Algèbre et géométrie 1

Patrick Le Meur et Pierre Gervais

October 30, 2016

Contents

Part I
Groupes

1 Définitions et premiers exemples

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

- G est un ensemble
- $* \ : \left\{ \begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & g * h \end{array} \right.$ 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 $\otimes \ : \left\{ \begin{array}{ccc} \mathbb{Z}^G \times \mathbb{Z}^G & \longrightarrow & \mathbb{Z}^G \\ (f_1, f_2) & \longmapsto & \left(g \longmapsto \sum_{h \in G} f_1(h) f_2(h^{-1} * g) \right) \end{array} \right.$
   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. $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\} \leqslant (\mathbb{C}^*, \times)$
5. Pour $n > 0$, $\mathbb{U}_n = \{z \in \mathbb{C}^* \mid z^n = 1\} \leqslant \mathbb{U} \leqslant \mathbb{C}^*$

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* $\bigcap\limits_{i \in I} H_i \leqslant G$

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 $\mathcal{O}_n(\mathbb{R})$ est engendré par les réflexions, c'est à dire les matrices 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 $(\mathbb{U}, \times)$, 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 $\mathbb{U}_6$, 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 strict k de d on a $g^k \neq e$.*

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

4.1 Définition

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 $\varphi \ : \ (\mathbb{R},+) \longrightarrow (\mathbb{R}_+^*, \times), \ x \longmapsto \exp(x)$
   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 homomorphisme f vérifie

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

4.2 Étude des homomorphismes de $\mathbb{Z}$

Soit $(G, \star)$ un groupe et un homomorphisme $f \ : \ (\mathbb{Z},+) \longrightarrow (G,\star)$, on a :

- $f(1) \in G$
- $\forall n > 0, \ f(n) = f\left(\sum_{i=1}^{n} 1\right) = \prod_{i=1}^{n} f(1) = f(1)^n$
  et $\forall n > 0, \ f(-n) = f(n)^{-1} = (f(1)^n)^{-1} = f(1)^{-n}$

On en déduit immédiatement que pour tout homomorphismes $f_1, f_2 \ : \ (\mathbb{Z},+) \longrightarrow (G,\star)$

$$f_1 = f_2 \Longleftrightarrow f_1(1) = f_2(1)$$

Théorème 2. *Soit* $(G,\star)$ *un groupe, l'application*

$$\varphi \ : \ \left\{ \begin{array}{lcl} \mathcal{H}(\mathbb{Z}, G) & \longrightarrow & G \\ f & \longmapsto & f(1) \end{array} \right.$$

est bijective et d'application réciproque

$$\varphi^{-1} \ : \ \left\{ \begin{array}{lcl} G & \longrightarrow & \mathcal{H}(\mathbb{Z}, G) \\ g & \longmapsto & n \longmapsto g^n \end{array} \right.$$

4.3 Compositions et isomorphismes

Définition 6.

- Un homomorphisme bijectif est appelé *isomorphisme*.
- Deux groupes sont dits *isomorphes* si et seulement s'il existe un isomorphisme entre eux.
- Un endomorphisme bijectif est un *automorphisme*.

Propriété 5.

- *La composée de deux homomorphismes est un homomorphismes.*
- *Si un homomorphisme est bijectif, alors son application réciproque est un homomorphisme.*
- *Soit G un groupe, $Aut(G) \leqslant \mathfrak{S}_G$.*

Exemple 7.

1. $\left\{ \begin{array}{rcl} \{\pm 1\} & \longrightarrow & Aut(\mathbb{Z}) \\ 1 & \longmapsto & id_{\mathbb{Z}} \\ -1 & \longmapsto & -id_{\mathbb{Z}} \end{array} \right.$

2. Soit $k > 0$, $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & kn \end{array} \right.$ est un endomorphisme mais pas un automorphisme.

4.4 Sous-groupes associés à un homomorphisme

Proposition 3. *Soit $f\ :\ G \longrightarrow H$ un homomorphisme de groupes*

- *Pour tout groupe $H' \leqslant H$, on a $f^{-1}(H') \leqslant G$*
- *Pour tout groupe $G' \leqslant G$, on a $f(G') \leqslant H$*

Définition 7. Pour tout homomorphisme f d'un groupe G dans un autre G', on appelle *noyau de* f l'ensemble $\ker(f) = \{g \in G \mid f(g) = e\} \leqslant G$ et l'*image de* f l'ensemble $Im(f) = f(G)$

Exercice 7. Soient $d, n > 0$, déterminer l'image et le noyau de l'homomorphisme :

$$\left\{ \begin{array}{ccc} \mathbb{U}_n & \longrightarrow & \mathbb{U}_n \\ x & \longmapsto & x^d \end{array} \right.$$

Théorème 3. *Soit $f\ :\ G \longrightarrow H$ un homomorphisme de groupes, l'application*

$$\varphi\ :\ \left\{ \begin{array}{rcl} \{\textit{Sous-groupes de } Im(f)\} & \longrightarrow & \{\textit{Sous-groupes de } G \textit{ contenant } \ker(f)\} \\ H & \longmapsto & f^{-1}(H') \end{array} \right.$$

est une bijection.

Preuve 3. Pour tout $G' \leqslant G$ contenant $\ker f$, on définit θ par $\theta(G') = f(G') \leqslant Im(f)$.
On démontre que θ est l'application réciproque de φ.

1. Soit $H' \leqslant Im(f)$, on vérifie $(\theta \circ \varphi)(H') = f(f^{-1}(H')) = H'$ car la co-restriction de f à $Im(f)$ est surjective.

2. Soit $G' \leqslant G$ tel que $\ker f \subseteq G'$, on a $G' \subseteq (\varphi \circ \theta)(G') = f^{-1}(f(G'))$, montrons maintenant $f^{-1}(f(G')) \subseteq G'$:
   Soit $x \in f^{-1}(f(G'))$, alors $f(x) \in f(G')$ et il existe $u \in G'$ tel que $f(x) = f(u)$.
   On a donc :
$$\begin{aligned} f(x) &= f(u) \\ f(xu^{-1}) &= e \\ xu^{-1} &\in \ker f \subseteq G' \\ x &\in \underbrace{(G') \cdot u}_{G' \text{ car } u \in G'} = G' \end{aligned}$$
   Ainsi $f^{-1}(f(G')) \subseteq G'$, et donc $(\varphi \circ \theta)(G') = G'$.

θ est bien la bijection réciproque de φ.

□

Part II
Opérations de groupes

5 Rappels sur les relations d'équivalence

Définition 8. Soit X un ensemble.
Une relation binaire $\sim$ sur X est une *relation d'équivalence* si :

1. $\sim$ est transitive : $\forall x, y, z \in X,\ (x \sim y \wedge y \sim z \Longrightarrow x \sim z)$
2. $\sim$ est réflexive : $\forall x \in X,\ x \sim x$
3. $\sim$ est symétrique : $\forall x, y \in X,\ x \sim x$

On appelle la *classe d'équivalence de x* l'ensemble $\{y \in X \mid x \sim y\}$ et on note $X/\sim$ l'ensemble des classes d'équivalence que l'on appelle *ensemble quotient*.

L'application de $X \longrightarrow X/\sim$ qui à tout élément x associe sa classe d'équivalence est appelée *surjection canonique*.

Proposition 4. *Pour une relation $\sim$ donnée, $X/\sim$ est une partition de X.*

Exemple 8. Soit $(G, \cdot)$ un groupe.

1. Soit $H \leqslant G$ et $\sim$ la relation définie par $\forall g_1, g_2 \in G,\ (g_1 \sim g_2 \Longleftrightarrow \exists h \in H\ :\ g_1 \cdot h = g_2)$
2. $\mathcal{R}$ par $\forall g_1, g_2 \in G,\ (g_1 \mathcal{R} g_2 \Longleftrightarrow \exists h \in H\ g_1 = h g_2 h^{-1})$
3. $\forall H, K \leqslant G,\ (H \sim K \Longleftrightarrow \exists g \in G\ :\ gHg^{-1} = K)$

Théorème 4. *Soit $\sim$ une relation d'équivalence, sur un ensemble X, Y un ensemble et $f\ :\ X \longrightarrow Y$ une application constante sur les classes d'équivalences.*
Il existe alors une unique application de $g\ :\ (X/\sim) \longrightarrow Y$ telle que $g \circ \pi = f$ où π est la surjection canonique.

6 Opérations de groupes

Définition 9. On définit une action de groupe $(G, \star)$ sur un ensemble X par la donnée d'une application

$$\phi \ : \ \begin{cases} G \times X & \longrightarrow \quad X \\ (g, x) & \longmapsto \quad g \cdot x \end{cases}$$

vérifiant $\forall x \in G, \ e \cdot x = x$ et $\forall g, h \in G, \ \forall x \in X, \ g \cdot (h \cdot x) = (h \star g) \cdot x$

Exemple 9. Soit G un groupe.

1. Soit H un sous-groupe de G, l'action de H sur G définie par $h \cdot g = hg$ est appelée action de H sur G par *translation à gauche.*
2. L'action de G sur lui même définie par $h \cdot g = hgh^{-1}$ est appelée action de G sur lui-même par *conjugaison.*
3. L'action de G sur $\mathcal{S}(G)$ définie par $g \cdot H = gHg^{-1} = i_g(H)$ est l'opération de G sur ses sous-groupes par *conjugaison.*

Proposition 5. *Soient $(G, \star)$ un groupe, X un ensemble et $\varphi \ : \ G \times X \longrightarrow X$.*

φ définit une action de groupe si et seulement si pour tout $g \in G$, l'application $\varphi_g \ : \ \begin{cases} G & \longrightarrow \quad X \\ x & \longmapsto \quad g \cdot x \end{cases}$ est bijective et $g \longmapsto \varphi_g$ est un homomorphisme de $(G, \star)$ dans $(\mathfrak{S}_X, \circ)$.

Remarque 4. On en déduit $\forall g, h \in G, \ \varphi_g \circ \varphi_h = \varphi_{g \star h}$ et $\varphi_{g^{-1}} = (\varphi_g)^{-1}$

Exemple 10.

1. L'action de $GL_n(\mathbb{K})$ sur $\mathbb{K}^n$ définie par $M \cdot x = Mx$ est une action de groupe.
2. L'action de $GL_n(\mathbb{K})$ sur $M_{m \times n}(\mathbb{K})$ définie par $M \cdot N = MN$ est une action de groupe.
3. L'action des applications linéaires inversibles de E sur les formes quadratiques de E définie par $g \cdot q = q \circ g^{-1}$

   Exercice 8. Le démontrer.
4. L'action par conjugaison des matrice inversibles sur les matrices carrées est une action de groupe.

7 Orbites, stabilisateurs

Définition 10. Soit G un groupe opérant sur X et $x \in X$, on définit :

- L'orbite de x l'ensemble $G \cdot x = \{g \cdot x \mid g \in G\}$
- Le stabilisateur de x l'ensemble $Stab_G(x) = G_x = \{g \in G \mid g \cdot x = x\}$

Exemple 11. Considérons l'action de G sur lui-même par translation à gauche. On a $G \cdot x = G$ et $G_x = \{e\}$

Proposition 6. *La relation sur X définie par :*

$$\forall x, y \in X, x \sim y \Longleftrightarrow \exists g \in G \ : \ g \cdot x = y$$

est une relation d'équivalence, dite associée à l'opération de G sur X.

Remarque 5. Si $x \in X$, alors $G \cdot x$ est la classe d'équivalence de x.

On rappelle aussi que si $\mathcal{R}$ est une relation d'équivalence sur un ensemble X, alors $X/\mathcal{R}$ est une partition de X. En particulier, dans le cas d'une relation d'équivalence associée à une action de groupe, $x \sim y \Longleftrightarrow G \cdot x = G \cdot y$.

On note alors l'ensemble quotient $X/\sim$ par $G\backslash X$ et on l'appelle ensemble quotient de X par G.

Remarque 6. Si on se donne une action à droite sur X, on note X/G l'ensemble des classes d'équivalence.

Définition 11. Soit $H \leqslant G$, on note l'ensemble quotient de G par l'opération de translation à gauche de H :

$$H\backslash G = \{Hg \mid g \in G\}$$

De même on note l'ensemble quotient de G par l'opération de translation à droite de H :

$$G/H = \{gH \mid g \in G\}$$

Définition 12. Une action de G sur X est dite :

- *transitive* s'il n'existe qu'une seule orbite
- *fidèle* si $\forall g \in G,\ (\forall x \in X,\ g \cdot x = x) \Longrightarrow g = e$
- *libre* si $\forall x \in X, \forall g \in G, g \cdot x = x \Longrightarrow g = e$

Remarque 7. L'action est fidèle si :

$$\bigcap_{x \in X} Stab(x) = \{e\}$$

et elle est transitive si $\forall x \in X,\ Stab(x) = \{e\}$.

Exercice 9. Une opération est fidèle si et seulement si l'homomorphisme associé est injectif.

Exemple 12.

1. L'action de $GL_n(\mathbb{R})$ sur $\mathbb{R}^n$ admet deux orbites : $\{0\}$ et $\mathbb{R}^n\backslash\{0\}$

2. L'action de $GL_n(\mathbb{R})$ sur $\mathbb{R}^n\backslash\{0\}$ admet une unique orbite $\mathbb{R}^n\backslash\{0\}$ donc l'action est transitive.

   Elle est fidèle ($(\forall x \in \mathbb{R}^n,\ Mx = x) \Longrightarrow M = I_n$) mais elle n'est pas libre car une matrice inversible différente de I_n de vecteur propre x et de valeur propre 1 vérifie $Mx = x$.

3. Soient $H \leqslant G$, l'action de H sur G par translation à gauche.

   L'action est transitive si et seulement si $G = H$.

   L'opération est libre car pour tout $g \in G$ et $x \in G$, si on a $g \star x = x$, alors en simplifiant par x on a $g = e$. Elle est donc également fidèle.

4. On considère les sommets du cube de côté 2 l'ensemble $\mathcal{C} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid \forall i,\ |x_i| = 1\}$ et le groupe $G \leqslant SO_3(\mathbb{R}^3)$ préservant globalement $\mathcal{C}$.

   L'opération est fidèle, car si g est une application fixant trois points distincts, alors elle possède trois vecteurs propres linéairement indépendants de valeur propre 1, elle est donc diagonalisable et est égale à l'identité.

   Elle est transitive car tout sommet peut être envoyé sur un autre.

   Elle n'est pas libre car la rotation autour d'une "diagonale" fixe les sommets par laquelle elle passe.

7.1 Aspects numériques

Proposition 7. *1. Étant donné une opération de G sur X, il existe une application bijective*

$$\varphi \; : \; \left\{ \begin{array}{ccc} G/Stab(x) & \longrightarrow & G \cdot x \\ gStab(x) & \longmapsto & g \cdot x \end{array} \right.$$

2. Si G et X sont finis, alors

$$|G \cdot x| = \frac{|G|}{|Stab(x)|}$$

3. Si G et X sont finis, on choisit pour chaque orbite ω un élément $x_\omega \in \omega$ et on obtient :

$$|X| = \sum_{\omega \in G \backslash X} \frac{|G|}{Stab_G(x_\omega)}$$

Les deux égalités s'appellent équations aux classes.

Preuve 4. Soit $x \in G$, on considère l'action de $Stab_G(x)$ sur G par translation à droite, et $\sim$ la relation d'équivalence sur G associée à celle-ci.

On définit :

$$f \; : \; \left\{ \begin{array}{ccc} G & \longrightarrow & G \cdot x \\ g & \longmapsto & g \cdot x \end{array} \right.$$

qui est constante sur les classes d'équivalences $G/\sim$, donc il existe $\varphi \; : \; G/Stab_G(x) \longrightarrow G \cdot x$ telle que $\forall g \in G, \; \varphi(gStab_G(x)) = g \cdot x$

Montrons que φ est bijective.

φ est surjective Soit $y \in G \cdot x$, il existe $g \in G$ tel que $y = g \cdot x = f(g) = \varphi(gStab_G(x))$. ✓

S oient $\alpha, \beta \in G/Stab_G(x)$ tels que $\varphi(\alpha) = \varphi(\beta)$.

Il existe $g, h \in G$ tels que $\alpha = gStab_G(x)$ et $\beta = hStab_G(x)$.

Alors $g \cdot x = f(g) = \varphi(\alpha) = \varphi(\beta) = f(h) = h \cdot x$, d'où $h^{-1} \star g \in Stab_G(x)$ ainsi $gStab_G(x) = hStab_G(x)$, on obtient alors $\alpha = \beta$. ✓

□

Exercice 10. Pour chaque classe $\omega \in G/Stab_G(x)$ on pose $g_\omega \in \omega$, alors pour tout $g \in G$ il existe un unique couple $(\omega, h) \in G/Stab_G(x) \times Stab_G(x)$ tel que $g = g_\omega \star h$

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 $n > 0$, $(g^n)^{-1} = g^{-n}$:

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

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

$$\cdots$$

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

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 : $\checkmark$

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 $\epsilon(g) = \left\{ \begin{array}{l} 1, \text{ si } g = e \\ 0, \text{ sinon} \end{array} \right.$, alors elle est neutre pour $\otimes$:

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

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

$\checkmark$

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

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

et

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

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 :

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

On rappelle que

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

$A \subseteq K$ 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) $g^{ord(g)} \neq e$ ✓

Solution de l'exercice 7 Soit $f\ :\ \left\{ \begin{array}{lcl} \mathbb{U}_n & \longrightarrow & \mathbb{U}_n \\ x & \longmapsto & x^d \end{array} \right.$

Noyau $\ker f = \{x \in \mathbb{U}_n \mid x^d = e\} = \mathbb{U}_d$

$Im(f) = \{x^d \mid x \in \mathbb{U}_n\} = \mathbb{U}_{\frac{n}{n \wedge d}}$

Solution de l'exercice 8 On considère l'action des applications linéaires inversibles de E sur les formes quadratiques de E définie par $g \cdot q = q \circ g^{-1}$, montrons que c'est une action de groupe.

Composition

Soient $f, g \in GL(E)$ et une forme quadratique q :

$f \cdot (g \cdot q) = (g \cdot q) \circ f^{-1} = q \circ g^{-1} \circ f^{-1} = q \circ (f \circ g)^{-1} = (f \circ g) \cdot q$ ✓

Élément neutre

$id \cdot q = q \circ id^{-1} = q$ ✓

$C_m \times C_n \cong C_{mn}$ Soient m et n premiers entre eux.

On considère l'application

$$\varphi\ :\ \left\{ \begin{array}{lcl} C_m \times C_n & \longrightarrow & C_{mn} \\ (g, h) & \longmapsto & gh \end{array} \right.$$

Pour tout $(g, h), (g', h') \in C_m \times C_n$, on a :

$$\varphi((g, h)(g', h') = \varphi(gg', hh') = gg'hh' = (gh)(g'h') = \varphi(g, h)\varphi(g', h')$$

Donc φ est un morphisme, de plus si elle est injective alors elle sera bijective car $|C_{mn}| = |C_m \times C_n|$.

Soit $(g, h) \in C_m \times C_n$ tel que $\varphi(g, h) = gh = e$

$g \in C_m$ donc l'ordre de g divise m, de même l'ordre de h^{-1} divise n. On a donc que l'ordre de $g = h^{-1}$ divise m et n, or m et n sont premiers entre eux, alors l'ordre de g divise $m \wedge n = 1$.

Ainsi $g = h = e$, φ est donc injective et donc un isomorphisme.

Solution de l'exercice 10 Montrons que pour tout $g \in G$ il existe un unique couple $(\omega, h) \in G/\mathrm{Stab}(x) \times \mathrm{Stab}(x)$ tel que $g_\omega \star h = g$, c'est-à-dire qu'il existe une bijection entre les ensembles G et $G/\mathrm{Stab}(x) \times \mathrm{Stab}(x)$.

On pose

$$\varphi \ : \ \left\{ \begin{array}{lcl} G/\mathrm{Stab}(x) \times \mathrm{Stab}(x) & \longrightarrow & G \\ (\omega, h) & \longmapsto & g_\omega \star h \end{array} \right.$$

Pour tout $g \in G$, $g \in \omega = \mathrm{Stab}(x)$ et il existe un certain $g_\omega \in \omega$ tel que $g_\omega \mathrm{Stab}(x) = g\mathrm{Stab}(x)$, c'est-à-dire qu'il existe un $h \in \mathrm{Stab}(x)$ tel que $g_\omega \star h = g$, d'où la surjectivité de φ.

φ est bijective car $|G/\mathrm{Stab}(x) \times \mathrm{Stab}(x)| = \frac{|G|}{\mathrm{Stab}(x)} \cdot |\mathrm{Stab}(x)| = |G|$.