vérifions qu'il s'agit bien d'une action : il est clair que $1P = P$, et pour deux permutations σ, τ on a $(\tau\sigma)P = \tau(\sigma P)$ puisque

$$\begin{aligned}
(\tau(\sigma P))(X_1, \ldots, X_n) &= (\sigma P)(X_{\tau(1)}, \ldots, X_{\tau(n)}) \\
&= P(\ldots, X_{\tau(i)}, \ldots) \text{ (la variable } X_{\tau(i)} \text{ est à la place d'indice } \sigma^{-1}(i)) \\
&= P(X_{\tau\sigma(1)}, \ldots, X_{\tau\sigma(n)}) \\
&= ((\tau\sigma)P)(X_1, \ldots, X_n) \ .
\end{aligned}$$

Définition 9.15 Soit σ une permutation. Une *inversion* pour σ est un couple d'entiers (i, j) dans $\{1, \ldots, n\}$ tels que $i < j$ et $\sigma(i) > \sigma(j)$.

Une inversion est donc un couple dont l'ordre est renversé par σ. Par exemple, si $\sigma = 1$, il n'y a pas d'inversion, donc $\epsilon(\sigma) = 1$, et si $\sigma = (12)$, la seule inversion est le couple $(1, 2)$. Nous pouvons passer à la démonstration du théorème.

Démonstration : Nous allons d'abord démontrer l'existence. Pour cela, notons n_σ le nombre d'inversions de σ, et posons $\epsilon(\sigma) = (-1)^{n_\sigma}$. On a vu juste au-dessus que la seule inversion pour $\sigma = (1, 2)$ est le couple $(1, 2)$, de sorte que $\epsilon(\sigma) = -1$. Ainsi l'application $\epsilon : \mathfrak{S}_n \to \{\pm 1\}$ est surjective. Pour démontrer qu'on a bien défini un morphisme, on va utiliser l'action de $\mathfrak{S}_n$ sur l'ensemble des polynômes en n indéterminées $X_1, \ldots, X_n$. Considérons le *polynôme de Vandermonde* défini par

$$V(X_1, \ldots, X_n) = \prod_{i<j} (X_j - X_i) \ .$$

Par exemple, pour $n = 3$, on a $V(X_1, X_2, X_3) = (X_3 - X_2)(X_3 - X_1)(X_2 - X_1)$. Nous voulons calculer σV, pour cela on va réordonner les facteurs dans l'expression

$$\sigma V(X_1, \ldots, X_n) = \prod_{i<j} (X_{\sigma(j)} - X_{\sigma(i)}) \ .$$

Si l'on prend un couple (i, j) avec $i < j$, il peut se passer deux choses :

- soit (i, j) est une inversion pour σ, auquel cas on pose $i' = \sigma(j)$, $j' = \sigma(i)$ et on a $i' < j'$.

- soit (i, j) n'est pas une inversion, alors on pose $i' = \sigma(i)$, $j' = \sigma(j)$ et on a $i' < j'$.

Avec ces notations, on a donc $X_{\sigma(j)} - X_{\sigma(i)} = (\pm 1)(X_{j'} - X_{i'})$ avec $i' < j'$, où le signe ± 1 vaut -1 lorsque i, j est une inversion et 1 sinon. En conclusion, lorsqu'on multiplie tous ces facteurs il apparaît un produit de signes -1 dont le nombre est égal au nombre d'inversions de σ, c'est-à-dire que :

$$\sigma V(X_1, \ldots, X_n) = \epsilon(\sigma) \prod_{i'<j'} (X_{j'} - X_{i'}) = \epsilon(\sigma) V(X_1, \ldots, X_n) \ .$$

Pour deux permutations σ, τ on a

$$\epsilon(\sigma\tau)V = \sigma\tau V = \sigma(\tau V) = \sigma(\epsilon(\tau)V) \overset{(*)}{=} \epsilon(\tau)\sigma V = \epsilon(\tau)\epsilon(\sigma)V \ .$$

On a utilisé, à l'endroit où il y a une étoile $(*)$, le fait que l'action de S_n sur $\mathbb{C}[X_1, \ldots, X_n]$ est une action par automorphismes de $\mathbb{C}$-espace vectoriel, donc en particulier $\sigma(\lambda P) = \lambda\sigma(P)$. Il résulte de ce calcul que $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$, donc ϵ est bien un morphisme de groupes.

Démontrons que ce morphisme est unique. Soit $\delta : S_n \to \{\pm 1\}$ un morphisme surjectif de groupes. Pour démontrer que δ est unique, il suffit de démontrer que sa valeur est -1 sur toutes les transpositions, car comme S_n est engendré par les transpositions, toute permutation σ est produit de transpositions : $\sigma = \tau_1 \ldots \tau_k$, et alors $\delta(\sigma) = \delta(\tau_1) \ldots \delta(\tau_k) = (-1)^k$.

Comme deux quelconques permutations τ, τ' sont conjuguées : $\tau' = \gamma\tau\gamma^{-1}$, on a $\delta(\tau') = \delta(\gamma\tau\gamma^{-1}) = \delta(\gamma)\delta(\tau)\delta(\gamma)^{-1} = \delta(\tau)$. La valeur de δ est donc la même sur toutes les transpositions. Si cette valeur est 1, alors $\delta(\tau) = 1$ pour toute transposition τ, donc $\delta(\sigma) = 1$ pour toute permutation σ (encore car S_n est engendré par les transpositions). Or on a supposé que δ est surjectif, donc ceci est impossible et finalement la valeur de δ sur les transpositions est -1.

Ceci termine la preuve du théorème sur la signature. □

Exemple 9.16 La permutation $\sigma = \binom{12345}{35412}$ a une décomposition en cycles à supports disjoints donnée par $\sigma = (134)(25)$. Pour calculer sa signature, on peut écrire $(134) = (14)(13)$ et on obtient $\epsilon(\sigma) = \epsilon(14)\epsilon(13)\epsilon(25) = (-1)^3 = -1$.

Pour finir, indiquons sans preuve diverses façons de calculer la signature :

1 Si n_σ est le nombre d'inversions de σ, on a $\epsilon(\sigma) = (-1)^{n_\sigma}$. En général, ceci est peu pratique pour calculer $\epsilon(\sigma)$.

2 Si σ est produit de k transpositions, on a $\epsilon(\sigma) = (-1)^k$.

3 Si σ est un r-cycle, on a $\epsilon(\sigma) = (-1)^{r-1}$.

4 Si s est le nombre d'orbites de σ (incluant les orbites ponctuelles), on a $\epsilon(\sigma) = (-1)^{n-s}$.