Université de Strasbourg
MPA Algèbre S1
P. Guillot, bureau 314, guillot@math.unistra.fr

Introduction aux groupes

Définitions & Premiers exemples

Définition. Un *groupe* est un ensemble G, sur lequel on a une opération

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,h) &\mapsto g \star h\,. \end{aligned}$$

On suppose aussi qu'il y a un élément distingué $e \in G$, appelé *l'élément neutre*. Enfin, à tout $g \in G$ on associe un certain élément $\tilde{g} \in G$. On exige que les conditions suivantes soient satisfaites, pour tous les $g, h, k \in G$:

1. $(g \star h) \star k = g \star (h \star k)$ (associativité)
2. $e \star g = g \star e = g$
3. $g \star \tilde{g} = \tilde{g} \star g = e$.

Exemple. Prenons

$$G = \{A \in \mathrm{M}_n(\mathbb{K}) \mid A^{-1} \text{ existe}\}\,.$$

(Ici, et partout ailleurs, $\mathbb{K}$ est un corps (commutatif).) Notre loi sera $A \star B = AB$, le produit usuel des matrices ; l'élément neutre que nous choisissons est $e = I$, la matrice identité ; et enfin on prend $\tilde{A} = A^{-1}$. Les conditions sont évidemment remplies. Donc G, avec ces choix, est un groupe ; on le note en général $GL_n(\mathbb{K})$, où GL est là pour « groupe linéaire ».

Exemple. Soit X un ensemble, et posons

$$G = \{f : X \to X \mid f \text{ est une bijection}\}\,.$$

On prend $f \star g = f \circ g$, la composition ; on prend $e = Id$, la fonction identité, c'est-à-dire $Id(x) = x$; et enfin, $\tilde{f} = f^{-1}$, la réciproque de f, qui est aussi une bijection (et donc est bien dans G). Alors G est un groupe. On le note souvent $S(X)$, le *groupe symétrique de* X. Lorsque $X = \{1, 2, \ldots, n\}$, on note simplement S_n (ou Σ_n, ou $\mathfrak{S}_n$).

Exemple. Prenons $G = \mathbb{Z}$, $n \star m = n + m$ (l'addition usuelle), $e = 0$, et $\tilde{n} = -n$. Alors G est aussi un groupe !

Remarque. Plus généralement, soit A un anneau. Alors on peut construire *deux* groupes. Tout d'abord, comme dans le dernier exemple, on peut prendre A lui-même avec l'addition, le 0, et $\tilde{a} = -a$; on dit parfois que c'est le groupe *additif sous-jacent à* A. Mais on peut aussi considérer

$$A^* = \{a \in A \mid a^{-1} \text{ existe}\}\,.$$

Sur A^* on pose $a \star b = ab$, le produit dans A, puis $e = 1$ (l'unité de A), et enfin $\tilde{a} = a^{-1}$. Ceci nous donne un autre groupe, appelé le *groupe multiplicatif de* A.

Pour $A = \mathrm{M}_n(\mathbb{K})$ on retrouve que $A^* = GL_n(\mathbb{K})$ est un groupe. On note aussi que $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour $+$, et que $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe pour la multiplication.

Définition. Soit G un groupe. On dit que G est *abélien*, ou *commutatif*, lorsque $g \star h = h \star g$ pour tous les $g, h \in G$.

Exemple. Le groupe $\mathbb{Z}$ (pour l'addition) est abélien, ainsi que $\mathbb{Z}/n\mathbb{Z}$ ou $(\mathbb{Z}/n\mathbb{Z})^*$. Mais pour $n \geq 2$, le groupe $GL_n(\mathbb{K})$ n'est pas abélien.

On va simplifier un peu les notations. Nous dirons que le groupe G est « en notation multiplicative » lorsque son opération est notée gh au lieu de $g \star h$, son élément neutre est noté 1, et on écrit g^{-1} au lieu de $\tilde{g}$. Par défaut, les groupes seront tous en notation multiplicative.

Lorsqu'un groupe est abélien, et seulement dans ce cas, on s'autorise parfois à le mettre « en notation additive », c'est-à-dire qu'on écrit $g+h$ pour $g \star h$, on écrit 0 pour l'élément neutre e, et on écrit $-x$ pour $\tilde{x}$ (ainsi que $x - y$ pour $x + (-y)$).

Sous-groupes

Les exemples de groupes seront en général obtenus par les considérations suivantes.

Définition. Soit G un groupe (en notation multiplicative), et soit $H \subset G$. On dit que H est un *sous-groupe* de G lorsque

1. $1 \in H$;
2. si $g \in H$ et $h \in H$, alors $gh \in H$;
3. si $g \in H$, alors $g^{-1} \in H$.

Remarque. Une observation évidente, mais fondamentale : si H est un sous-groupe de G, alors H est lui-même un groupe !

Exemple. Soit $n \geq 1$, et posons

$$\mu_n = \mu_n(\mathbb{C}) = \{z \in \mathbb{C}^* \mid z^n = 1\}.$$

Alors μ_n est un sous-groupe de $\mathbb{C}^*$. En effet, si $z^n = w^n = 1$, alors $(zw)^n = z^n w^n = 1$, et $(z^{-1})^n = (1/z)^n = 1/z^n = 1$. Et bien sûr $1 \in \mu_n$.

Exemple. Soit

$$T = \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \mid a, b, c \in \mathbb{R},\ ab \neq 0 \right\}.$$

Vérifions que T est un sous-groupe de $GL_2(\mathbb{R})$; on note déjà que $T \subset GL_2(\mathbb{R})$, car ab est le déterminant de la matrice proposée. On calcule donc

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \begin{pmatrix} a' & c' \\ 0 & b' \end{pmatrix} = \begin{pmatrix} aa' & ac' + cb' \\ 0 & bb' \end{pmatrix} \in T$$

et

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}^{-1} = \frac{1}{ab} \begin{pmatrix} b & -cc \\ 0 & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & -\frac{c}{ab} \\ 0 & \frac{1}{b} \end{pmatrix} \in T,$$

et la dernière vérification est évidente.

Définition. Soit G un groupe en notation multiplicative, soit $g \in G$, et soit $n \in \mathbb{N}^*$. On note g^n pour $gg \cdots g$, répété n fois ; pour $n \in \mathbb{Z}$, mais $n < 0$, on définit $g^n = g^{-1}g^{-1} \cdots g^{-1}$, répété $-n$ fois ; et on pose $g^0 = 1$. Les règles de calcul usuelles s'appliquent sans aucune surprise (on le vérifie), comme $g^n g^m = g^{n+m}$, et $(g^n)^{-1} = g^{-n}$.

Si G est en notation additive, on définit de même ng pour $n \in \mathbb{Z}$. En particulier $0g = 0$.

Définition. Soit G un groupe et $g \in G$. Le *sous-groupe cyclique engendré par* g, par définition, est

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}\,.$$

Si G est en notation additive, on a

$$\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}\,.$$

Pour justifier ce nom, il faut vérifier que $\langle g \rangle$ est bien un sous-groupe de G ! Mais c'est assez évident, ça provient des identités $g^n g^m = g^{n+m}$ etc. Ajoutons une autre définition :

Définition. On dit que le groupe G est *cyclique* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Exemple. Le groupe $\mathbb{Z}$ est cyclique, puisque $\mathbb{Z} = \langle 1 \rangle$. De même $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ est cyclique. (Attention, dans les deux cas, l'élément neutre est 0.) Nous verrons plus loin que tous les groupes cycliques sont « modelés » sur ceux-ci. Pour un exemple en notation multiplicative, considérer μ_n, le groupes des racines n-ièmes dans $\mathbb{C}$: il est cyclique, puisque $\mu_n = \langle \exp(\frac{2i\pi}{n}) \rangle$.

Exemple. Soit G un groupe ne comportant que deux éléments. Montrons que G est cyclique. En effet, appelons g l'unique élément de G tel que $g \neq 1$. Alors $G = \{g^0 = 1, g\} = \langle g \rangle$.

Exemple. Un groupe cyclique est toujours abélien. Donc $GL_2(\mathbb{K})$ n'est pas cyclique, par exemple.

Définition. Si G est un groupe fini, alors le nombre d'éléments de G est appelé *l'ordre* de G, noté $|G|$. Si G n'est pas fini, on dit parfois que son ordre est ∞. Si $g \in G$, où G est un groupe quelconque, alors l'ordre du groupe $\langle g \rangle$ est appelé *l'ordre de* g (ça peut donc être ∞).

Lemme 1. *Soit $g \in G$. L'ordre de g est le plus petit entier $k > 0$ tel que $g^k = 1$, ou alors ∞ s'il n'en existe pas. On a alors*

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{k-1}\}\,.$$

Enfin, si $n, m \in \mathbb{Z}$, alors

$$g^n = g^m \iff n \equiv m \bmod k\,.$$

En particulier, on voit que $g^n = 1 \Leftrightarrow k$ divise n.

Démonstration. Soit $H = \langle g \rangle$. Supposons d'abord que H est fini, c'est-à-dire que l'ordre de g est fini. Alors les éléments g^i, pour $i \in \mathbb{N}$, ne sont pas tous différents. Soient donc $i < j$ deux entiers tels que $g^i = g^j$. On en déduit $1 = g^{j-i}$, donc il existe des entiers $k > 0$ tels que $g^k = 1$ (par exemple $k = j - i$). Par contraposée, on obtient que, si des entiers tels que k n'existent pas, alors l'ordre de g est ∞.

On suppose donc qu'il existe de tels entiers, et on appelle k le plus petit d'entre eux. Les éléments $1, g, g^2, \ldots, g^{k-1}$ sont tous différents, car $g^i = g^j$ avec $i < j < k$ entraînerait $g^{j-i} = 1$, mais $j - i < k$, c'est absurde. Par ailleurs, prenons $n \in \mathbb{Z}$ et écrivons la division euclidienne $n = kq + r$ avec $0 \leq r < k$. On a alors $g^n = g^{kq+r} = (g^k)^q g^r = 1^q g^r = g^r$. Donc $g^n \in \{1, g, \ldots, g^{k-1}\}$.

Finalement $H = \{1, g, \ldots, g^{k-1}\}$. Il comporte donc k éléments, ce qui montre que l'ordre de g est fini, et même que cet ordre est k. Par ailleurs, on a constaté que g^n ne dépend que de $\bar{n} = r \in \mathbb{Z}/k\mathbb{Z}$, donc le reste est clair. □

Exercices 1 et 2.

Lagrange et Fermat

Théorème 2 (Lagrange)**.** *Soit G un groupe fini, et soit H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.*

Démonstration. On définit une relation sur G par $x \sim y \Leftrightarrow y = xh$ pour un $h \in H$ (il revient au même de demander que $x^{-1}y \in H$). On vérifie sans peine que c'est une relation d'équivalence.

La classe d'équivalence de x est $[x] = \{xh \mid h \in H\}$, par définition. Cet ensemble est en bijection avec H : en effet on peut définir une fonction $H \to [x]$ par $h \mapsto xh$, et une autre $[x] \to H$ par $y \mapsto x^{-1}y$. Ceci a un sens, car $y \in [x]$ est de la forme $y = xh$, donc $x^{-1}y = h \in H$. Ces deux fonctions sont des bijections réciproques l'une de l'autre, puisque $x^{-1}(xh) = h$ et $x(x^{-1}y) = y$.

Donc chaque classe d'équivalence est de taille $|H|$, l'ordre de H. Puisque G est l'union disjointe de (disons) k classes d'équivalence, on a $|G| = k|H|$. □

Corollaire 3. *Si $g \in G$, alors l'ordre de g divise l'ordre de G. En particulier, on a $g^{|G|} = 1$.*

Démonstration. Le théorème de Lagrange appliqué à $H = \langle g \rangle$ donne la première phrase. Si k est l'ordre de g, on a donc $|G| = kd$, donc $g^{|G|} = (g^k)^d = 1^d = 1$. □

Corollaire 4 (Petit théorème de Fermat)**.** *Soit p un nombre premier, et $x \in \mathbb{Z}$. Alors $x^p \equiv x$ mod p. Si p ne divise pas x, alors $x^{p-1} \equiv 1$ mod p.*

Démonstration. On prend $G = (\mathbb{Z}/p\mathbb{Z})^*$, qui est d'ordre $p - 1$. Si x n'est pas divisible par p, alors $\bar{x} \in G$, et donc $\bar{x}^{p-1} = \bar{1}$ par le corollaire précédent, ce qui s'écrit $x^{p-1} \equiv 1$ mod p. On obtient $x^p \equiv x$ mod p en multipliant par x.

Si par contre p divise x, alors $x \equiv 0$ mod p, donc certainement $x^p \equiv 0 \equiv x$ mod p. □

Exercices 3, 4, 5.

Sous-groupes des groupes cycliques

Commençons par les sous-groupes de $\mathbb{Z}$:

Théorème 5. *Soit H un sous-groupe de $\mathbb{Z}$ (avec l'addition). Alors il existe un entier $n \geq 0$ tel que*

$$H = n\mathbb{Z} := \langle n \rangle = \{xn \mid x \in \mathbb{Z}\} = \{\text{les multiples de } n\}\,.$$

Démonstration. Si $H = \{0\}$, le résultat est vrai pour $n = 0$. Sinon, il existe $x \in H$ avec $x \neq 0$, et $-x \in H$ car H est un sous-groupe, donc le nombre $|x| \in H$, et $|x| > 0$. On peut donc poser

$$n = \min\{x \in H \mid x > 0\}\,.$$

(L'ensemble étant non-vide.) Montrons que $H = n\mathbb{Z}$. En effet, pour tout $x \in H$, faisons la division $x = nq + r$ avec $0 \leq r < n$. Puisque $n \in H$, on a $qn \in H$, et $x - qn \in H$, car H est un sous-groupe. Donc $r \in H$. Mais $0 < r < n$ est impossible par minimalité de n, donc $r = 0$. Ainsi $x = qn$, et x est un multiple de n.

Ceci montre $H \subset n\mathbb{Z}$, mais bien sûr $n\mathbb{Z} = \langle n \rangle \subset H$, donc finalement $H = n\mathbb{Z}$. □

Voyons maintenant les sous-groupes d'un groupe cyclique fini d'ordre n. Par Lagrange, l'ordre d'un tel sous-groupe doit diviser n.

Théorème 6. *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n (en notation multiplicative). Soit d un diviseur de n, et écrivons $n = de$. Alors G possède un unique sous-groupe H_d d'ordre d, et de plus*

$$H_d = \langle g^e \rangle = \{x \in G \mid x^d = 1\}\,.$$

Démonstration. Commençons par montrer que

$$\langle g^e \rangle = \{x \in G \mid x^d = 1\}\,.$$

En effet, un $x \in G$ peut s'écrire $x = g^k$, par définition. Alors $x^d = g^{kd}$, de sorte que $x^d = 1$ équivaut à $g^{kd} = 1$, c'est-à-dire à $n|kd$. Mais $de|dk$ si et seulement si $e|k$; et si $k = e\ell$, alors $g^k = (g^e)^\ell$, et $x \in \langle g^e \rangle$. Finalement, on constate que $x^d = 1$ équivaut à $x \in \langle g^e \rangle$, d'où l'égalité. On note H_d pour le groupe en question.

Le groupe H_d est cyclique, engendré par g^e, donc son ordre est le plus petit entier k tel que $(g^e)^k = 1$ (lemme précédent). Mais $g^{ek} = 1$ si et seulement si $n|ek$, donc $d|k$. L'entier k est un multiple de d, donc $k \geq d$; mais $(g^e)^d = g^n = 1$ par Lagrange, donc par minimalité on a $k = d$. On a montré que H_d est d'ordre d.

Montrons enfin l'unicité. Soit H un sous-groupe de G d'ordre d. Alors pour tout $x \in H$, on a $x^d = 1$ par Lagrange ; ceci montre $H \subset H_d$, et par égalité des ordres, $H = H_d$. □

Dans les exercices, on verra une deuxième démonstration de ce théorème, qui s'appuie sur le précédent.

Exercice 6

Homomorphismes

Définition. Soit G_1 un groupe, avec élément neutre e_1 et opération notée $\star$, et soit G_2 un autre groupe, avec élément neutre e_2 et opération notée $\bullet$. Un *homomorphisme de groupes* entre G_1 et G_2 est une fonction $\phi\colon G_1 \to G_2$ telle que

$$\phi(g \star h) = \phi(g) \bullet \phi(h)\,,$$

pour tous les g, h. Si les deux groupes sont en notation multiplicative, cette condition s'écrit

$$\phi(gh) = \phi(g)\phi(h)\,.$$

Si, par exemple, G_1 est en notation additive, et G_2 en multiplicative, la condition est

$$\phi(g + h) = \phi(g)\phi(h)\,.$$

Remarque. Lorsque ϕ est un homomorphisme, on a automatiquement $\phi(e_1) = e_2$. En effet, $e_1^2 = e_1$, donc $\phi(e_1^2) = \phi(e_1)^2 = \phi(e_1)$, ce qui s'écrit $x^2 = x$ en posant $x = \phi(e_1)$. En multipliant par x^{-1} on obtient $x^{-1}x^2 = x = x^{-1}x = e_2$. Mais de toute façon, dans tous les exemples, la propriété $\phi(e_1) = e_2$ est toujours évidente. On vous laisse montrer, de la même façon, que l'on a toujours $\phi(x^{-1}) = \phi(x)^{-1}$ automatiquement.

Exemple. On considère $\mathbb{R}$, qui est un groupe pour l'addition, et $\mathbb{R}^\times$ qui est un groupe pour la multiplication. Alors l'exponentielle est un homomorphisme $\mathbb{R} \to \mathbb{R}^\times$. Son image est le sous-groupe $\mathbb{R}^{>0}$. Le logarithme est un homomorphisme $\mathbb{R}^{>0} \to \mathbb{R}$.

Exemple. Reprenons le groupe

$$T = \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \mid a, b, c \in \mathbb{R},\ ab \neq 0 \right\} \subset GL_2(\mathbb{R})\,.$$

Alors on a un homomorphisme $T \to \mathbb{R}^*$ défini par

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \mapsto a \qquad (\text{ou } b)\,.$$

Exemple. L'application

$$\det\colon GL_2(\mathbb{K}) \longrightarrow \mathbb{K}^*$$

est un homomorphisme : $\det(AB) = \det(A)\det(B)$.

Exemple. Soit G un groupe quelconque, et $g \in G$. Alors on a toujours un homomorphisme

$$\begin{aligned} \phi_g\colon \mathbb{Z} &\longrightarrow G \\ n &\mapsto g^n\,. \end{aligned}$$

(En effet $\phi_g(n+m) = g^{n+m} = g^n g^m = \phi(n)\phi(m)$.) Nous l'appellerons simplement « l'homomorphisme défini par le choix de $g \in G$ ».

Définition. Un *isomorphisme* entre G_1 et G_2 est un homomorphisme $G_1 \to G_2$ qui est aussi une bijection. Lorsqu'il existe au moins un tel isomorphisme, on dit que G_1 et G_2 sont *isomorphes*, et on note $G_1 \cong G_2$.

Lemme 7. *Si $\phi\colon G_1 \to G_2$ est un isomorphisme, alors la bijection réciproque $\phi^{-1}\colon G_2 \to G_1$ est aussi un isomorphisme.*

Démonstration. Soient $x, y \in G_2$. Soient $g, h \in G_1$ tels que $\phi(g) = x$ et $\phi(h) = y$; en d'autres termes, soient $g = \phi^{-1}(x)$, et $h = \phi^{-1}(y)$. Alors $\phi^{-1}(xy) = \phi^{-1}(\phi(g)\phi(h)) = \phi^{-1}(\phi(gh)) = gh$, en utilisant que ϕ est un homomorphisme. Donc $\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y)$, ce qui montre bien que ϕ^{-1} est un homomorphisme (et donc un isomorphisme puisque c'est une bijection). □

Pour illustrer la notion d'isomorphisme, nous allons montrer la chose suivante :

Proposition 8. *Soit $G = \langle g \rangle$ un groupe cyclique. Alors G est soit isomorphe à $\mathbb{Z}$, soit isomorphe à $\mathbb{Z}/k\mathbb{Z}$ pour un certain $k \geq 1$.*

Démonstration. On considère l'homomorphisme $\mathbb{Z} \to G$ défini par g. Envisageons d'abord le cas où ϕ_g est injective. Elle est surjective par définition (G étant cyclique), donc c'est un isomorphisme, et $G \cong \mathbb{Z}$.

Supposons donc que ϕ_g n'est pas injective. On retrouve un argument connu : il existe $i < j$ avec $\phi_g(i) = g^i = \phi_g(j) = g^j$, donc $g^{j-i} = 1$, avec $j - i > 0$. Par un lemme précédent, l'ordre de g est fini ; appelons-le k. Définissons alors $\psi\colon \mathbb{Z}/k\mathbb{Z} \to G$ par $\psi(n) = g^n$. Le même lemme que précédemment montre que ψ est une bijection. Il faut tout de même vérifier que c'est un homomorphisme.

Écrivons $\oplus$ pour l'addition de $\mathbb{Z}/k\mathbb{Z}$, c'est-à-dire $n \oplus m =$ le reste dans la division de $n + m$ par k. On a $n \oplus m \equiv n + m \bmod k$ par définition. Par ailleurs, $\psi(n)\psi(m) = g^n g^m = g^{n+m}$. Mais le fameux lemme (toujours le même !) nous dit que $g^x = g^y$ si $x \equiv y \bmod k$, donc $g^{n+m} = g^{n \oplus m} = \psi(n \oplus m)$. On a bien prouvé que ψ est un isomorphisme. □

Exercices 7, 8, 9.