# MATHF-203 – Algèbre I

R. Petit

Année académique 2016 - 2017

## Table des matières

# 1 Les groupes

## 1.1 Définitions

**Définition 1.1.** Un *groupe* $(G, *)$ est un ensemble non-vide G muni d'une loi de composition $* : G \times G \to G$ tels que :
- $*$ est associative ;
- G possède un élément neutre noté $e \in G$ ;
- chaque élément $g$ de G possède un inverse noté $g^{-1}$.

**Définition 1.2.** Un ensemble non-vide M muni d'une loi de composition $* : M \times M \to M$ associative telle que M admet un neutre par $*$ est appelé un *monoïde*.

**Définition 1.3.** Un monoïde $(M, *)$ est dit *abélien* (ou *commutatif*) lorsque $*$ est commutative.

*Remarque.* Un groupe est un monoïde admettant un inverse pour chaque élément. Dès lors, les résultats et définitions sur les monoïdes s'appliquent également aux groupes.

**Proposition 1.4.** *Dans un groupe* $(G, *)$*, les équations :*

$$x * a = b, \tag{1}$$

*et :*

$$a * y = b \tag{2}$$

*admettent une unique solution, i.e. :*

$$(x, y) = (b * a^{-1}, a^{-1} * b) \in G^2.$$

*Démonstration.* G est un groupe, du coup $a$ et $b$ admettent un inverse. L'existence de la solution est donc triviale.

Soit $x$, solution de (1). On a alors :

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

Similairement pour $y$, solution de (2), on a :

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

□

**Proposition 1.5.** *Le neutre d'un groupe est unique, et l'inverse de tout élément l'est également.*

*De plus :*

$$\forall a, b, c, d \in G : \begin{cases} c * a = d * a \Rightarrow c = d, \\ a * c = a * d \Rightarrow c = d. \end{cases}$$

*Démonstration.* EXERCICE. □

**Proposition 1.6.** *Si* G *est un ensemble non-vide muni d'une loi de composition* $*$ *associative telle que* (1) *et* (2) *admettent une unique solution, alors* $(G, *)$ *est un groupe.*

*Démonstration.* Pour chaque élément $a \in G$, prenons $e_a^L$ tel que $e_a^L * a = a$ et $e_a^R$ tel que $a * e_a^R = a$. Ces deux équations admettent une unique solution par hypothèse. On trouve alors :

$$e_a^L * a = a = a * e_a^R,$$

d'où l'on déduit :

$$a * e_a^L * a = a * a = a * e_a^R * a,$$

et donc $e_a^L = e_a^R$ en multipliant à gauche et à droite par $a^{-1}$. On en déduit l'unicité d'un neutre pour $a$ et notons-le $e_a$. Montrons que ce neutre l'est pour tous les éléments de G. Prenons $(a, b) \in G^2$ et leur neutre respectif $e_a$ et $e_b$. On peut écrire :

$$a * e_b * b = a * b = a * e_a * b,$$

d'où l'on déduit $e_a = e_b$ en multipliant à gauche par $a^{-1}$ et à droite par $b^{-1}$. □

**Définition 1.7.** Si $|G| < \infty$, on peut définir la *table de multiplication* de $(G, *)$ par un tableau de dimensions $|G| \times |G|$ reprenant tous les résultats de $g * h$ pour $g, h \in G$.

## 1.2 Groupes de transformation

**Définition 1.8.** Soit S un ensemble non-vide. Soit G l'ensemble des bijections de S dans S. On définit la loi de composition :

$$\circ : G \times G \to G : (\psi, \varphi) \mapsto (\psi \circ \varphi),$$

tels que $\forall s \in S : (\psi \circ \varphi)(s) = \psi(\varphi(s))$.

**Proposition 1.9.** $(G, \circ)$ *est un groupe (de permutation sur S).*

*Démonstration.* Le neutre est donné par $Id \in G$ où $\forall s \in S : Id(s) = s$. La loi $\circ$ est trivialement associative, et l'inverse d'une fonction est bien définie sur les bijections. □

*Exemple* 1.1. L'ensemble $SO(3, \mathbb{R})$ des rotations axiales passant par $\mathcal{O}$ forme un groupe de transformations.
*Remarque.* Un groupe de transformation est composé de fonctions bijectives. L'ensemble G est donc un ensemble fonctionnel.

## 1.3 Sous-groupes

**Définition 1.10.** Soit $(G, *)$ un groupe, et soit $S \subset G$. Si $(S, *)$ est un groupe, alors on dit que $(S, *)$ est un *sous-groupe* de $(G, *)$.

**Proposition 1.11.** *Soit* $(G, *)$ *un groupe.* $S \subseteq G$ *est un sous-groupe de* G *si et seulement si :*

$$\forall a, b \in S : a * b^{-1} \in S.$$

*Démonstration.* $\boxed{\Rightarrow}$ Trivial car S est un groupe.

$\boxed{\Leftarrow}$ S est non-vide, donc $e \in S$ car si $a \in S$, alors par hypothèse $e = a * a^{-1} \in S$. De même, soit $a \in S$. On sait que $a^{-1} = e * a^{-1} \in S$. Et S est stable par $*$ car si $a, b \in S$, on sait que $b^{-1} \in S$, et donc $a * \left(b^{-1}\right)^{-1} \in S$. □

**Proposition 1.12.** *Si* $\{S_\alpha$ *t.q.* $\alpha \in I\}$ *est une famille de sous-groupes de* $(G, *)$*, alors* $S \coloneqq \bigcap_{\alpha \in I} S_\alpha$ *est un sous-groupe de* $(G, *)$ *également.*

*Démonstration.* On sait que $e \in S$ car $e \in S_\alpha$ pour tout $\alpha \in I$. Donc $S \neq \emptyset$. Prenons $a, b \in S$. On sait que $a, b \in S_\alpha$ pour tout $\alpha \in I$. Donc $b^{-1}$ et $a * b^{-1}$ sont dans $S_\alpha$ pour tout $\alpha \in I$ également. Donc $a * b^{-1} \in S$. □

**Définition 1.13.** Soit $(G, *)$ un groupe et soit $P \subseteq G$. On appelle le *sous-groupe de* $G$ *engendré par* $P$ le plus petit sous-groupe de $G$ contenant $P$. On le note $\langle P \rangle$

**Définition 1.14.** Soit $(G, *)$ un groupe et soit $g \in G$. On appelle *ordre de* $g$ le plus petit $n \in \mathbb{N}^*$ tel que $g^n = e$. On le note $\text{ord}(e)$.

L'ordre de $(G, *)$ est$|G|$.

**Définition 1.15.** Un groupe $(G, *)$ est dit *cyclique* lorsqu'il existe $g \in G$ tel que $G = \langle g \rangle \coloneqq \langle \{g\} \rangle$.

## 1.4 Isomorphismes

**Définition 1.16.** Un *isomorphisme* entre deux groupes $(G, *)$ et $(H, \star)$ est une bijection $\phi : G \to H$ telle que :

$$\forall g_1, g_2 \in G : \phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2).$$

*Remarque.* La relation « *être isomorphe* » dans l'ensemble des groupes est une relation d'équivalence.

De plus, sis $G$ et $H$ sont deux groupes finis, $\phi : G \to H$ est un isomorphisme si et seulement si $\phi$ est bijective, et la table de multiplication de $H$ par $\phi(G)$ est l'image de la table de multiplication de $G$ par $G$.

**Proposition 1.17.** *Soit* $\phi : (G, *) \to (H, \star)$ *un isomorphisme de groupes. Alors :*
- $\phi(e_G) = e_H$ ;
- $\forall g \in G : \phi(g)^1 = \phi(g^{-1})$.

*Démonstration.* On sait que $\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \star \phi(e_G)$. Dès lors, il est évident que $\phi(e_G)$ est le neutre de $H$.

Soit $g \in G$. On sait également que $e_H = \phi(e_G) = \phi(g * g^{-1}) = \phi(g) \star \phi(g^{-1})$. On a donc bien, en multipliant par $\phi(g)^{-1}$ à gauche que $\phi(g)^{-1} = \phi(g^{-1})$. □

**Théorème 1.18.** *Tout groupe est isomorphe à un groupe de transformation.*

*Démonstration.* Soit $(G, *)$ un groupe, et soit $g \in G$. On définit $\phi : G \to \{\ell_g$ t.q. $g \in G\}$, où $\ell_g : G \to G : h \mapsto g * h$.

Pour $g \in G$, montrons que $\ell_g$ est bijective :
- il est évident que $\forall g, h, h' \in G : g * h = g * h' \iff h = h'$ par les règles de simplification ;
- $\forall h \in G : \ell_g(g^{-1} * h) = g * g^{-1} * h = h$.

On a donc que $\ell_g$ est bien bijective pour tout $g \in G$.

Montrons maintenant que $\phi : g \mapsto \ell_g$ est un isomorphisme de groupes :
- $\phi$ est surjective par définition.
- soient $g, h \in G$. $\ell_g = \ell_h$ si et seulement si pour tout $\gamma \in G$, on a $g * \gamma = h * \gamma$, et donc si et seulement si on a $g = h$. $\phi$ est donc injective.
- Soient $g, h, \gamma \in G$. $\phi(g * h)(\gamma) = g * h * \gamma = g * \ell_h(\gamma) = (\ell_g \circ \ell_h)(\gamma)$.

□

**Théorème 1.19.** *Tout groupe cyclique est déterminé, à isomorphisme près, par l'ordre d'un élément* $g$ *qui l'engendre.*

*Plus précisément, si* $(G, *)$ *est un groupe engendré par un élément* $g$ *d'ordre* $\mathrm{ord}(g)$ *fini, alors* $G \cong (\mathbb{Z}_{\mathrm{ord}(g)}, +)$ *; et si* $g$ *est d'ordre infini, alors* $(G, *) \cong (\mathbb{Z}, +)$.

*Démonstration.* S'il existe $g \in G$ tel que $G = \langle g \rangle$ et $\mathrm{ord}(g) \lneqq +\infty$, alors $G = \{e, g, \dots, g^{\mathrm{ord}(g)-1}\}$.

Soit $\phi : \mathbb{Z}_{\mathrm{ord}(g)} \to G : k \mapsto g^k$. $\phi$ est trivialement bijective, et on observe :

$$\phi(k + l) = g^{k+l} = g^k * g^l = \phi(k) * \phi(l).$$

Supposons maintenant qu'il existe $g \in G$ tel que $\mathrm{ord}(g) = +\infty$ et $\langle g \rangle = G$. On pose :

$$\forall p \in \mathbb{N}^* : g^{-p} \coloneqq g^{-1} * g^{1-p}.$$

Puisque $\mathrm{ord}(g) = +\infty$, si $g^x = g^y$ pour $x, y \in \mathbb{Z}$, alors $x = y$. En reprenant le même $\phi$ étendu à $\mathbb{Z}$, on a bien, à nouveau, un isomorphisme de groupes. □

**Corollaire 1.20.** *Tout groupe cyclique est commutatif.*

*Démonstration.* Étant isomorphe à $\mathbb{Z}_n$ pour un certain $n \in \mathbb{N}$ ou à $\mathbb{Z}$, par passage à l'isomorphisme, la propriété d'additivité est conservée. □

**Proposition 1.21.** *Si* $(G, *)$ *est un groupe cyclique, tout sous-groupe* $S$ *de* $G$ *est cyclique.*

*Démonstration.* Prenons $a \in G$ tel que $G = \langle a \rangle$. Posons $N \coloneqq \{n \in \mathbb{Z} \text{ t.q. } a^n \in S\}$. Dans le cas fini, prenons $\underline{n}$, le plus petit entier positif de $N$. Supposons par l'absurde que $a^t \in S$ ne soit pas une puissance entière de $a^{\underline{n}}$. Par Euclide, on a :

$$\exists (q, r) \in \mathbb{Z} \times \mathbb{N} \text{ t.q. } t = q\underline{n} + r,$$

et donc :

$$a^t = a^{q\underline{n}} * a^r,$$

avec $0 \lneqq r \lneqq \underline{n}$. On sait que $a^t \in S$, et $a^{q\underline{n}} \in S$ (donc $a^{-q\underline{n}} \in S$). Dès lors, $a^r \in S$. Or $\underline{n}$ est le plus petit entier positif tel que $a^{\underline{n}} \in S$. Il y a donc contradiction, et $a^t$ est une puissance entière de $a^{\underline{n}}$. Dès lors, $S = \langle a^{\underline{n}} \rangle$. □

## 1.5 Classes latérales et théorème de Lagrange