Algèbre et géométrie 1

Patrick Le Meur et Pierre Gervais

September 26, 2016

Contents

Part I
Groupes

1 Définitions et premiers exemples

Définition 1. Un *groupe* est un couple $(G, *)$ où

- G est un ensemble

- $* \ : \left\{ \begin{array}{lll} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & g*h \end{array} \right.$ est une loi de composition interne associative admettant un élément neutre e, c'est à dire tel que $\forall g \in G, g*e = e*g = g$

- tout élément g admet un symétrique pour $*$ noté g^{-1} tel que $g*g^{-1} = g^{-1}*g = e$

Remarque 1.

- L'élément neutre et le symétrique d'un élément donné est unique.

- Pour tout $g, h \in G$ on a $(g*h^{-1}) = h^{-1}*g^{-1}$

- Si on a $gh = e$, alors $g = h^{-1}$

- Soit $g \in G$ et $n > 0$, on définit $g^n = \underbrace{g*g*g...g}_{n \text{ fois}}$, $g^0 = e$, $g^{n+1} = g*g^n$ et $g^{-n} = \left(g^{-1}\right)^n$

Exercice 1. Montrer que pour tout $m, n \in \mathbb{Z}$ on a $g^{m+n} = g^m * g^n$ et $g^{-n} = \left(g^{-1}\right)^n$

Exemple 1.

1. $G = \mathbb{Z}, * = +$

2. Soit E un espace vectoriel, $(E, +)$

3. $(\mathbb{C}^*, \times)$ et $(\mathbb{C}, +)$

4. Si $\mathbb{K}$ est un corps, $(\mathbb{K}, *)$

   Ces exemples sont des groupes abéliens (c'est à dire commutatifs), les suivants n'en sont pas.

5. Soit $(G, \cdot)$ un groupe fini, on définit $\otimes \ : \left\{ \begin{array}{lll} \mathbb{Z}^G \times \mathbb{Z}^G & \longrightarrow & \mathbb{Z}^G \\ (f_1, f_2) & \longmapsto & \left(g \longmapsto \displaystyle\sum_{h \in G} f_1(h) f_2(h^{-1} * g) \right) \end{array} \right.$

   Exercice 2. Montrer que $\mathbb{Z}^G$ muni de cette opération n'est pas un groupe mais que $\otimes$ est une loi associative.

6. $GL_n(\mathbb{R})$ muni de la multiplication de matrices.

Proposition 1. *Soit E un ensemble non-vide, on note $\mathfrak{S}(E)$ l'ensemble des applications bijectives de E dans E et $(\mathfrak{S}(E), \circ)$ est un groupe.*

2 Sous-groupe

Définition 2. Soit $(G, *)$ un groupe, on appelle *sous-groupe* de G toute partie $H \subseteq G$ munie de $*$ telle que $e \in H$, $\forall (h_1, h_2) \in H^2, h_1 * h_2 \in H$ et $\forall h \in H, h^{-1} \in H$. On note $H \leqslant G$

Exemple 2. 1. Si $(G, *)$ est un groupe alors $\{e\} \leqslant G$

2. On définit $SL_n(\mathbb{R}) = \{M \in \mathcal{M}_n | \det M = 1\}$ le *groupe spécial linéaire* qui est un sous-groupe de $GL_n(\mathbb{R})$

3. On définit $\mathcal{O}_n(\mathbb{R}) = \{M \in \mathcal{M}_n | {}^tMM = I_n\}$ le *groupe orthogonal* qui est un sous-groupe de $GL_n(\mathbb{R})$

4. $\mathfrak{U} = \{z \in \mathbb{C} \mid |z| = 1\} \leqslant (\mathbb{C}^*, \times)$

5. Pour $n > 0$, $\mathfrak{U}_n = \{z \in \mathbb{C}^* \mid z^n = 1\} \leqslant \mathfrak{U} \leqslant \mathbb{C}^*$

Proposition 2.

1. *Soit $n \in \mathbb{Z}$, $n\mathbb{Z} \leqslant \mathbb{Z}$*

2. *Tout sous-groupe de $\mathbb{Z}$ est de cette forme*

Preuve 1.

1. $n\mathbb{Z} \subseteq \mathbb{Z}$, $0 \in \mathbb{Z}$, $xn + yn = (x+y)n \in n\mathbb{Z}$ et $-(xn) \in n\mathbb{Z}$

2. Soit $H \leqslant \mathbb{Z}$, si $H = \{0\}$ ✓
   Soit $n = min\{h \in H \mid h > 0\}$ (il existe par la propriété de la borne supérieure), montrons $H = n\mathbb{Z}$
   $\boldsymbol{nZ \subseteq H}$ ✓
   $\boldsymbol{nZ \subset H}$
   Soit $h \in H$, on considère sa division euclidienne par n : $h = nq + r$ avec $0 \leqslant r < n$. $h - nq = r \in H$, et n est le plus petit élément non-nul, donc $r = 0$. ✓

□

Lemme 1. *Soit G un groupe et $(H_i)_i \in I$ une famille de sous-groupes de G, alors $\bigcap_{i \in I} H_i \leqslant G$*

Définition 3. Soit G un groupe et A une partie de G, l'intersection des sous-groupes de G contenant A est appelée *sous-groupe engendré par* A et notée $\langle A \rangle$.

Propriété 1.

- *$A \subseteq \langle A \rangle \leqslant G$*

- *Si H est un sous-groupe contenant A, alors $\langle A \rangle \subseteq H$*

Exercice 3. Montrer que $\langle A \rangle$ est l'unique sous-groupe vérifiant ces propriétés.

Propriété 2. *Soit G un groupe et $g \in G$, $\langle \{g\} \rangle = \langle g \rangle = \{g^n, n \in \mathbb{Z}\}$*

Exercice 4. Le démontrer.

Propriété 3. *Soit A une partie de G, $\langle A \rangle$ est l'ensemble des éléments de la forme $a_1^{n_1} * a_2^{n_2} * ... * a_p^{n_p}$ où $a_i \in A$ et $n_i \in \mathbb{Z}$.*

Preuve 2. On pose K l'ensemble des éléments de cette forme. Montrons

1. $A \subseteq K$ et $K \leqslant G$

2. Pour tout $H \leqslant G$ tel que $A \subseteq H$ on a $K \subseteq H$

Exemple 3. 1. Soient k et n deux entiers relatifs, $\langle k, n \rangle = k\mathbb{Z} + n\mathbb{Z} = (k \wedge n)\mathbb{Z}$ d'après l'identité de Bézout.

2. Soit $n > 0$, si $M \in \mathcal{O}_n(\mathbb{R})$, alors il existe $P \in \mathcal{O}_n(\mathbb{R})$ et $r, s \in \mathbb{N}$, $\theta_1, ...\theta_p \in \mathbb{R}$ tels que $P^{-1}MP$ soit diagonale par blocs :

$$\begin{pmatrix} I_r & & & & \\ & -I_s & & & \\ & & R(\theta_1) & & \\ & & & \ddots & \\ & & & & R(\theta_p) \end{pmatrix}$$

Exercice 5. Montrer que $\mathcal{O}_n(\mathcal{R})$ est engendré par les réflexions, c'est à dire les matrices de orthogonales semblables à $\begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$ en base orthonormée.

3 Ordre d'un élément dans un groupe

Soit $g \in G$, on suppose qu'il existe $n > 0$ tel que $g^n = e$. On a alors $\langle g \rangle = \{e, g, g^2, g^3, ..., g^{n-1}\}$, en effet pour tout $k > 0$, de division euclidienne $k = nq + r$ avec $0 \leqslant r < n$, on a $g^k = g^{nq+r} = e^q g^r = g^r$ d'où $g^r \in \{e, g, g^2, ..., g^{n-1}\}$.

Définition 4. Soit $g \in G$, on définit *l'ordre* de g par $d = \min\{k > 0 \mid g^k = e\}$, on a ainsi que $e, g, g^2, ..., g^d$ sont deux à deux distincts. On en conclut que $\langle g \rangle = \{g^k \mid 0 \leqslant k < d\}$ est de cardinal d.

En effet $0 \leqslant k \leqslant l < d$, on a $g^l = g^k \Longrightarrow g^{l-k} = e$.
Or $0 \leqslant l - k < d$ et par minimalité de d, $l = k$.

Exemple 4.

1. Dans $(\mathfrak{U}, \times)$, pour $n > 0$ on a $g = \exp\left(\frac{2i\pi}{n}\right)$
   g est d'ordre fini égal à n.
2. Dans $GL_n(\mathbb{R})$ $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ est d'ordre 2 et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ d'ordre 4.

Théorème 1. *Soit G un groupe fini et $H \leqslant G$, alors $|H|$ divise $|G|$.*

Corollaire 1. *Soit g un élément d'un groupe fini, g est d'ordre fini divisant $|G|$.*

Exemple 5. Dans $\mathfrak{U}_6$, d'ordre 6, les éléments peuvent avoir pour ordre 1, 2, 3 et 6.

Propriété 4. *$d > 0$ est l'ordre de g si et seulement si $g^d = e$ et pour tout diviseur de d $0 < t < d$ on a $g^t \neq e$.*

Exercice 6. Le démontrer.

Remarque 2. Si $g \in G$ et p est un nombre premier tel que $g^p = e$, alors $g = e$ ou l'ordre de g est p.

4 Homomorphisme de groupe

Définition 5. Soient G et G' deux groupes, un homomorphisme de G dans G' est une application de G dans G' tel que .

Exemple 6.

1. On considère $\phi \ : \ (\mathbb{R},+) \longrightarrow (\mathbb{R}_+^*,\times), \ x \longmapsto \exp(x)$
   On a $\forall x, y \in \mathbb{R}, \ \exp(x+y) = \exp(x)\exp(y)$
   ln est l'application réciproque.
2. Le déterminant est un homomorphisme de $(GL_n(\mathbb{R}),\times)$ dans $(\mathbb{R}^*,\times)$

Remarque 3. Un homorphisme f vérifie

- $f(e) = f(e')$, car $f(e) = f(e \cdot e) = f(e)f(e)$ puis en simplifiant : $e' = f(e)$
- Pour tout $g \in G$, $f(g^{-1}) = f(g)^{-1}$

Pour tout x,

Part II
Opérations de groupes

Part III
Groupes symétriques

Part IV
Sous-groupes distingués et groupes quotient

Part V
Théorème de Sylow

Part VI
Solutions des exercices

Solution de l'exercice 1 Commençons par montrer pour tout $n > 0$, $(g^n)^{-1} = g^{-n}$:

$$(g^n)^{-1} = (g * g^{n-1})^{-1} = ((g^{n-1})^{-1} * g^{-1})^{-1}$$

$$(g^n)^{-1} = ((g^{n-2})^{-1} * g^{-1} * g^{-1})^{-1}$$

$$\dots$$

$$(g^n)^{-1} = \underbrace{g^{-1} * g^{-1} ... g^{-1}}_{n \text{ fois}} = (g^{-1})^n = g^{-n}$$

Pour tout $m, n \in \mathbb{Z}$, on distingue plusieurs cas :

- $m = 0$ ou $n = 0$ ✓
- $m, n > 0$: ✓
- $m > 0, n < 0$ avec $m + n < 0$:

$$g^m * g^n = g^m * \left(g^{-1}\right)^{|n|} = g^m * \left(g^{-1}\right)^m * \left(g^{-1}\right)^{|n|-m} = e * \left(g^{-1}\right)^{|n|-m} = \left(g^{-1}\right)^{-n-m} = g^{m+n}$$

- $m, n < 0$:

$$g^{m+n} = \left(g^{-1}\right)^{|m|+|n|} = \left(g^{-1}\right)^{|m|} * \left(g^{-1}\right)^{|n|} = g^m * g^n$$

- les autres cas se démontrent de la même façon

Solution de l'exercice 2 Supposons par l'absurde que $\left(\mathbb{Z}^G, \otimes\right)$ est un groupe :

Stabilité de l'opération : ✓

Élément neutre : On cherche $\epsilon \ : \ G \longrightarrow \mathbb{Z}$ tel que

$$\forall f \in \mathbb{Z}^G, \ \forall g \in G, \ \sum_{h \in G} \epsilon(h) f(h^{-1} * g) = \sum_{h \in G} f(h) \epsilon(h^{-1} * g) = f(g)$$

Pour f valant 1 sur G on a

$$\sum_{h \in G} \epsilon(h) = \sum_{h \in G} \epsilon(h^{-1} * g) = 1$$

Vérifions que si ϵ est définie par $\epsilon(g) = \begin{cases} 1, \text{ si } g = e \\ 0, \text{ sinon} \end{cases}$, alors elle est neutre pour $\otimes$:

$$\sum_{h \in G} \underbrace{\epsilon(h)}_{1 \ ssi \ h=e} f(h^{-1} * g) = f(e^{-1} * g) = f(g)$$

$$\sum_{h \in G} f(h) \underbrace{\epsilon(h^{-1} * g)}_{1 \text{ ssi } h=g} = f(g)$$

✓

Existence d'un inverse : Soit $f : G \longrightarrow \mathbb{Z}$, il existe $\phi : G \longrightarrow \mathbb{Z}$ telle que $f \otimes \phi = \phi \otimes f = \epsilon$

$$\forall g \neq e,\ \sum_{h \in G} \phi(h) f(h^{-1} * g) = \sum_{h \in G} f(h)\phi(h^{-1} * g) = 0$$

et

$$\sum_{h \in G} \phi(h) f(h^{-1}) = \sum_{h \in G} f(h)\phi(h^{-1}) = 1$$

la deuxième égalité est impossible lorsque f est la fonction nulle, $\left(\mathbb{Z}^G, \otimes\right)$ n'est donc pas un groupe.

Solution de l'exercice 3 Soit K un sous-groupe vérifiant les propriétés suivantes :

$$\begin{array}{ll} (1) & \forall H \leqslant G,\ A \subseteq H \Longrightarrow K \subseteq H \\ (2) & \qquad A \subseteq K \leqslant G \end{array}$$

On rappelle que

$$\begin{array}{ll} (3) & \forall H \leqslant G,\ A \subseteq H \Longrightarrow \langle A \rangle \subseteq H \\ (4) & \qquad A \subseteq \langle A \rangle \leqslant G \end{array}$$

$A \subseteq K$ alors d'après (3) $\langle A \rangle \subseteq K$ et $A \subseteq \langle A \rangle$ alors d'après (1) $K \subseteq \langle A \rangle$

Solution de l'exercice 4 On pose $A = \{g^n \mid n \geqslant 0\}$.
$g \in A$ donc $\langle g \rangle \subseteq A$, de plus $g \in \langle g \rangle$ alors par récurrence $\forall n \geqslant 0,\ g^n \in \langle g \rangle$, d'où $A \subset \langle g \rangle$.

Solution de l'exercice 6 Soit $d > 0$ et $g \in G$, montrons l'équivalence entre les deux propositions suivantes

$$\begin{array}{ll} (i) & d \text{ est l'odre de } g \\ (ii) & g^d = e \text{ et } \forall k | d,\ (k < d \Longrightarrow g^k \neq e) \end{array}$$

(i)* $\Longrightarrow$ *(ii)
d étant l'ordre de g, on a $g^d = e$, et par minimalité de d on a pour tout $k < d$, $g^k \neq e$ (en particulier pour tout diviseur strict de d). ✓
(ii)* $\Longrightarrow$ *(i)
d vérifie :

1. $g^d = e$
2. $\forall k < d,\ (k | d \Longrightarrow g^k \neq e)$

On a que $d \geqslant ord(g)$, par minimalité de $ord(g)$.
Supposons maintenant que $d \neq ord(g)$, c'est à dire que $d > ord(g)$, l'ordre de g divise nécessairement d, d'où l'existence d'un entier $n > 1$ tel que $d = n \cdot ord(g)$.
$ord(g)$ est donc un diviseur strict de d ! d est ainsi égal à l'ordre de g, sinon on aurait d'après (2) $g^{ord(g)} \neq e$ ✓