Bert Wiest
Université de Rennes 1
Institut Mathématique
Cours B03, Avril 2006

La théorie des groupes

Philosophiquement, un groupe est un ensemble sur lequel un a défini une opération binaire $G \times G \to G$ qui est, selon le cas, notée "+", ou "$*$", ou, le plus souvent, "$\cdot$" ("multiplication"). On demande que cette opération aie des propriétés raisonnables. Avant de donner la définition formelle, on va regarder quelques exemples.

1 Le groupe cyclique à n éléments

Exemple : le groupe cyclique à 12 éléments.

Première description On s'imagine une horloge avec *une* aiguille, qui peut prendre 12 positions possibles (pas de positions intermédiaires). On appelle les 12 positions $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{11}$. Sur l'ensemble des positions je peux définir une *addition*, par ex., $\overline{2}+\overline{3}=\overline{5}$, $\overline{3}+\overline{2}=\overline{5}$, $\overline{5}+\overline{7}=\overline{0}$, $\overline{9}+\overline{5}=\overline{2}$, $\overline{1}-\overline{8}=\overline{5}$. Une façon de faciliter les calculs dans cet objet est de légaliser les symboles $\overline{14}, \overline{25}, \overline{-9}$ etc, sous-entendant que $\ldots = \overline{-9} = \overline{3} = \overline{15} = \overline{27} = \ldots$. Donc, par exemple, $\overline{9}+\overline{5}=\overline{14}=\overline{2}$, $\overline{1}-\overline{8}=\overline{-7}=\overline{5}$.

Deuxième description On rappelle que l'ensemble $\mathbb{Z}/12\mathbb{Z}$ a 12 éléments, à savoir

$$\begin{aligned} \overline{0} := 12\mathbb{Z} &= \{\ldots, -12, 0, 12, 24, \ldots\} \\ \overline{1} := 1+12\mathbb{Z} &= \{\ldots, -11, 1, 13, 25, \ldots\} \\ \ldots &= \ldots \end{aligned}$$

Maintenant on définit sur $\mathbb{Z}/12\mathbb{Z}$ une addition :

$$(a+12\mathbb{Z})+(b+12\mathbb{Z}) := (a+b)+12\mathbb{Z}.$$

On observe que cette addition est bien-définie: si l'on rajoute un multiple de 12 à a ou à b, alors l'élément $(a+b)+12\mathbb{Z}$ de $\mathbb{Z}/12\mathbb{Z}$ ne change pas.

Idée: on calcule comme dans $\mathbb{Z}$, sauf on regarde tout qu'à multiples de 12 près.

Troisième description du même objet, et qui explique le nom "cyclique" : En $\mathbb{C}$, on définit $x := e^{\frac{2\pi i}{12}}$. On a $x^{12} = x^0 = 1$, et pour $a, k \in \mathbb{Z}$, on a $x^a = x^{a+12k}$. Voir figure 1.

Définition L'ensemble $\mathbb{Z}/12\mathbb{Z}$, muni de la structure d'addition, s'appelle le groupe cyclique à 12 éléments, et se note $(\mathbb{Z}/12\mathbb{Z}, +)$. Souvent on le note plus simplement $\mathbb{Z}/12\mathbb{Z}$.

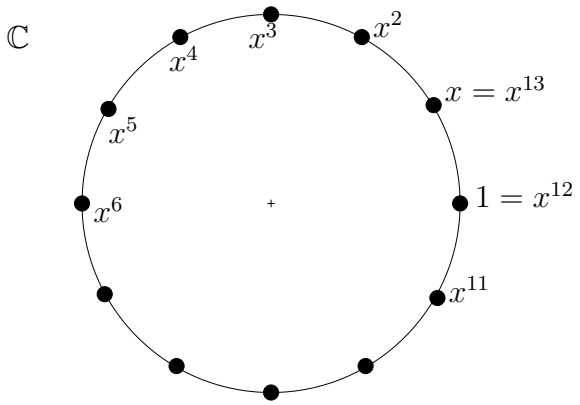

Figure 1: Le groupe cyclique à 12 éléments

De façon semblable, on définit le groupe cyclique $\mathbb{Z}/1463\mathbb{Z}$ à 1463 éléments, ou en général $\mathbb{Z}/n\mathbb{Z}$ à n éléments...

On observe que $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$, c.à.d. le groupe est *commutatif*.

2 Le groupe symétrique S_n ($n \in \mathbb{N}$)

Ceci est notre premier exemple d'un groupe non-commutatif. On rappelle qu'il y a $n!$ bijections $\{1, \ldots, n\} \to \{1, \ldots, n\}$. Autrement dit, il y a $n!$ permutations de l'ensemble $\{1, \ldots, n\}$.

Notation On note $\left(\begin{smallmatrix}1&2&3&4\\3&2&4&1\end{smallmatrix}\right)$ la permutation σ telle que $\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 4, \sigma(4) = 1$. (On verra une autre notation bientôt.)

Étant donné σ et τ, deux permutations, il est naturel de regarder leur composition $\tau \circ \sigma$ (d'abord σ, puis τ, on lit de droite à gauche comme pour la composition de fonctions).

Exemple Si $\sigma = \left(\begin{smallmatrix}1&2&3&4\\3&2&4&1\end{smallmatrix}\right)$ et $\tau = \left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right)$, alors $\tau \circ \sigma = \left(\begin{smallmatrix}1&2&3&4\\4&1&3&2\end{smallmatrix}\right)$ et $\sigma \circ \tau = \left(\begin{smallmatrix}1&2&3&4\\2&3&1&4\end{smallmatrix}\right)$.

Nous allons interpréter la composition comme une "multiplication" de permutations. Cette multiplication est non-commutative: comme l'exemple précédent le montre, on a en général $\sigma \circ \tau \neq \tau \circ \sigma$.

Chaque bijection a un inverse (une fonction réciproque) – par exemple, $\sigma^{-1} = \left(\begin{smallmatrix}1&2&3&4\\4&2&1&3\end{smallmatrix}\right)$. Géométriquement, pour calculer l'inverse σ^{-1} d'un élément σ, il suffit de prendre la réflexion du dessin de σ dans un axe horizontal.

Définition L'ensemble des permutations d'un ensemble avec n éléments, muni de cette structure de multiplication, s'appelle le *groupe symétrique*, et se note S_n.

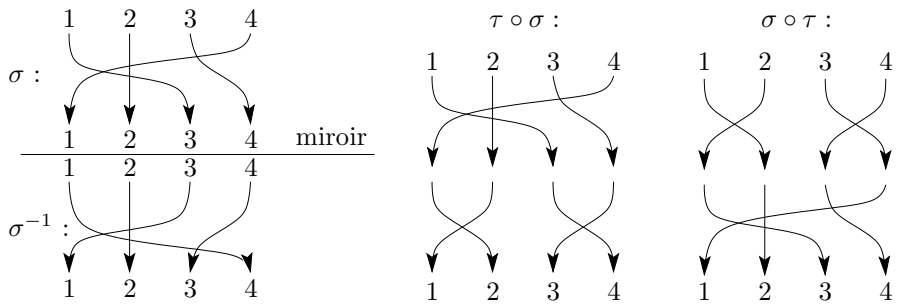

Figure 2: Exemples de multiplication et d'inversion dans S_4

Donc S_n est un groupe non-commutatif avec $n!$ éléments.

3 Groupe des symétries d'un objet géométrique

On s'intéresse aux groupes pas seulement parce qu'on adore l'algèbre, mais aussi parce que les groupes apparaîssent souvent très naturellement comme l'ensemble de toutes les symétries d'un objet donné. On va regarder quelques exemples.

Soit X un objet géométrique – par exemple, dans le plan, un coeur, la lettre Φ, un pentagone régulier,...

Définition informelle Une *symétrie* de X est une application (bijective) rigide de X vers lui-même.

Étant donné deux symétries $r\colon X \to X$ et $s\colon X \to X$, on peut considérer la composée $r \circ s$. De nouveau, on va interpréter la composition comme une "multiplication" de symétries.

Nous observons que toute symétrie r a un "inverse" r^{-1}, à savoir l'application inverse.

Définition Le *groupe des symétries* de X est l'ensemble des symétries de X, muni de la structure de multiplication donnée par composition.

Exemple Le coeur $\heartsuit$. Son groupe de symétries a deux éléments, à savoir l'application identité id, et l'application r_v : réflexion dans l'axe verticale. On observe que $r_v \circ r_v = id$.

Exemple La lettre Φ. Son groupe de symétries a quatre éléments : l'identité id, les deux réflexions r_h et r_v, et la rotation par l'angle π, qu'on va noter t_π. Exemple de la multiplication : $r_h \circ r_v = t_\pi$; et $t_\pi \circ t_\pi$ est la rotation par un angle de 2π, ce qui est la même application que l'application identique, donc $t_\pi \circ t_\pi = id$.

Exemple Le pentagone régulier $\pentagon$. Son groupe de symétries a 10 éléments, à savoir les rotations $t_0 = id$, $t_{2\pi/5}$, $t_{4\pi/5}$, $t_{6\pi/5}$, $t_{8\pi/5}$, ainsi que les 5 réflexions

dans les 5 axes de symétrie. Les règles de multiplication sont un peu compliqués dans cet exemple – on peut néanmoins observer que le produit de deux réflexions est toujours une rotation.

Plus généralement, le groupe de symétries d'un n-gone régulier (si n est impair) a exactement $2n$ éléments. Ce groupe s'appelle le *groupe dihédral* D_{2n}.

Exemple Le symbole ⏚ (je m'excuse pour la ressemblance avec la croix gammée, qui est en effet le seul symbole bien-connu ayant le groupe de symétrie que je veux). Son groupe de symétrie a, lui aussi, quatre éléments, à savoir les rotations $t_0 = id$, $t_{\pi/2}$, t_π, $t_{3\pi/2}$.

Comparons les groupes de symétrie de la lettre Φ et de ⏚ . On s'aperçoit intuitivement que leur symétries sont de nature très différentes, bien qu'il y en aie quatre dans les deux cas. En va rendre cette intuition exacte bientôt.

4 Groupes, ordres d'éléments, systèmes de générateurs

Définition Un groupe $(G, \cdot)$ est un ensemble G muni d'une opération binaire "$\cdot$", qu'on appelle la multiplication, telle que

- La multiplication est associative : si $g, h, k \in G$ alors $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.
- il existe un élément e, qu'on appelle l'élément neutre, qui a la propriété que pour tout $g \in G$, $g \cdot e = g$ et $e \cdot g = g$.
- Pour tout élément g il existe un élément qu'on note g^{-1} et qu'on appelle l'inverse de g, qui est caractérisé par la propriété que $g \cdot g^{-1} = e$ et $g^{-1} \cdot g = e$.

On peut démontrer (exercice) que dans un groupe il existe un *seul* élément neutre, et que pour tout élément g il existe un *seul* élément inverse g^{-1}.

Attention, la multiplication n'est pas forcement commutative !!!

Exercice Se convaincre que $(\mathbb{Z}, +)$, $(\mathbb{Z}^2, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$ sont des groupes.

Exercice De même, démontrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(S_n, \circ)$ sont des groupes.

En particulier, il y a des groupes avec un nombre fini d'éléments, et d'autres avec un nombre infini !

Exercice difficile Soit p un nombre premier. Démontrer que $((\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}), \cdot)$ est un groupe (avec $p-1$ éléments) – ici, $\cdot$ note la multiplication habituelle. Indication: il faut d'abord vérifier que la multiplication est bien-définie. La partie vraiment astucieuse est de démontrer que tout élément a un inverse, c.à.d. que pour tout $k \in \{1, \ldots, p-1\}$, il existe un nombre $\ell \in \{1, \ldots, p-1\}$ tel que le nombre $k \cdot \ell$ appartient à $1 + p\mathbb{Z}$ (c.à.d., que $\overline{k \cdot \ell} = \overline{1} \in \mathbb{Z}/p\mathbb{Z}$).

Définition Un sous-ensemble S d'un groupe G *engendre* le groupe G si tout élément de G s'écrit comme produit d'éléments de S.

Définition L'*ordre* d'un élément g d'un groupe $(G, \cdot)$ est

$$ord(g) = \inf\{n \in \mathbb{N}^* \mid g^n = e\}.$$

(Ici, g^n note le produit avec n facteurs $g \cdot g \cdot \ldots \cdot g$.) Attention, l'ordre peut être un entier positif ou égal à $+\infty$.

Remarque L'ordre d'un élément n'a rien a voir avec les ordres partielles ou totaux sur un ensemble qu'on a vus précédemment dans le cours. On utilise, malheureusement, le même mot pour deux choses complètement différentes.

Exemples (a) Dans $(\mathbb{Z}, +)$, l'ensemble $\{1\}$ engendre le groupe. De même, $\{-1\}$ engendre le groupe. Aucun autre élément peut, lui seul, engendrer le groupe.

(b) Le groupe cyclique $(\mathbb{Z}/15\mathbb{Z}, +)$ n'est pas engendre par $\{\overline{6}\}$, car les seuls multiples de $\overline{6}$ sont

$$\overline{6},\ \overline{6}+\overline{6} = \overline{12},\ \overline{6}+\overline{6}+\overline{6} = \overline{18} = \overline{3},\ \overline{6}+\overline{6}+\overline{6}+\overline{6} = \overline{9},\ \text{et } \overline{6}+\overline{6}+\overline{6}+\overline{6}+\overline{6} = \overline{0}.$$

Explication pourquoi : 6 et 15 ont un facteur commun 3, donc les multiples de $\overline{6}$ dans $\mathbb{Z}/15\mathbb{Z}$ sont tous de la forme $\overline{\ell}$, où ℓ est un entier entre 0 et 14 qui est divisible par 3.

Exercice facile : vérifier à la main que, par contre, $\overline{8}$ engendre le groupe $\mathbb{Z}/15\mathbb{Z}$.

(c) (Généralisation de **(b)**) Regardons le groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$. Soit a un entier entre 0 et $n-1$. L'ordre de $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ se calcule par la formule

$$ord(a) = \frac{ppcm(a, n)}{a}$$

Démonstration de cette dernière formule : l'ordre de a est, par définition, le plus petit $k \in \mathbb{N}^*$ tel que $k \cdot a$ est un multiple de n. Donc k a la propriété que $k \cdot a = ppcm(a, n)$. On conclut que $k = \frac{ppcm(a,n)}{a}$. □

On peut déduire de cette formule une équivalence

$$\{\overline{a}\} \text{ engendre le groupe } \mathbb{Z}/n\mathbb{Z} \ \Leftrightarrow\ pgcd(a, n) = 1,$$

c.à.d., si et seulement si a et n n'ont pas de diviseur en commun.

(d) Dans le groupe des symétries de la lettre Φ, l'identité est d'ordre 1, et les trois autres éléments sont d'ordre 2 (vérifiez !). Par contre, dans le groupe des symétries de  , l'élément $t_{\pi/2}$ est d'ordre 4. Donc, effectivement, Φ et n'ont pas le même groupe de symétries.

Remarque hors programme En fait, on peut démontrer que le groupe de symétries de est "isomorphe" au groupe cyclique $\mathbb{Z}/4\mathbb{Z}$, et celui de Φ est isomorphe à un groupe qui s'appelle $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ – on ne va pas définir formellement la signification du mot "isomorphe".

5 Groupes de permutations (suite)

Définition On dit qu'un élément σ de S_n est un *cycle d'ordre* k, ou un k-*cycle*, s'il existent $a_1, a_2, \ldots, a_k \in \{1, \ldots, n\}$ tels que

- σ envoie a_1 sur a_2, a_2 sur a_3,...,a_{k-1} sur a_k, et a_k sur a_1,
- σ fixe tous les autres éléments de S_n.

Notation alternative pour un tel élément : $\sigma = (a_1\ a_2\ \ldots\ a_k)$.

Exemple Dans S_4, l'élément $\sigma = \left(\begin{smallmatrix}1&2&3&4\\3&2&4&1\end{smallmatrix}\right)$ est le 3-cycle (1 3 4). Une autre notation pour encore le même élément serait (3 4 1), ou encore (4 1 3).

Observation L'ordre d'un k-cycle est k (d'où le nom !). Par exemple,

$$\text{si } \sigma = (1\ 3\ 4),\ \text{alors } \sigma^2 = (1\ 4\ 3) \text{ et } \sigma^3 = id.$$

Notation On dit qu'une permutation σ est un *cycle* s'il existe un $k \in \mathbb{N}$ tel que σ est un k-cycle.

Observation Toute permutation s'écrit comme un produit de cycles *disjoints* (c.à.d., un nombre qui apparaît dans un cycle ne doit pas apparaître dans un autre cycle). Par exemple, dans S_9, on a

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9\\5&2&8&3&7&1&6&4&9\end{pmatrix} = (1\ 5\ 7\ 6)(2)(3\ 8\ 4)(9).$$

On peut simplifier encore plus cette notation : les 1-cycles peuvent être supprimés de la notation, et on écrit simplement (1 5 7 6)(3 8 4). Dans cette écriture il est sous-entendu que les $\sigma(2) = 2$ et $\sigma(9) = 9$. Donc σ est un produit d'un 4-cycle et d'un 3-cycle disjoint. Une image assez intuitive est dans la figure 3.

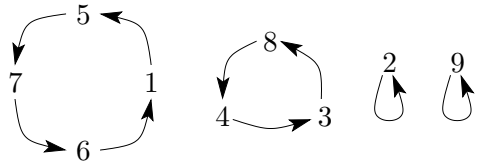

Figure 3: La permutation $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9\\5&2&8&3&7&1&6&4&9\end{smallmatrix}\right)$

Quelle est l'ordre de σ ? Réponse : $ord(\sigma)$ est le plus petit $k \in \mathbb{N}$ tel que $(1\ 5\ 7\ 6)^k = id$ *et* $(3\ 8\ 4)^k = id$. Donc, k est le plus petit entier qui est un multiple de 4 et de 3, c.à.d., $k = ppcm(3, 4) = 12$.

Plus généralement, on a

Proposition *Si σ est un élément qui a une décomposition en c cycles disjoints de longueur $n_1, n_2, \ldots, n_c$, alors $ord(\sigma) = ppcm(n_1, n_2, \ldots, n_c)$.*

Notation Un 2-cycle dans S_n s'appelle aussi une *transposition* – donc, une transposition est une permutation qui échange deux éléments de $\{1, \ldots, n\}$, et laisse tous les autres éléments fixes. Par exemple, l'élément $(3\ 7) \in S_8$ est une transposition.

Proposition *$S := \{$transpositions dans $S_n\}$ engendre S_n. Autrement dit, toute permutation s'écrit comme un produit de transpositions.*

Deux démonstrations *Première :* Il suffit de démontrer que tout *cycle* s'écrit comme produit de transpositions. Au lieu de donner une démonstration rigoureuse, on donne juste un exemple qui montre bien la recette générale. Par exemple, dans S_6

$$(3\ 1\ 6\ 2\ 4) = (3\ 1)(1\ 6)(6\ 2)(2\ 4) \qquad \text{(vérifiez cette égalité !)}.$$

Deuxième démonstration, qui est plus géométrique. On regarde encore l'exemple $\sigma = (3\ 1\ 6\ 2\ 4)$. Une façon géométrique de trouver une décomposition de σ en un produit de transpositions est dans la figure 4.

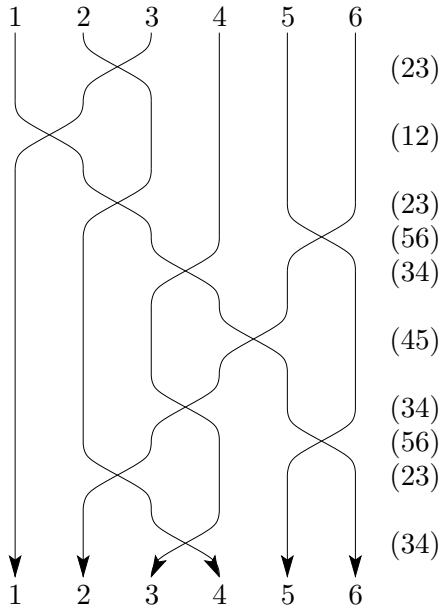

Figure 4: Pour trouver une écriture d'une permutation comme produit de transpositions (et mieux encore, de transpositions "adjacentes"): $(3\ 1\ 6\ 2\ 4) = (3\ 4)(2\ 3)(5\ 6)(3\ 4)(4\ 5)(3\ 4)(5\ 6)(2\ 3)(1\ 2)(2\ 3)$

Définition Soit $\sigma \in S_n$ une permutation. On dit que σ est *paire* si, dans une écriture de σ comme produit de transpositions, il y a un nombre pair de facteurs. On dit que σ est *impaire* si, dans une écriture de σ comme produit de transpositions, il y a un nombre impair de facteurs.

Par exemple, $\sigma = (3\ 1\ 6\ 2\ 4)$ est paire, parce qu'on a écrit σ comme un produit de 4 facteurs, et 4 est un nombre pair. On a, d'ailleurs, trouvé une autre écriture avec 10 facteurs (qui correspondent aux 10 croisements dans la figure 4), mais 10 est un nombre pair aussi. Ceci est une bonne illustration du résultat suivant :

Proposition *La définition précédente est raisonnable : si σ a une écriture comme un produit de k transpositions, où k est pair, alors toute autre écriture comme un produit de transpositions a aussi un nombre pair de facteurs. De même dans le cas k impair.*

Démonstration admise.

En général, on a vu (dans la "Première démonstration") qu'un k-cycle s'écrit comme produit de $k-1$ transpositions. Donc:

Proposition *Si σ est un k-cycle avec k pair, alors σ est impaire, et si k est impaire, alors σ est paire.*