Université de Bourgogne

Structures algébriques fondamentales

Johan Taflin

2019-2020

johan.taflin@u-bourgogne.fr
Bureau : A316

Préface

Ce texte est destiné aux étudiants de deuxième année de licence à l'université de Bourgogne. Il s'agit d'une à la théorie des groupes. Cette version est susceptible de contenir des coquilles et des erreurs. Tout commentaire est le bienvenu.

Méthodologie : L'assimilation d'un nouveau cours est difficile et exige un travail personnel concéquent. Il est important de s'approprier les notions, de trouver ses propres exemples et contre-exemples, de connaître les définitions, de s'interroger sur les hypothèses des énoncés etc.

Par ailleurs, il est illusoire de penser que ces notes de cours puissent remplacer une présence attentive en cours magistral.

Table des matières

Chapitre 1

Groupes

Malgré sa simplicité, la notion de groupe s'avère particulièrement importante. Elle intervient aussi bien dans des problèmes abstraits que dans des applications concrètes.

1.1 Définitions et exemples

Définition 1.1. On appelle *groupe* un ensemble G muni d'une loi $*\colon G\times G\to G$, $(a,b)\mapsto a*b$ telle que

i) la loi $*$ est *associative* c-à-d pour tout a,b,c dans G, $(a*b)*c=a*(b*c)$,

ii) il existe un *élément neutre* e c-à-d pour tout a dans G, $a*e=e*a=a$,

iii) tout élément de G possède un *inverse* c-à-d pour tout a dans G, il existe b dans G tel que $a*b=b*a=e$.

On parle alors du groupe $(G,*)$ ou simplement G s'il n'y a pas d'ambiguïté sur la loi.

Remarque 1.2. Bien que la loi n'est souvent pas explicitée dans les notations, un groupe est la donnée d'un ensemble **et** d'une loi. En particulier, l'inverse d'un élément dépend de la loi. Comme nous allons le voir, l'inverse de 2 pour la loi $+$ est -2 alors que l'inverse de 2 pour la loi $\times$ est $1/2$.

Lemme 1.3. *Soit $(G,*)$ un groupe. L'élément neutre de la loi $*$ est unique.*

Démonstration. Soit e et e' deux éléments neutres de $(G,*)$. Par définition, on a alors

$$e'=e'*e=e.$$

Donc $e=e'$ et il n'y a qu'un élément neutre. □

Lemme 1.4. *Soit $(G,*)$ un groupe. Soit $a\in G$. Montrer que l'inverse de a est unique.*

Démonstration. Soit $a\in G$. Soit $b,c\in G$ deux inverses de a, c-à-d

$$a*b=b*a=e=a*c=c*a.$$

En particulier, $a*c=e$ et en multipliant à gauche par b on obtient

$$b*(a*c)=(b*a)*c=e*c=c$$

pour le premier terme et

$$b * e = b$$

pour ce second. Donc $b = c$. □

Dans la suite de ce chapitre G désignera toujours un groupe dont l'élément neutre est noté e.

Remarque 1.5. 1) On note souvent a^{-1} l'inverse de a mais ce n'est pas toujours le cas (voir les exemples ci-dessous).
2) Il arrive souvent, quand la loi est notée $*$, $\cdot$ ou $\times$, de ne plus mettre le symbole de la loi, c-à-d écrire ab à la place de $a * b$.
3) Si $a \in G$ alors on utilise souvent les notations suivantes (qui sont définies pour récurrence) :
— $a^0 = e$, où e est l'élément neutre de G,
— si $n \geq 0$ est un entier alors $a^{n+1} = a * (a^n)$,
— si $n \leq -1$ est un entier négatif alors $a^n = (a^{-1})^{|n|}$.
On vérifie alors que pour tout $n, l \in \mathbb{Z}$, $a^{l+n} = (a^l) * (a^n)$. Si le symbole pour la loi est $+$ alors on écrira na à la place de a^n.

En utilisant ces notations, on pose la définition suivante.

Définition 1.6. Soit $a \in G$. On dit que a est d'*ordre fini* s'il existe un entier $k \geq 1$ tel que $a^k = e$. Dans ce cas, le plus petit $k \geq 1$ vérifiant cette égalité s'appelle l'*ordre* de a.

Exemple 1.7 (de groupes)**. 1)** L'ensemble des entiers relatifs $\mathbb{Z}$ muni de la loi d'addition est un groupe $(\mathbb{Z}, +)$. L'élément neutre correspond à 0 et si n est dans $\mathbb{Z}$ alors son inverse (dans le sens de ce cours) est $-n$.
2) $(\mathbb{N}, +)$ n'est pas un groupe car 1 n'a pas d'inverse pour la loi $+$ dans $\mathbb{N}$.
3) $(\mathbb{R}, +)$ est aussi un groupe dont l'élément neutre est 0 et l'inverse de x est $-x$.
4) $(\mathbb{R}, \times)$ n'est pas un groupe car 0 n'a pas d'inverse pour la loi $\times$. En revanche, si on note $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ alors $(\mathbb{R}^*, \times)$ est un groupe. Son élément neutre est 1 et l'inverse de x est x^{-1}.
5) Si $(E, +, \cdot)$ est un espace-vectoriel (où $+$ est l'addition de vecteurs et $\cdot$ est la multiplication d'un vecteur par un scalaire) alors $(E, +)$ est un groupe.

Remarque 1.8. Dans tous les exemples ci-dessus, on a que $a * b = b * a$. Mais ceci n'est pas vrai pour tout les groupes, ce qui motive la définition suivante.

Définition 1.9. Un groupe $(G, *)$ est dit *abélien* (ou encore *commutatif*) si tout a, b dans G vérifient $a * b = b * a$.

Remarque 1.10. Dans un groupe G non abélien, il faut faire attention à l'inverse d'un produit. Si a, b sont dans G alors $(a * b)^{-1} = b^{-1} * a^{-1}$ et a priori $(a * b)^{-1} \neq a^{-1} * b^{-1}$. En effet,

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e.$$

En particulier, **il ne faut pas écrire** $\frac{a}{b}$ à la place de $a * (b^{-1})$.

L'un des exemples les plus simples de groupes non-abélien provient de la construction suivante.

Définition 1.11. Soit E un ensemble. On note par $S(E)$ (où parfois $\mathrm{Bij}(E)$) l'ensemble des bijections de E dans E. On vérifie facilement que la loi de composition des applications $\circ$ est une loi sur $S(E)$ telle que $(S(E),\circ)$ est un groupe. En effet, fixons 3 éléments f,g et h de $S(E)$, c-à-d trois bijections de E. On vérifie (faites-le !) alors que

- $g\circ f$ est encore un élément de $S(E)$,
- $h\circ(g\circ f)=(h\circ g)\circ f$,
- l'application Id_E, définie par $\forall x\in E\ \mathrm{Id}_E(x)=x$, est l'élément neutre de $(S(E),\circ)$, c-à-d
$$\mathrm{Id}_E\circ f=f\circ\mathrm{Id}_E=f,$$
- l'inverse de f pour $\circ$ est son application réciproque f^{-1}, i.e.
$$f\circ f^{-1}=f^{-1}\circ f=\mathrm{Id}_E.$$

Ce groupe s'appelle le *groupe symétrique de E* ou encore *groupe des permutations de E*. Quand $n\geq 1$ est un entier, on note S_n à la place de $S(\{1,\cdots,n\})$ pour le groupe de permutations des n premiers entiers.

Notation 1.12. Si f est dans S_n, on utilisera souvent la notation
$$f=\begin{pmatrix}1 & \cdots & n\\ f(1) & \cdots & f(n)\end{pmatrix},$$
et parfois, plus simplement en oubliant la ligne du haut,
$$f=\begin{pmatrix}f(1) & \cdots & f(n)\end{pmatrix}.$$
Par exemple, si $n=3$ et $f,g\in S_3$ sont définis par $f(1)=2$ $f(2)=1$ $f(3)=3$ et $g(1)=2$ $g(2)=3$ $g(3)=1$ alors
$$f=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\quad\text{et}\quad g=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}.$$

Attention à ne pas confondre ces notations avec des matrices. Dans ce cadre, les composées $f\circ g$ et $g\circ f$ sont
$$f\circ g=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\quad\text{et}\quad g\circ f=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$
car
$$f\circ g(1)=1\ \ f\circ g(2)=3\ \ f\circ g(3)=2\ \text{ et }\ g\circ f(1)=3\ \ g\circ f(2)=2\ \ g\circ f(3)=1.$$
Cela n'a rien à voir avec les produits de $\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$ avec $\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ au sens matricielle (qui ne sont d'ailleurs pas bien définis pour des raisons de taille).

Exemple 1.13. On vient de voir que S_3 n'est pas abélien car
$$f\circ g=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\neq\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}=g\circ f.$$
Ceci est également vrai pour S_n pour tout $n\geq 3$.

Voici un autre exemple de groupe non-abélien.

Exemple 1.14. Soit $n \geq 2$ un entier. On note par $\mathrm{Gl}_n(\mathbb{R})$ l'ensemble des matrices de taille $n \times n$ à coefficients réels qui sont inversibles. Si $\times$ désigne la multiplication matricielle alors $(\mathrm{Gl}_n(\mathbb{R}), \times)$ est un groupe non-abélien. Son élément neutre est la matrice identité de taille $n \times n$ et si $A \in \mathrm{Gl}_n(\mathbb{R})$ alors son inverse est simplement l'inverse A^{-1} au sens matriciel.

Définition 1.15. Soit $(G, *)$ un groupe. On dit que $H \subset G$ est un *sous-groupe* de G si
i) H est non-vide,
ii) pour tout a, b dans H, $a * b$ est aussi dans H,
iii) pour tout a dans H, a^{-1} est aussi dans H.
On écrit $H < G$ pour signifier que H est un sous-groupe de G.

On vérifie facilement que si $H < G$ alors l'élément neutre e de G est dans H. En effet, H est non-vide donc il existe $a \in H$ et donc par iii) a^{-1} est aussi dans H et d'après ii) c'est encore le cas pour $e = a * a^{-1}$. On peut donc remplacer la condition i) ci-dessus par $e \in H$. On vérifie de manière similaire que la restriction de $*$ à H lui confère une structure de groupe.

Remarque 1.16. Un groupe G a toujours deux sous-groupes "triviaux" : $\{e\}$ et G tout entier.

Exemple 1.17. Pour tout $k \in \mathbb{N}$, l'ensemble $k\mathbb{Z} := \{kn \,|\, n \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$. Nous verrons en TD que ce sont les seuls sous-groupes de $\mathbb{Z}$.

Une intersection de sous-groupes est encore un sous-groupes. En revanche, une union de sous-groupes n'est pas forcement un sous-groupe.

Proposition 1.18. Soit $(G, *)$ un groupe et soit $(H_i)_{i \in I}$ une famille de sous-groupes de G (c-à-d pour chaque i dans I, H_i est un sous-groupe de G). Alors $\cap_{i \in I} H_i$ est un sous-groupe de G.

Démonstration. Comme nous l'avons remarqué ci-dessus, un sous-groupe de G contient toujours l'élément neutre e donc pour tout i dans I, e est dans H_i c-à-d $e \in \cap_{i \in I} H_i$ et donc cet ensemble est non-vide. Si a et b sont dans $\cap_{i \in I} H_i$ alors pour tout $i \in I$, a et b sont dans H_i et donc $a * b$ appartient à H_i. Cela montre que $a * b \in \cap_{i \in I} H_i$. On procède de même pour l'inverse : si a est dans $\cap_{i \in I} H_i$ alors pour tout $i \in I$, $a \in H_i$ et donc $a^{-1} \in H_i$ ce qui implique que $a^{-1} \in \cap_{i \in I} H_i$. □

Exemple 1.19. Si k_1 et k_2 sont deux entiers alors $k_1\mathbb{Z} \cap k_2\mathbb{Z} = k_3\mathbb{Z}$ où k_3 est le ppcm de k_1 et k_2.

Définition 1.20. Soit G un groupe et soit $A \subset G$ un sous ensemble non-vide. On appelle *sous-groupe engendré par* A l'intersection de tous les sous-groupes de G contenant A. On le note $< A >$.

D'après la Proposition 1.18, $< A >$ est un sous-groupe de G. Il s'agit en fait du plus petit sous-groupe de G contenant A dans le sens que si H est un sous-groupe de G contenant A alors $< A > \subset H$.

1.2 Groupes finis

Un cas particulièrement important de groupes est le cas où l'ensemble G est fini. Rappelons que si E est un ensemble fini, le *cardinal* de E est simplement le nombre d'éléments de E. On le note $\mathrm{Card}(E)$ ou $|E|$.

Définition 1.21. Un groupe $(G,*)$ est dit fini si l'ensemble G est fini. Le cardinal de G s'appelle alors l'*ordre* de $(G,*)$.

Exercice 1.22. Montrer que tout éléments d'un groupe fini est d'ordre fini.

Exemple 1.23. 1) Le groupe symétrique S_n (défini dans la Définition 1.11) est un groupe fini. On peut montrer que son ordre est $n!$ (c-à-d $1\times 2\times\cdots\times n$).
2) Soit $n\geq 2$ un entier. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\{0,\dots,n-1\}$ muni de la loi $+$ définie comme suit : si a et b sont dans $\{0,\dots,n-1\}$ alors $a+b$ désigne le reste de la division euclidienne du nombre $a+b$ par n. (Nous verrons avec les groupes quotients une manière plus naturelle de définir $\mathbb{Z}/n\mathbb{Z}$)
2) i) Par exemple, si $n=2$ alors les éléments de $\mathbb{Z}/2\mathbb{Z}$ sont 0 et 1 et on a $0+0=0$, $0+1=1$ et $1+1=0$.
2) ii) Pour $n=3$, $\mathbb{Z}/3\mathbb{Z}$ a 3 éléments 0, 1 et 2 et sa loi respecte entre autres

$$1+1=2,\quad 1+2=0\quad\text{et}\quad 2+2=1.$$

Théorème 1.24 (Lagrange)**.** *Soit G un groupe fini. L'ordre de tout sous-groupe H de G divise l'ordre de G.*

Ce théorème a plusieurs conséquences immédiates. Par exemple, un groupe d'ordre 9 n'a pas de sous-groupe d'ordre 4. Si l'ordre d'un groupe G est un nombre premier alors les seuls sous-groupe de G sont les deux donnés dans la Remarque 1.16.

Démonstration. Pour $a\in G$ on pose $aH := \{a*h \,|\, h\in H\}$. La stratégie de preuve est la suivante. On va montrer trois choses :

i) si a est dans G alors $\mathrm{Card}(aH)=\mathrm{Card}(H)$,
ii) si a et b sont dans G alors $aH=bH$ ou $aH\cap bH=\varnothing$,
iii) $G=\cup_{a\in G} aH$.

On peut déduire de ces trois choses qu'il existe des éléments $a_1,\cdots,a_k$ de G tels que G soit l'union disjointe des a_iH avec $1\leq i\leq k$ et que chacun des a_iH a le même nombre d'éléments que H. Cela implique que $\mathrm{Card}(G)=k\mathrm{Card}(H)$ et donc que l'ordre de H devise l'ordre de G. Il reste donc à démontrer ces trois points.

Pour i), il suffit de remarquer que l'application $h\mapsto a*h$ est une bijection de H vers aH dont la réciproque est $b\mapsto a^{-1}*b$. Puisqu'il existe une bijection entre H et aH, ces deux ensembles ont le même nombre d'éléments.

Pour ii), supposons que $aH\cap bH\neq\varnothing$, c-à-d qu'il existe deux éléments h_1 et h_2 de H tels que $a*h_1=b*h_2$. En particulier, $a=b*h_2*h_1^{-1}$. Donc si $a*h$ est un élément de aH on a $a*h=b*h_2*h_1^{-1}*h$ qui est un élément de bH car H est un sous-groupe donc $h_2*h_1^{-1}*h$ est un élément de H. Ceci montre que $aH\subset bH$. En inversant les rôles de a et b, on obtient $bH\subset aH$ et donc $aH=bH$.

Finalement, pour iii), on sait que l'élément neutre e est dans H donc si $b\in G$ alors $b=b*e\in bH$ ce qui donne $G\subset\cup_{a\in G}aH$. L'inclusion $\cup_{a\in G}aH\subset G$ est évidente car si $a\in G$ et $h\in H$ alors $a*h$ est dans G. □