Groupes

Les notes qui suivent sont ce que l'on pourrait considérer comme le squelette de ce qu'il faut savoir comme généralités sur les groupes.

Références. Vous pourrez consulter par exemple :
Élements de théorie des groupes par Josette Calais, Éditeur : Puf.
Groupes (observation, théorie, pratique) par Alain Bouvier et Denis Richard, Éditeur : Hermann.

Exemples. Voici une liste de groupes que l'on connaît et dans laquelle on puise exemples et contre-exemples pour comprendre la théorie :
- groupe des bijections d'un ensemble,
- groupes cycliques, groupes diédraux, groupes symétriques, groupes alternés,
- groupe additif d'un anneau (ou d'un corps), groupe multiplicatif des éléments inversibles d'un anneau (ou d'un corps) ou l'un de ses sous-groupes ; $\mathbb{R}^{+*}$, $\mathbb{C}^*$, $\mathbb{U} = \{z \in \mathbb{C}\,, |z| = 1\}$,
- espaces vectoriels de dimension finie,
- espaces vectoriels de dimension infinie, ensembles de polynômes ou de fonctions (continues, dérivables...),
- $\mathrm{GL}_n(K)$, $\mathrm{SL}_n(K)$, $\mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$,
- groupe des translations d'un espace affine, des isométries affines, homothéties, similitudes,
- groupe des homographies $h : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$.

1 Définitions, sous-groupes

Définitions 1.1 Groupe G. Sous-groupe $H \subset G$.

Définitions 1.2 Groupe commutatif, ou abélien.

Exemple 1.3 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 possède strictement plus de deux éléments, le groupe $S(E)$ n'est pas abélien.

1.4 Notations. Il est traditionnel d'adopter une notation multiplicative :
- gh pour le composé (*produit*) de deux éléments pour la loi de G,
- 1 pour l'élément neutre,
- g^{-1} pour l'*inverse* de g.

Cependant, dans le cas particulier des groupes abéliens, on utilise en général la notation additive ($g+h$ pour le composé, 0 pour l'élément neutre, $-g$ pour l'*opposé*).

Proposition 1.5 *Soit $\{H_i\}_{i\in I}$ une famille de sous-groupes de G. Alors l'intersection des H_i est un sous-groupe.*

Proposition 1.6 *Soit A une partie de G et $\langle A\rangle$ l'ensemble des produits $a_1 \dots a_n \in G$ tels que $n \geq 0$ est entier, et $a_i \in A$ ou $a_i^{-1} \in A$, pour tout i. Alors $\langle A\rangle$ est un sous-groupe de G, égal à l'intersection des sous-groupes de G contenant A.*

Définition 1.7 Le sous-groupe $\langle A\rangle$ est appelé *sous-groupe de G engendré par A.*

Définitions 1.8 Morphisme de groupes $f : G \to G'$. Noyau $N = \ker(f)$. Image $H' = \mathrm{im}(f) = f(G)$. Isomorphisme. Automorphisme.

Définition 1.9 Soit $g \in G$. On a les bijections suivantes :
Translation à gauche $\gamma_g : G \to G$, $\gamma_g(x) = gx$.
Translation à droite $\delta_g : G \to G$, $\delta_g(x) = xg$.

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. (Démonstration : exercice facile.) La classe d'équivalence de x ou *classe à gauche de x modulo H* est l'ensemble $xH = \gamma_g(H)$. L'ensemble des classes à gauche modulo H est noté G/H et on a une surjection $\pi : G \to G/H$ qui à x associe sa classe xH. 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. Noter que comme γ_g est une bijection, les classes sont toutes en bijection avec H.

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 $Hx = \delta_g(H)$, l'ensemble des classes à droite modulo H est noté $H\backslash G$, etc.

2 Groupes finis

Définitions 2.1 Ordre, ou cardinal, d'un groupe G ; notations : $|G|$, $\mathrm{card}(G)$, $\mathrm{ord}(G)$, $o(G)$.

Ordre d'un élément $g \in G$, notation : $\mathrm{ord}(g)$ ou $o(g)$.

Indice d'un sous-groupe $H \subset G$, notation : $[G : H]$ ou $(G : H)$.

Ces notions ont un sens dans le cas infini (groupe de cardinal infini, élément d'ordre infini, etc). Dans la suite de ce paragraphe, les groupes sont d'ordre fini.

Théorème 2.2 (Cayley) *Soit G un groupe fini d'ordre n et $S(G)$ le groupe des bijections de l'ensemble sous-jacent à G. Alors l'application $\gamma : G \to S(G)$ qui à g associe la translation à gauche $\gamma_g : G \to G$, est un morphisme injectif de groupes.*

Théorème 2.3 (Lagrange) *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 $(G : K) = (G : H)(H : K)$.*

Corollaire 2.4 *Dans un groupe fini d'ordre n on a, pour tout $x \in G$, $x^n = 1$.*

Démonstration : soit $H = \langle x \rangle$ 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 $x^n = (x^m)^d = 1$.

Définition 2.5 L'exposant a d'un groupe G est le plus petit entier k tel que $x^k = 1$ pour tout $x \in G$.

En fait, l'ensemble des $k \in \mathbb{Z}$ tels que $x^k = 1$ pour tout $x \in G$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $a\mathbb{Z}$. La remarque qui précède la définition montre que $a > 0$ et que a divise n.

3 Noyaux et images

Noyaux et images servent à étudier l'injectivité et la surjectivité d'un morphisme $f : G \to G'$. Précisément f est injectif ssi $\ker(f) = \{1\}$ et f est surjectif ssi $\mathrm{im}(f) = G'$.

3.1 Images. *Quels sous-groupes $H \subset G$ peuvent être l'image d'un morphisme $f : G' \to G$?*

La réponse est facile : tous, car H est l'image du morphisme injectif $i : H \to G$ donné par l'inclusion (c'est-à-dire $i(h) = h$). Nous consacrons le reste de ce paragraphe à la question :

3.2 Noyaux. *Quels sous-groupes $H \subset G$ peuvent être le noyau d'un morphisme $f : G \to G'$?*

La réponse est plus subtile. Si $H = \ker(f)$, alors pour tout $h \in H$ et pour tout $g \in G$ on a

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = 1$$

donc $ghg^{-1} \in H$. On est amené à faire une définition.

Définition 3.3 Un sous-groupe $H \subset G$ tel que pour tout $g \in G$, $gHg^{-1} \subset H$ est appelé un sous-groupe *distingué* (on dit parfois aussi *normal* ou *invariant*). On note alors $H \lhd G$.

Il y a des groupes qui possèdent des sous-groupes non distingués : par exemple, dans le groupe des isométries directes affines du plan (c'est-à-dire les rotations et les translations) le sous-groupe des rotations de centre l'origine n'est pas distingué.

C'est la même chose de dire que H est distingué, ou que les classes à gauche et à droite sont identiques ($xH = Hx$ pour tout x). Ainsi $G/H = H\backslash G$ et on appelle cet ensemble l'ensemble des classes modulo H.

On vient donc de voir que le noyau d'un morphisme est toujours un sous-groupe distingué. Réciproquement, nous allons voir que tout sous-groupe distingué $H \lhd G$ est le noyau d'un morphisme. En fait :

Théorème 3.4 *Si H est distingué, l'ensemble G/H possède une structure naturelle de groupe pour laquelle la surjection $\pi : G \to G/H$ est un morphisme de groupes.*

Dans cette situation, le noyau de π est égal à H, donc H est le noyau d'un morphisme. On a répondu à la question de départ ainsi : les sous-groupes $H \subset G$ qui sont le noyau d'un morphisme $f : G \to G'$ sont les sous-groupes distingués.