Géométrie dans l'espace et visualisation : Résumé de cours sur les groupes Version préliminaire

29 mars 2013

Remarques :

1. Les définitions qui ne sont pas rappelées sont dans n'importe quel bouquin de niveau L1.
2. La notion d'opération de groupe est introduite plus tardivement que dans un cours classique, pour rester à un niveau élémentaire assez longtemps. En particulier Lagrange est démontré sans actions de groupes.
3. Si vous trouvez une faute, vérifiez auprès des autres puis transmettez par mail.
4. Ceci est une version préliminaire ; j'ajouterai des exercices, mais le cours lui-même ne devrait pas trop changer.

Table des matières

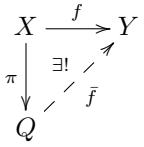
Le cardinal d'un ensemble A sera noté $|A|$, $\sharp A$ ou $Card(A)$.

1 Groupes

1.1 Rappels sur les quotients. Propriété universelle.

Soit X un ensemble muni d'une relation d'équivalence $\sim$; on note $Q = X/\sim$ le quotient et $\pi : X \to Q$ la surjection (ou projection) canonique sur le quotient. Le quotient et la projection vérifient la propriété universelle suivante.

Théorème 1.1.1. Soit $f : X \to Y$ une application constante sur les classes d'équivalence ; alors il existe une unique application $\bar{f} : Q \to Y$ telle que $f = \bar{f} \circ \pi$. Autrement dit on a le diagramme :



L'application $\bar{f}$ est dite induite par f par passage au quotient.

Si $f : X \to Y$ est une application, on peut définir une relation d'équivalence $\simeq$ sur X par $x \sim y \Leftrightarrow f(x) = f(y)$. Toujours en notant $Q = X/\sim$, l'application f induit une application $\bar{f}$ de Q dans Y qui est injective (et donc induisant une bijection de Q sur $Im(f)$).

1.2 Généralités sur les groupes

Définitions 1.2.1.
1. Loi de composition associative sur un ensemble. Élement neutre, unicité. Inverse, unicité de l'inverse.
2. Groupe. Sous-groupe. Notation $H < G$ pour un H un sous-groupe de G. Un groupe (noté multiplicativement) est abélien, ou commutatif, si $xy = yx$, $\forall x, y \in G$. Il existe des groupes non commutatifs, par exemple la plupart des groupes de permutation, voir plus bas.
3. Un groupe fini est un groupe de cardinal fini. Si un groupe est fini, on dit aussi « ordre », à la place de cardinal.
4. Groupe produit.

Proposition 1.2.1. L'intersection de sous-groupes est un sous-groupe.

Exemples 1.2.2.
1. On a une chaîne de sous-groupes $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, et une autre chaîne $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$. L'ensemble $\mathbb{R}$ muni de la multiplication n'est pas un groupe, en effet l'élément 0 n'a pas d'inverse pour la multiplication.
2. Si X est un ensemble, alors l'ensemble $Bij(X)$ des bijections de X sur X, aussi noté $\mathfrak{S}_X$, muni de la composition des bijections, est un groupe. Si $|X| \geq 3$, $\mathfrak{S}_X$ n'est pas abélien. Si X est fini de cardinal n, alors $\mathfrak{S}_X$ est fini de cardinal $n!$.
3. Si A est un ensemble et G un groupe, alors l'ensemble G^A des applications de A dans G est un groupe. La loi est la loi de G sur l'ensemble d'arrivée : par définition $\forall a \in A$, $(f \cdot g)(a) = f(a)g(a)$.
4. Le sous-ensemble $\mathbb{U} \subset \mathbb{C}^*$ des complexes de module 1 est un sous-groupe multiplicatif de $(\mathbb{C}^*, \times)$. Étant donné $n \in \mathbb{N}^*$, l'ensemble des racines n-èmes de l'unité est un sous-groupe fini de cardinal n de $(\mathbb{C}^*, \times)$.
5. Si $n \in \mathbb{Z}$, alors l'ensemble $n\mathbb{Z} = \{nk, , \quad k \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.
6. Soit G un groupe. Le centre de G, noté $Z(G)$, est le sous-ensemble de G formé des éléments $x \in G$ tels que $xg = gx$, $\forall g \in G$. C'est un sous-groupe de G.

7. Exemple de groupe produit : $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$, avec l'addition composante par composante, $\mathbb{Z} \times \mathbb{Z}$ idem, avec élément neutre $(0,0)$. Autre exemple : $\mathbb{C}^* \times \mathbb{Q}$ avec la multiplication sur la première composante et l'addition sur la seconde (l'élément neutre est alors $(1,0)$).

Proposition 1.2.2. Tout sous-groupe de $\mathbb{Z}$ est du type $n\mathbb{Z}$, pour un certain $n \in \mathbb{Z}$ déterminé au signe près.

Preuve : Soit $H < \mathbb{Z}$ un sous-groupe. S'i n'est pas réduit à 0, il intersecte $\mathbb{N}^*$. Soit $n = inf(H \cap \mathbb{N}^*)$. Alors comme H est un sous-groupe, il contient $n\mathbb{Z}$. Réciproquement, soit $a \in H$ positif ; la division euclidienne de a par n donne $a = bn + r$, avec $r < n$. Par définition de n, on a alors $r = 0$, d'où $a \in n\mathbb{Z}$. Raisonnement similaire si a est négatif.

Exemple 1.2.3. . Soit n un entier strictement positif. La relation binaire $\sim$ sur $\mathbb{Z}$ définie par $x \sim y \Leftrightarrow x - y \in n\mathbb{Z}$ est une relation d'équivalence. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient, de cardinal n, et on note $\overline{x}$ la classe d'un élément $x \in \mathbb{Z}$. La formule « $\overline{x} + \overline{y} = \overline{x+y}$ » ne dépend que pas des représentants x et y et définit une loi de composition interne, qui fait de $\mathbb{Z}/n\mathbb{Z}$ un groupe. C'est un groupe fini abélien d'ordre n.

1.3 Morphismes

Morphisme de groupe. L'image et le noyau d'un morphisme sont des sous-groupes. Plus généralement, l'image ou l'image réciproque d'un sous-groupe sont des sous-groupes. Un endomorphisme est un morphisme d'un groupe sur lui-même ; un isomorphisme est un morphisme bijectif ; un automorphisme est un endomorphisme bijectif, autrement dt un isomorphisme d'un groupe sur lui-même. Un morphisme est injectif ssi si noyau est trivial.

Exemple 1.3.1. L'exponentielle réelle est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, \times)$, injectif et non surjectif. L'exponentielle complexe est un morphisme de groupes de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$, surjectif et non injectif. Son noyau est $2i\pi\mathbb{Z}$. Le logarithme réel est un isomorphisme de groupes de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$.

Exemples 1.3.2. (morphismes de $\mathbb{Z}$ dans un groupe)

1. Considérons le groupe $\mathbb{Z}$ muni de la loi $+$. Étant donné un entier n, on définit $\phi : \mathbb{Z} \to \mathbb{Z}$ par $\phi : k \mapsto nk$. Ce morphisme est injectif sauf si n est nul. Il est surjectif ssi $n = \pm 1$. Son image est le sous-groupe $n\mathbb{Z}$.
2. L'application de passage au quotient $p : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad , x \mapsto \bar{x}$ est un morphisme de groupe. Ce morphisme est surjectif, et son noyau est $n\mathbb{Z}$.
3. Soit G un groupe noté multiplicativement, et $g \in G$. On définit l'application $\phi_g : \mathbb{Z} \to G$ par $\phi_g(k) = g^k$, avec la convention $g^0 = 1$, et, si $k < 0$, $g^k := (g^{-1})^{-k}$. Alors ϕ_g est un morphisme de groupe de $\mathbb{Z}$ dans G.
4. Réciproquement, montrons que tout morphisme de $\mathbb{Z}$ dans un groupe G est de ce type. Soit $\phi : \mathbb{Z} \to G$ un morphisme de groupes. Alors le noyau de ϕ est un sous-groupe de $\mathbb{Z}$, donc il existe un unique $n \in \mathbb{N}$, tel que $Ker(\phi) = n\mathbb{Z}$. Comme on a $\phi(k) = \phi(1 + 1 + ... + 1) = \phi(1).\phi(1)...\phi(1) = \phi(1)^k$, on voit que le morphisme ϕ est complètement déterminé par l'élément $\phi(1)$. Notons $g = \phi(1)$. Alors on voit que $\phi = \phi_g$.
5. Cas particulier : soit $\phi : \mathbb{Z} \to G$ un morphisme de groupe non injectif, de noyau $n\mathbb{Z}$. Alors par les rappels sur la propriété universelle du quotient ϕ induit une application (d'ensembles)

$$\bar{\phi} : \quad \mathbb{Z}/n\mathbb{Z} \to Im(\phi), \quad \bar{x} \mapsto \phi(x)$$

qui est bijective. En particulier l'image est de cardinal n. On vérifie facilement que ϕ est en fait un isomorphisme de groupes entre $\mathbb{Z}/n\mathbb{Z}$ et le groupe $Im(\phi)$.

Exemple 1.3.3. (conjugaison) Soit G un groupe, et $g \in G$. On définit l'application $\psi : G \to G$ par $\psi(x) = gxg^{-1}$. C'est l'application de conjugaison par g (penser aux matrices). Alors, ψ est un automorphisme de G, en général non trivial, si le groupe n'est pas abélien. Un automorphisme de ce type est dit intérieur. Il existe en général des automorphismes non intérieurs. Deux éléments du groupe x et y sont dits conjugués s'il existe $z \in G$ tel que $x = zyz^{-1}$. La classe de conjugaison d'un élément $x \in G$ est l'ensemble des éléments qui lui sont conjugués. La relation de conjugaisons est une relation d'équivalence, donc G est union disjointe de classes de conjugaison.

1.4 Parties génératrices

L'intersection de sous-groupes est un sous-groupe. Si A est une partie d'un groupe G, on note $\langle A \rangle$ l'intersection de tous les sous-groupes contenant A. C'est le plus petit sous-groupe contenant A. On l'appelle le sous-groupe engendré par A.

Soi $a \in G$. Considérons le morphisme de groupes $\phi_a : k \mapsto a^k$. Son image est $\{a^k, k \in \mathbb{Z}\}$. Cette image est exactement le sous-groupe $\langle a \rangle$.

Preuve : un sous-groupe contenant a contient tous les $a^k, k \in \mathbb{Z}$, c'est-à-dire contient l'image de ϕ_a. Cette image est un sous-groupe de G. On en déduit le résultat par minimalité de $\langle a \rangle$.

Soit A une partie de G. Si $\langle A \rangle = G$, on dit que A est une partie génératrice de G. Si de plus A contient un unique élément, le groupe est donc engendré par un seul élément, on dit qu'il est monogène. Si de plus il est fini, on dit qu'il est cyclique.

Exemples 1.4.1. $\mathbb{Z}$ est monogène, il est engendré par 1, ou par -1. Le groupe U_n des racines n-èmes de l'unité est monogène, engendré par exemple par $e^{i\frac{2\pi}{n}}$ (exercice : trouver les autres générateurs). Les groupes $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ne sont pas monogènes.

Exemple 1.4.2. . Le groupe $\mathbb{Z}/n\mathbb{Z}$ est monogène (engendré par la classe de 1 par exemple), donc cyclique.

Exercice 1.4.3. . Suivant n, quels sont les autres éléments qui engendrent $\mathbb{Z}/n\mathbb{Z}$? Montrer qu'un groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En particulier, U_n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

1.5 Ordre d'un élément

Soit G un groupe noté multiplicativement, et g un élément de G.

Définition 1.5.1. L'ordre (fini ou infini) d'un élément $g \in G$ est le cardinal (fini ou infini) du sous-groupe $\langle g \rangle$.

De façon équivalente, on considère le morphisme de groupes $\phi_g : \mathbb{Z} \to G, k \mapsto g^k$, dont l'image est $\langle g \rangle$. Si ce morphisme est injectif, on dit que g est d'ordre infini. Si ϕ_g n'est pas injectif, il a un noyau non trivial égal à $n\mathbb{Z}$, avec n strictement positif uniquement déterminé. On dit que g est d'ordre fini, et que son ordre est n. D'après ce qui a été dit sur les sous-groupes de $\mathbb{Z}$, n est le plus petit entier strictement positif tel que $g^n = e$.

Exemples 1.5.2.

1. Le seul élément d'ordre 1 est l'élément neutre.
2. Dans $\mathbb{Z}$, tous les éléments sont d'ordre infini (à part 0).
3. Si G est fini, tout morphisme $\mathbb{Z} \to G$ a un noyau non trivial et donc tout élément $g \in G$ est d'ordre fini.
4. Dans $\mathbb{Z}/6\mathbb{Z}$, l'élément $\bar{0}$ est d'ordre 1, les éléments $\bar{1}$ et $\bar{5}$ sont d'ordre 6, les éléments $\bar{2}$ et $\bar{4}$ sont d'ordre 3, et l'élément $\bar{3}$ est d'ordre 2. Faire l'exercice pour $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$. Généraliser.
5. Dans un groupe infini, les deux cas sont possibles. Par exemple , dans le groupe $\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$, l'élément $(0, 1)$ est d'ordre deux, l'élément $(1, 0)$ est d'ordre infini.

1.6 Classes à gauche, à droite, ensembles quotient

Soit G un groupe fini noté multiplicativement, et H un sous-groupe. Si $g \in G$, on note gH l'ensemble $\{gh \mid h \in H\}$. C'est une partie de G. Exemple de classe à gauche : H (prendre $g = 1$). Si A est une partie de G et qu'il existe un élément $a \in G$ tel que $A = aH$, on dit que A est une classe à gauche, et que a est un représentant de cette classe. Remarque : dans ce cas, a appartient forcément à A. La réciproque est vraie : pour tout élément $b \in A$, on a $A = bH$, autrement dit tout élément de A est un représentant de la classe.

On définit également Hg, l'ensemble $\{hg \mid h \in H\}$. C'est une classe à droite. On rappelle que le groupe n'est pas forcément commutatif, donc en général $gh \neq hg$, et $Hg \neq gH$. Si g et g', les classes à gauche gH et $g'H$ peuvent être égales même si g et g' sont distincts, par exemple s'ils sont tous les deux dans H, auquel cas $gH = g'H = H$.

En fait, deux classes à gauche (ou deux classes à droite) sont soit disjointes, soit égales. Voici pourquoi. La relation binaire $x\mathcal{R}_1 y \Leftrightarrow x^{-1}y \in H$ est une relation d'équivalence. Ses classes d'équivalence sont les classes à gauche. On a $x\mathcal{R}_1 y \Leftrightarrow y \in xH$. Ceci montre que G est réunion disjointe des classes à gauche. On note G/H l'ensemble des classes à gauche. C'est un ensemble, pas un groupe, a priori.

On peut également définir la relation d'équivalence $x\mathcal{R}_2 y \Leftrightarrow xy^{-1} \in H$. Ses classes d'équivalence sont les classes à droite. On note $H \setminus G$ l'ensemble des classes à droite.

Soit $\phi : G \to G,\ g \mapsto g^{-1}$. Alors, l'image d'une classe à gauche est une classe à droite, et vice versa. Ceci définit une application $\bar{\phi} : G/H \to H \setminus G$. Cette application est bijective. En particulier, il y a autant de classes à gauche que de classe à droite. Le nombre est l'indice de H dans G, il peut être fini ou infini.

1.7 Théorème de Lagrange

Théorème 1.7.1. Soit G un groupe fini, et H un sous-groupe. Alors le cardinal de H divise celui de G, plus précisemment, on a $|G| = |H| \times |G/H|$.

Preuve. L'ensemble G est union disjointe des classes à gauche. Il suffit de prouver qu'elles ont toutes les même cardinal, c'est-à-dire qu'elles ont le même cardinal que H. Soit C une classe et $x \in C$. Donc $C = xH$. Soit $\psi : G \to G,\ g \to x^{-1}g$. Elle est bijective, et l'image de C est exactement H. Donc C et H ont même cardinal. □

Corollaire 1.7.2. Si G est un groupe fini et que $g \in G$, l'ordre de g divise l'ordre (cardinal) de G. En effet, il suffit d'appliquer le théorème de Lagrange au sous-groupe engendré par g. Autre corollaire : un groupe de cardinal p, avec p un nombre premier, est forcément cyclique, donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

si G est un groupe fini et que k est un entier divisant son ordre, il n'existe pas forcément d'élément d'ordre k, ni même de sous-groupe de G cardinal k. Exercice : trouver des contre-exemples (d'ordre 12 sans sous-groupe d'ordre 6, peut-être un peu dur à ce stade du cours).

1.8 Exercices

1. Montrer que $\mathbb{Z}/6\mathbb{Z}$ est isomorphe au produit $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.
2. Montrer que $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe au produit $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$. (Étudier l'ordre des éléments)
3. Déterminer tous les sous-groupes de $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$.
4. Soit $n \in \mathbb{N}^*$. Déterminer tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.
5. Décrire tous les groupes d'ordre 2, 3, 4, 5.
6. Soient x et y deux éléments de G. Montrer que xy et yx ont même ordre. Si x et y commutent et son d'ordre fini, montrer qu'il existe un élément d'ordre $ppcm(ordre(p), ordre(q))$.
7. Exercice sur les parties génératrices

8. Montrer qu'un groupe de cardinal 6 n'a pas que des éléments d'ordre deux.
9. Montrer qu'un groupe abélien d'ordre six est isomorphes à $\mathbb{Z}/6\mathbb{Z}$.
10. Soient p et q des nombres premiers. Montrer qu'un groupe abélien d'ordre pq est cyclique.
11. Montrer qu'un groupe d'ordre pair a un nombre impair d'éléments d'ordre deux. [1]

2 Opérations de groupes

2.1 Définition

Soit X un ensemble et G un groupe. Alors, une opération (ou action) (à gauche) de G sur X est la donnée d'un morphisme de groupes ρ de G dans $\mathrm{Bij}(X)$. Pour simplifier, on note $g \cdot x$ ou simplement gx l'élément $\rho(g)(x) \in X$, lorsqu'il n'y a pas d'ambiguité sur l'action de G sur X. L'opération est *fidèle* si ρ est injectif.

Si ρ est une opération de G sur X, on peut définir l'application $\phi : G \times X \to X,\ (g, x) \mapsto g \cdot x$. Elle vérifie les propriétés suivantes :

1. $\forall x \in X, \quad \phi(e, x) = x$;
2. $\forall g, g' \in G, \phi(g, \phi(g', x)) = \phi(gg', x)$.

Réciproquement, toute application $\psi : G \times X \to X$ vérifiant ces propriétés définit une opération de groupe de G sur X. C'est d'ailleurs souvent sous cette forme que l'on définit une opération de groupe. Les deux définitions ont leurs avantages, mais ceux de la seconde apparaissent plutôt en L3-M1, ou après.

Exemples 2.1.1. Si E est un espace vectoriel, alors le groupe $GL(E)$ des automorphismes linéaires de E opère sur E. L'opération est donnée par le morphisme de groupes (injectif) $GL(E) \hookrightarrow \mathrm{Bij}(E)$ (un automorphisme linéaire est en particulier une bijection). Si E est un espace affine, l'espace vectoriel $\overrightarrow{E}$, considéré comme groupe additif, opère sur E en translatant les points. Plus généralement, le groupe $GA(E)$ des applications affines bijectives de E dans E opère sur E. Si E est un espace vectoriel euclidien, et $O(E)$ est le groupe orthogonal, alors $O(E)$ opère sur E par isométries vectorielles. De même, si E est un espace affine euclidien, alors le groupe des isométries affines opère sur E. Toutes ces opérations sont fidèles.

2.2 Orbites

La relation binaire sur X définie par $x \sim y \Leftrightarrow (\exists g \in G,\ y = gx)$ est une relation d'équivalence. Ses classes d'équivalence sont les orbites de l'opération. L'orbite d'un élément x sera notée $\mathcal{O}(x)$, $\mathcal{O}_x$, $Orb(x)$, $G \cdot x$ ou Gx. Deux éléments sont équivalents s'ils sont dans la même orbite. On note Ω l'ensemble des orbites. L'ensemble X est union disjointe des orbites, autrement dit

$$X = \bigcup_{\omega \in \Omega} \omega.$$

Si G et X sont de cardinal fini, alors en prenant le cardinal on obtient l'égalité suivante :

$$|X| = \sum_{\omega \in \Omega} |\omega|.$$

Définitions 2.2.1.
1. L'opération est dite transitive s'il n'y a qu'une seule orbite.
2. Une orbite réduite à un élément x est dite triviale. Dans ce cas, cet élément est fixe sous G, autrement dit $gx = x,\ forall g \in G$. On dit que x est un point fixe sous G.
3. Si $g \in G$, on note $Fix(g) = \{x \in X \mid gx = x\}$. Ses éléments sont les points fixes de g. Attention un point fixe de g n'est fixe que pour g a priori, il n'est pas forcément fixe pour G en entier.

1. Ce résultat sera généralisé au chapitre deux.

Exemple 2.2.2. . G opère sur lui-même par translation à gauche : si $g \in G$, on définit $\rho(g)$, une bijection de G sur G, par : $x \mapsto gx$. Attention, $\rho(g)$ est seulement une bijection de G, pas un automorphisme, car l'image de 1 est g. Le groupe G opère également sur lui-même par translation à droite : si $g \in G$, on définit la bijection $\phi(g) : G \to G$ par : $x \mapsto xg^{-1}$.

Exemple 2.2.3. . Si H est un sous-groupe de G, alors H opère sur G par translation à droite de la même façon que ci-dessus : si $h \in H$, $\phi(h)$ est la bijection $x \mapsto xh^{-1}$. Les orbites pour cette opération sont les classes à gauche (pour H), du type gH. On peut aussi faire opérer H sur G par translation à gauche, les orbites sont les classes à droite.

Exemple 2.2.4. . Si g et h sont dans G, on appelle ghg^{-1} le conjugué de h par g (déjà vu). Ceci définit une opération de G sur lui-même par conjugaison, de la façon suivante. Si $g \in G$, on définit $\phi(g)$, une bijection de G sur G, par : $h \mapsto ghg^{-1}$. Cette fois-ci, c'est une opération par automorphisme de groupes et pas simplement par bijections : en effet, on vérifie facilement qu'une fois $g \in G$ fixé, la bijection $\phi(g)$ est un morphisme de groupes bijectif.

Exemple 2.2.5. . Si $A \subset G$ est une partie de G, alors gAg^{-1} est une partie de G, de même cardinal, différente de A ou pas. Donc G opère par conjugaison sur ses parties de cardinal fixé. De même, si H est un sous-groupe de G, alors gHg^{-1} est un sous-groupe de G, isomorphe à H.

Exemple 2.2.6. . Si H est un sous-groupe de G, alors G opère par translation à gauche sur l'ensemble des classes à gauche G/H, par $g \cdot xH = gxH$.

2.3 Stabilisateurs, formule des classes, formule de Burnside

Définitions 2.3.1.

1. Le stabilisateur d'un élément $x \in X$, noté $\mathrm{Stab}(x)$, est l'ensemble des $g \in G$ tels que $g \cdot x = x$. C'est un sous-groupe de G.
2. Si les stabilisateurs de tous les éléments de X sont triviaux (réduits à $\{e\}$), on dit que l'action est libre.
3. Une opération de G sur X est dite simplement transitive si elle est à la fois libre et transitive. Autrement dit, $\forall x, y \in X$, $\exists! g \in G$, $g \cdot x = y$. Ce concept est fondamental pour la suite du cours sur les polyèdres réguliers.

Soit maintenant $g \in G$, et $g.\mathrm{Stab}(x).g^{-1}$ le conjugué. On sait que c'est un sous-groupe de G. Soit $g' \in g.\mathrm{Stab}(x).g^{-1}$. Alors $g'(gx) = gx$, donc $g.\mathrm{Stab}(x).g^{-1} \subset \mathrm{Stab}(gx)$. En fait, il y a égalité. Pour l'inclusion inverse observer que $x = g^{-1}y$ conjuguer par g^{-1}.

Théorème 2.3.2. Soit G un groupe fini opérant sur un ensemble fini X, $x \in X$, et $\mathcal{O}(x)$ l'orbite de x. Alors, on a :

$$|G| = |\mathrm{Stab}(x)| \times |\mathcal{O}(x)|.$$

Preuve. Il suffit de montrer que $|G/\mathrm{Stab}(x)| = |\mathcal{O}(x)|$. Considérons la surjection

$$\psi_x : G \to \mathcal{O}(x), \quad g \mapsto g \cdot x.$$

Alors, $\psi_x(g) = \psi_x(g') \Leftrightarrow gx = g'x \Leftrightarrow g'^{-1}gx = x \Leftrightarrow g'^{-1}g \in \mathrm{Stab}(x)$, autrement dit les classes à gauche pour $\mathrm{Stab}(x)$ sont exactement les images réciproques de points. Par la propriété universelle du quotient, on en déduit que l'application ψ_x passe au quotient en une bijection

$$\phi_x : G/\mathrm{Stab}(x) \to \mathcal{O}(x), \quad \bar{g} \mapsto g \cdot x.$$

On l'appelle l'application orbitale. Comme cette application est une bijection, on en déduit l'égalité des cardinaux. □

Corollaire 2.3.3. (Formule des classes) Avec les notations et hypothèses du théorème, choisissons un représentant x_ω de chaque orbite ω. On a $|X| = \sum_{\omega \in \Omega} |\omega| = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}(x_\omega)|}$.

Théorème 2.3.4. (Formule de Burnside) Sous les mêmes hypothèses, le nombre d'orbites est

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

Preuve. Exercice. Considérer l'ensemble $A = \{(g, x) \in G \times X,\ gx = x\} \subset G \times X$, et calculer son cardinal de deux façons différentes, en l'écrivant comme une union sur les éléments $g \in G$, ou bien une union sur les éléments $x \in X$. Cette formule sera utile pour les polyèdres.

Remarque 2.3.5. Si G opère de façon simplement transitive sur X, alors G est en bijection avec X. Ceci sera également très utilisé dans l'étude des polyèdres réguliers pour déterminer les cardinaux de leurs groupes d'isométries.

Beaucoup de théorèmes que vous connaissez déjà se formulent en fait naturellement dans le langage des opérations de groupes (théorèmes de réduction des endomorphismes, ou de réduction des formes quadratiques). Il y a également de nombreuses applications en géométrie, en combinatoire ou en théorie des groupes. En voici une classique.

2.4 Théorème de Cauchy

Théorème 2.4.1. Soit G un groupe fini, et p un nombre premier divisant son cardinal. Alors, il existe un élément $g \in G$ d'ordre p.

Preuve. On fait opérer $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble X des p-uplets $(x_1, ...x_p)$ d'éléments de G tels que $x_1x_2...x_p = e$, par permutation circulaire des facteurs. On voit alors qu'il y a au moins $p-1$ éléments d'ordre p.

Application : dans un groupe d'ordre 6, il existe un élément d'ordre 2, et un autre d'ordre 3. Combien y a-t-il de groupes de cardinal 6 différents ? Autre application : soient p et q deux nombres premiers distincts, et G un groupe abélien d'ordre pq ; montrer que G est cyclique.

3 Groupe des permutations d'un ensemble fini

3.1 Généralités

Soit X un ensemble. On note $S_X = Bij(X)$ le groupe des bijections de X muni de la composition. On a déjà vu que si le cardinal de X excède 3, il n'est pas abélien. Le groupe S_X opère sur X par définition. Le support d'une bijection est l'ensemble des points qui ne sont pas fixes. Deux bijections à support disjoint commutent (explication imagée : elles ne touchent pas aux mêmes éléments, donc peu importe l'ordre dans lequel on les applique sur X). On a $Supp(f \circ g) \subset Supp(f) \cup Supp(g)$. Une partie $A \subset X$ est stable pour une transposition f si $f(A) \subset A$. On a une bijection induite $f|_A : A \to f(A)$. Si X est fini, on a forcément $A = f(A)$ si A est stable par f, mais si X est infini, ce n'est pas nécessaire.

Exemple 3.1.1. Soit $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^3$. C'est une bijection. Les seuls points fixes sont -1, 0 et 1. le support est $\mathbb{R} \setminus \{-1, 0, 1\}$. Les parties $\{0\}$, $[0, 1]$ et $[0, \frac{1}{2}]$ sont stables. Les parties $[\frac{1}{2}, 1]$ ou $[1, 2]$ ne sont pas stables.

Soit $n \in \mathbb{N}^*$, $X = \{1, 2, ..., n\}$, et $G = \mathfrak{S}_n$ le groupe des permutations de X. Il est de cardinal $n!$, et non commutatif si $n \geq 3$. Si σ est une permutation, on notera parfois σx au lieu de $\sigma(x)$.

Une permutation non triviale dont le support est de cardinal 2 est appelée 2-cycle, ou transposition. Une transposition est involutive (i.e. d'ordre 2). Une transposition de support $\{i, j\}$ sera souvent notée (i, j) ou $\tau_{i,j}$.

Voici plusieurs façons de représenter géométriquement une permutation, sur un exemple.

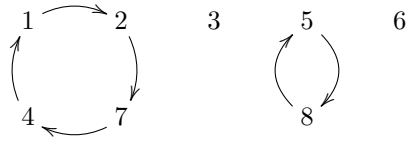
Sous forme de tableau (l'image d'un élément est située en-dessous de l'élément).

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 7 & 3 & 1 & 8 & 6 & 4 & 5 \end{pmatrix} \in \mathfrak{S}_8$$

En suivant les images des divers éléments, on peut écrire ceci sous la forme

$$1 \mapsto 2 \mapsto 7 \mapsto 4 \mapsto 1, \quad 3 \mapsto 3, \quad 5 \mapsto 8 \mapsto 5, \quad 6 \mapsto 6,$$

ou encore, de façon plus visuelle.



Cette écriture fait apparaître les parties stables $\{1, 2, 4, 7\}$, $\{5, 8\}$ et les points fixes 3 et 6. On verra au paragraphe suivant que cette écriture est unique.

3.2 Cycles

Soient $a_1, ...a_k$ des éléments distincts de $\{1, 2, ..., n\}$. L'application qui envoie a_k sur a_1, a_i sur a_{i+1}, et qui fixe les autres éléments, est appelée k-cycle. Son support est $\{a_1, ...a_k\}$, son ordre est k. On le note $(a_1, a_2, ...a_k)$. Par exemple,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 2 & 5 & 6 & 1 \end{pmatrix} \in \mathfrak{S}_7$$

est un 4-cycle de $\mathfrak{S}_7$. Son support est $\{1, 2, 4, 7\}$. On le note $(1, 4, 2, 7)$. Attention à l'ordre (modulo k) dans l'écriture d'un k-cycle : deux éléments sont consécutifs ssi le second est l'image du premier. Il n'y a pas unicité dans la façon de noter un cycle. Par exemple, on a $(1, 4, 2, 7) = (4, 2, 7, 1) = (2, 7, 1, 4) = (7, 1, 4, 2)$. Cependant, l'ordre est quand même important, par exemple $(1, 4, 2, 7) \neq (1, 2, 4, 7)$!

Exemple 3.2.1. La permutation $\phi : \{1, 2, ..., n\} \to \{1, 2, ..., n\}, \quad k \mapsto k + 1 (mod\, n)$ est appelée permutation circulaire. Elle est d'ordre n.

Soit $\sigma \in G$. Alors, le sous-groupe $\langle \sigma \rangle$ opère également sur X. Les orbites de cette action sont les orbites de σ. Une orbite réduit à un élément est dite triviale. Une permutation est un cycle s'il n'y a qu'une orbite non triviale. On dit que c'est un k-cycle si cette orbite est de cardinal k. Le support d'un k-cycle est précisément l'unique orbite non triviale, tous les autres éléments de X sont fixes. On admet qu'une permutation se décompose d'une unique manière sous forme de produit de cycles à supports disjoints (unicité modulo l'ordre dans lequel on place les cycles, donc).

3.3 Un système de générateurs

Théorème 3.3.1. Les transpositions engendrent le groupe symétrique, autrement dit, pour toute permutation σ, il existe des transpositions $\tau_1, \tau_2 ... \tau_l$ telles que $\sigma = \tau_l ... \tau_2 \tau_1$.

Preuve. Par récurrence sur le cardinal du support : si le support est de cardinal ≤ 1, c'est l'identité, c'est bon. Soit σ une permutation et $\mathrm{Supp}(\sigma)$ son support, dont on suppose que le cardinal est ≥ 2. Soit $x \in \mathrm{Supp}(\sigma)$. On a donc $x \neq \sigma(x)$ donc $\sigma\sigma(x) \neq \sigma(x)$ car σ est injective, et donc $\sigma(x) \in \mathrm{Supp}(\sigma)$. Soit τ la transposition qui échange x et $\sigma(x)$. Alors, $\mathrm{Supp}(\tau) \subset \mathrm{Supp}(\sigma)$, donc $\mathrm{Supp}(\tau\sigma) \subset \mathrm{Supp}(\sigma)$. D'autre part, $\tau\sigma(x) = x$, donc $x \notin \mathrm{Supp}(\tau\sigma)$, et donc le cardinal de $\mathrm{Supp}(\tau\sigma)$ et strictement inférieur à celui de $\mathrm{Supp}(\sigma)$. On applique l'hypothèse de récurrence à $\tau\sigma$, et on finit en remarquant que $\sigma = \tau\tau\sigma$. □

Remarque 3.3.2. Cette démonstration fournit un algorithme effectif pour décomposer une permutation σ en un produit de transpositions : prendre le plus petit entier k non fixe de la permutation, alors en notant τ la transposition qui échange k et $\sigma(k)$, on a $\sigma = \tau\tau\sigma$, et on recommence avec $\tau\sigma$.

3.4 Signature

Définition 3.4.1. Soit $\sigma \in \mathfrak{S}_n$ une permutation et Ω l'ensemble de ses cycles (y compris les triviaux). On définit $\epsilon(\sigma) = (-1)^{n-|\Omega|}$.

Exemple 3.4.2. La signature d'un k-cycle est $(-1)^{k-1}$ (il y a une orbite de cardinal k et $n-k$ orbites triviales). En particulier la signature d'une transposition est -1.

Théorème 3.4.3. La signature $\epsilon : \mathfrak{S}_n \to \{-1, 1\}$ est un morphisme de groupe.

Preuve. Par le théorème sur l'engendrement par les transpositions, il suffit de montrer que $\epsilon(\tau\sigma) = -\epsilon(\sigma)$ si τ est une transposition.

Soit $\tau = (i, j)$ une transposition. Il y a deux : soit i et j sont dans la même σ-orbite, soit non. Dessin. Dans le premier cas $\tau\sigma$ a une orbite de plus, dans le second cas une orbite de moins.

Définition 3.4.4. On note $\mathfrak{A}_n$ et on appelle groupe alterné le noyau de ϵ. Autrement dit, $\mathfrak{A}_n = \{\sigma \in S_n, \quad \epsilon(\sigma) = 1\}$. C'est un sous-groupe. Ses éléments sont appelés les permutations *paires*. Les permutations de signature -1 sont dites *impaires*.

Proposition 3.4.1. Le cardinal de $\mathfrak{A}_n$ est $n!/2$.

Preuve. si τ est une transposition, $\sigma \mapsto \tau\sigma$ est une bijection de $\mathfrak{S}_n$ qui induit une bijection de $\mathfrak{A}_n$ sur son complémentaire.

On verra apparaitre les groupes de permutation et alternés comme groupes d'isométries ou de déplacements de polyèdres ou polygones. Notamment $\mathfrak{S}_3$, $\mathfrak{S}_4$, et $\mathfrak{A}_5$.

3.5 Exercices sur la section

1. Savoir décomposer n'importe quelle permutation en produit de cycles disjoints. Savoir écrire la composée de deux permutations, savoir trouver le support. Savoir écrire n'importe quelle permutation comme produit de transpositions. Savoir calculer la signature d'une permutation.
2. Décrire tous les éléments de $\mathfrak{S}_3$, donner leur ordre, dresser la table de multiplication de ses éléments. Trouver tous les sous-groupes de $\mathfrak{S}_3$.
3. Soit $z = (a_1, ...a_k)$ un k-cycle, et σ une permutation. D'écrire le conjugué $\sigma z \sigma^{-1}$.
4. Montrer que $\mathfrak{S}_3$ est engendré par le 3-cycle $(1, 2, 3)$ et la transposition $(1, 2)$. De façon générale, si $\tau \in \mathfrak{S}_n$ est une transposition, montrer que $\mathfrak{S}_n$ est engendré par le n-cycle $(1, 2, ..., n)$ et τ.