Géométrie dans l'espace et visualisation : Compléments de cours sur les groupes Liste de résultats à connaître

Une partie a été vue en cours. Détails variables, peu au début, un peu plus ensuite. Les théorèmes importants sont démontrés. Nombreux (?) exemples.

1 Définitions de base sur les groupes

Généralités Loi de composition associative sur un ensemble. Élement neutre, unicité. Inverse, unicité de l'inverse. Groupe. Sous-groupe. 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.

Exemples. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, sont des groupes. Étant donné $n \in \mathbb{N}^*$, l'ensemble des racines n-èmes de l'unité est un sous-groupe de cardinal n de $(\mathbb{C}^*, \times)$.

Exemple. 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.

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

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. 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 $n\mathbb{Z}$ des entiers multiples de n. Tous les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$.

Exemple. 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 $x \in \mathbb{Z}$. Montrer rigoureusement que la formule « $\overline{x} + \overline{y} = \overline{x + y}$ » permet de définir une loi de composition interne, et que cela fait de $\mathbb{Z}/n\mathbb{Z}$ un groupe.

Exemple. Soit G un groupe noté multiplicativement, et $x \in G$. On définit l'application $\psi : \mathbb{Z} \to G$ par $\psi(k) = x^k$, avec la convention $x^0 = 1$, et, si $k < 0$, $x^k := (x^{-1})^{-k}$. Alors ψ est un morphisme de groupe de $\mathbb{Z}$ dans G.

Exemple. Soit G un groupe, et $g \in G$. On définit l'application $\phi : G \to G$ par $\phi(x) = gxg^{-1}$. C'est l'application de conjugaison par g (penser aux matrices). Alors, ϕ 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.

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. 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. $\mathbb{Z}$ 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. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est monogène (engendré par 1), donc cyclique.

Exercice. 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 $\mathbb{Z}/n\mathbb{Z}$.

Exemple. On appelle groupe dérivé de G et on note $D(G)$ le sous-groupe de g engendré par tous les éléments de la forme $xyx^{-1}y^{-1}$ (les commutateurs).

Groupes finis Un groupe fini est un groupe de cardinal fini. Si un groupe est fini, on dit aussi « ordre », à la place de cardinal.

Exemple. soit X un ensemble à n éléments. L'ensemble des bijections de X dans X (ou des permutations de X) est un groupe pour la composition des applications. Si $X = \{1, 2, ..n\}$, on le note $\mathfrak{S}_n$, on l'appelle le groupe symétrique sur n éléments. Son cardinal est $n!$. Si $n \geq 3$, le groupe n'est pas commutatif.

Exemple. $\mathbb{Z}/n\mathbb{Z}$ est un groupe fini d'ordre n, abélien.

Ordre d'un élément Soit G un groupe fini noté multiplicativement, et g un élément de G. L'application $f : \mathbb{N}^* \to G$, $n \to g^n$ ne peut pas être injective car $\mathbb{N}$ est infini. Il existe donc p et q avec $p < q$ tels que $g^p = g^q$, et donc, en multipliant par $(g^p)^{-1}$, on a $g^{q-p} = 1$. Il existe donc $k > 0$ tel que $g^k = 1$. Le plus petit tel entier est appelé l'ordre de g. C'est le cardinal du sous-groupe $\langle g\rangle$. Ce sous-groupe est constitué des éléments $1, g, g^2, g^3, ..., g^{ordre(g)-1}$ (démonstration : division euclidienne d'un entier par l'ordre de g).

Attention, dans un groupe infini, un élément peut avoir un ordre, ou pas (dans ce cas, on dit qu'il est d'ordre infini). Par exemple , dans $\mathbb{Z}$, l'élément 2 est d'ordre infini. Le groupe $\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$ est infini mais il contient un élément d'ordre 2 (et des éléments d'ordre infini).

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.

Théorème de Lagrange 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 : 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 important : 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 $\mathbb{Z}/p\mathbb{Z}$.

Remarque : 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 (peut-être un peu dur à ce stade du cours).

2 Opérations de groupes

Exemple fondamental. Soit X un ensemble, et σ une bijection de X dans lui-même. Alors on peut dire que σ *opère* (ou *agit*) sur l'ensemble X, en envoyant un élément x sur $\sigma(x)$. On peut aussi dire que le groupe des bijections de X dans lui-même $\mathrm{Bij}(X)$ opère tout entier sur l'ensemble X, par bijections. Par exemple, le groupe des permutations de $\{1, 2, ..., n\}$ opère sur $\{1, 2, ..., n\}$, en permutant les éléments. Il y a une définition plus générale, que voici.

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 $\phi : G \times X \to X,\ (g, x) \mapsto gx$. Exercice : déterminer à quelles conditions une application $\psi : G \times X \to X$ correspond à une opération de G sur X.

Autres exemples. 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.

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. Deux éléments sont équivalents s'ils sont dans la même orbite.

L'opération est transitive s'il n'y a qu'une seule orbite. Une orbite réduite à un élément x est dite triviale. Dans ce cas, cet élément est fixe sous G, autrement dit $gx = x,\ forall g \in G$.

Exemple. 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. 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. 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. 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. 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 $g \cdot xH = gxH$. Exercice.

Stabilisateurs Soit $x \in G$. Le stabilisateur de x, noté $\mathrm{Stab}(x)$, est l'ensemble des $h \in G$ tels que $hx = x$. C'est un sous-groupe de G. 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 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 $|G/\mathrm{Stab}(x)| = |\mathcal{O}(x)|$. Soit $\phi : G/\mathrm{Stab}(x) \to \mathcal{O}(x)$ l'application qui à une classe contenant un élément g associe le point $g \cdot x$. Cette application est bien définie : si g' est un autre élément de la classe, alors $g' = gh$ avec $h \in \mathrm{Stab}(x)$, d'où $g \cdot x = g' \cdot x$. On montre facilement que cette application est une bijection, d'où l'égalité des deux cardinaux. □

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.

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

La preuve consiste à faire 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

Généralités 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 $n \geq 3$. Le groupe G opère par définition sur l'ensemble X, si σ est une permutation, on notera parfois σx au lieu de $\sigma(x)$. Le support d'une permutation est l'ensemble des points $x \in X$ qui ne sont pas fixes. Deux permutations dont le support est disjoint commutent (explication imagée : elles ne touchent pas aux mêmes éléments, donc peu importe l'ordre dans lequel on les applique sur X). Une permutation non triviale dont le support est de cardinal 2 est appelée une transposition. Une transposition est d'ordre 2.

Exemple. La permutation $k \mapsto k+1 (mod n)$ est appelée permutation circulaire. Elle est d'ordre n.

Cycles Soit $\sigma \in G$. Alors, le sous-groupe $\langle \sigma \rangle$ opère également sur X. Les orbites de cette action sont les orbites, ou cycles, de σ. Un cycle réduit à un élément est dit trivial. Une permutation est un cycle s'il n'y a qu'un cycle non trivial. On dit que c'est un k-cycle si l'unique cycle non trivial est de cardinal k. Le support d'un k-cycle est précisemment l'unique cycle non trivial, tous les autres éléments de X sont des cycles triviaux, donc sont fixés par G. 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).

Théorème 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 $\text{Supp}(\sigma)$ son support, dont on suppose que le cardinal est ≥ 2. Soit $x \in \text{Supp}(\sigma)$. On a donc $x \neq \sigma(x)$ donc $\sigma\sigma(x) \neq \sigma(x)$ car σ est injective, et donc $\sigma(x) \in \text{Supp}(\sigma)$. Soit τ la transposition qui échange x et $\sigma(x)$. Alors, $\text{Supp}(\tau) \subset \text{Supp}(\sigma)$, donc $\text{Supp}(\tau\sigma) \subset \text{Supp}(\sigma)$. D'autre part, $\tau\sigma(x) = x$, donc $x \notin \text{Supp}(\tau\sigma)$, et donc le cardinal de $\text{Supp}(\tau\sigma)$ et strictement inférieur à celui de $\text{Supp}(\sigma)$. On applique l'hypothèse de récurrence à $\tau\sigma$, et on finit en remarquant que $\sigma = \tau\tau\sigma$. □

Remarque. 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 $\tau\sigma$. Exercice : démontrer que l'algorithme termine (voir la preuve du théorème).

Signature Le nombre de transpositions nécessaires pour écrire une permutation n'est pas bien défini, mais sa parité oui. C'est ce que l'on va démontrer.