Algèbre et géométrie 1

Patrick Le Meur et Pierre Gervais

December 13, 2016

Contents

Part I
Groupes

1 Définitions et premiers exemples

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

- G est un ensemble
- $* : \begin{cases} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & g*h \end{cases}$ 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* $\bigcap_{i \in I} H_i \leqslant G$

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*

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

est bijective et d'application réciproque

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

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

$$\begin{cases} \mathbb{U}_n & \longrightarrow & \mathbb{U}_n \\ x & \longmapsto & x^d \end{cases}$$

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

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

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

$$\phi : \left\{ \begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array} \right.$$

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 $\varphi_g : \left\{ \begin{array}{ccc} G & \longrightarrow & X \\ x & \longmapsto & g \cdot x \end{array} \right.$ 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 :*

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

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, $x \sim y \iff G \cdot x = G \cdot y$.
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 de $G/\sim$ (de la forme $g\mathrm{Stab}_G(x)$), 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 $y = g \cdot x = f(g) = \varphi(gStab_G(x))$. ✓

φ est injective

Soient $\alpha, \beta \in G/Stab_G(x)$ 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 $g = g_\omega \star h$

Théorème 5. *Soit $(G, \star)$ un p-groupe (avec p premier) opérant sur un ensemble fini X, on note $X^G = \{x \in X \mid \forall g \in G,\ g \cdot x = x\}$, on a :*

$$|X^G| \equiv |X| \mod p$$

Preuve 5. On remarque tout d'abord

$$\forall x \in X, (x \in X^G \iff G \cdot x = \{x\})$$

et de manière équivalente sachant qu'une orbite n'est jamais vide

$$\forall x \in X, (x \notin X^G \iff |G \cdot x| \geqslant 2)$$

Soient $\omega_1, \omega_2, ...\omega_n$ les orbites de X sous l'actions de G ordonnées de telle façon que les k premières soient les orbites réduites à un élément, où $k = \left|X^G\right|$, et $x_1, x_2, ...x_n$ des éléments de X tels que $\forall i \leqslant n,\ x_i \in \omega_i$.

Les orbites de $(\omega_i)_{i \leqslant n}$ forment une partition de X, d'où :

$$|X| = \sum_{i=1}^{n} |\omega_i|$$

$$|X| = \sum_{i=1}^{k} |w_i| + \sum_{i=k+1}^{n} |w_i|$$

$$|X| = \sum_{i=1}^{k} 1 + \sum_{i=k+1}^{n} |w_i|$$

$$|X| = \left|X^G\right| + \sum_{i=k+1}^{n} |w_i|$$

Chaque $\mathrm{Stab}(x_i)$ est un sous-groupe de G, qui est d'ordre puissance de p, donc d'après le théorème de Lagrange, $\mathrm{Stab}(x_i)$ l'est aussi, et ainsi $|\omega_i| = \dfrac{|G|}{|\mathrm{Stab}(x_i)|}$ est une puissance de p.

De plus, pour tout $i > k$, $x_i \notin X^G$ donc $|G \cdot x_i| = |w_i| \geqslant 2$, et comme $p \geqslant 2$, $|\omega_i|$ est une puissance non-nulle de p.

On en déduit que $\sum_{i=k+1}^{n} |w_i|$ est un multiple de p, d'où :

$$|X| \equiv \left|X^G\right| \mod p$$

□

Théorème 6. *Théorème de Cauchy*
Soit G un groupe fini et p un diviseur premier de $|G|$, alors il existe $g \in G$ tel que $|g| = p$.

Preuve 6. Soit $n = |G|$ et soit $X = \{(g_1, g_2, ...g_p) \mid g_1 g_2 ... g_p = e\}$, cet ensemble est de cardinal n^{p-1} car il existe n^{p-1} $(p-1)$-uplets $(g_1, ..., g_{p-1})$ de G et il existe pour chacun un unique $g_p = (g_1 ... g_{p-1})^{-1}$ tel que $g_1 ... g_p = e$.
On pose ω la permutation de X

$$\omega : \left\{ \begin{array}{ccc} X & \longrightarrow & X \\ (g_1, g_2, ...g_p) & \longmapsto & (g_2, g_3, ...g_p, g_1) \end{array} \right.$$

Celle-ci est bien définie car pour tout $(g_1, ...g_p) \in X$

$$g_1 ... g_p = e$$

$$g_2 ... g_p g_1 = g_1^{-1} g_1$$

$$g_2 ... g_p g_1 = e$$

$$\underbrace{(g_2, ..., g_p, g_1)}_{\omega(g_1, ...g_p)} \in X$$

et par récurrence, pour tout $k \geqslant 0$, $\omega^k(g_1, ...g_p) \in X$.
De plus, elle est d'ordre p, il existe donc un unique homomorphisme de G vers $\mathcal{S}_X$ envoyant $e^{2i\pi/p}$ sur ω, on définit une action de $\mathbb{U}_p$ sur X à l'aide de celle-ci.
D'après le théorème précédent, on a :

$$\left|X^G\right| \equiv |X| \mod p$$

$$\left|X^G\right| \equiv n^{p-1} \mod p$$

$$\left|X^G\right| \equiv 0 \mod p, \text{ car } p \text{ divise } n$$

Or X^G est non-vide, il contient $(e, e, ...e)$, donc X^G est un multiple de $p \geqslant 2$, c'est-à-dire qu'il contient un élément $g = (g_1, g_2, ...g_p)$ tel que $e^{2i\pi/p} \cdot g = g$, donc $g_1 = g_2$, $g_2 = g_3$, etc. et alors $g_1 = g_2 = ... = g_p$.
$g = (g_1, ..., g_1) \in X^G$ donc $g_1^p = e$ avec $g_1 \neq e$, il existe donc un élément d'ordre p dans G.

□

8 Applications à la géométrie affine

Soit $\mathbb{K}$ un corps.

8.1 Espaces affines

Définition 13. Soit $\mathcal{E}$ un ensemble non-vide, et E un espace vectoriel, $\mathcal{E}$ est un *espace affine* de *direction* E s'il existe une action libre et transitive de E sur $\mathcal{E}$

$$\begin{cases} E & \longrightarrow & \mathcal{E} \\ (M,u) & \longmapsto & M+u \end{cases}$$

On a alors :

- Pour tout $A, B \in \mathcal{E}$ il existe un unique $u \in E$ tel que $A + u = B$, on note $\overrightarrow{AB} = u$.
- Pour tout $A, B, C \in \mathcal{E}$ on a :
  1. $\overrightarrow{AB} = 0 \Leftrightarrow A = B$
  2. $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$
  3. $-\overrightarrow{AB} = \overrightarrow{BA}$

En effet, pour tout $A, B \in \mathcal{E}$, l'action étant transitive, il existe $u \in E$ tel que $B + u = A$, et étant libre, s'il existe un autre $v \in E$ tel que $B = A + u = A + v$ on a que $u = v$.

De plus, pour tout $A, B, C \in \mathcal{E}$ on vérifie les propriétés :

1. $\overrightarrow{AB} = 0 \Longleftrightarrow B = A + \overrightarrow{AB} = A \Longleftrightarrow A = B$
2. $A + (\overrightarrow{AB} + \overrightarrow{BC}) = (A + \overrightarrow{AB}) + \overrightarrow{BC} = B + \overrightarrow{BC} = C$ d'où $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$
3. $A = A + 0 = A + \overrightarrow{AA}$ donc $\overrightarrow{AA} = 0$, alors $\overrightarrow{AA} = \overrightarrow{AB} + \overrightarrow{BA} = 0$, donc $-\overrightarrow{AB} = \overrightarrow{BA}$.

8.2 Sous-espaces affine

Soit $\mathcal{E}$ un espace affine de direction E.

Définition 14. On appelle *sous-espace affine* de $\mathcal{E}$ tout sous-ensemble $\mathcal{F} \subseteq \mathcal{E}$ tel que $\mathcal{F}$ est l'orbite d'un élément de $\mathcal{E}$ pour l'opération d'un sous-espace vectoriel de E.

Exemple 13.

1. $E = \mathcal{E} = \mathcal{K}^3$

   $\mathcal{F} = \{(x,y,z) \in \mathbb{K}^3 \mid z = 1\}$

   $\mathcal{F} = (0,0,1) + \{(x,y,z) \in \mathbb{K}^3 \mid z = 0\}$

2. Soit V un $\mathbb{K}$-espace vectoriel et φ une forme linéaire non-nulle, alors $\{u \in V \mid \varphi(u) = 1\} = u_0 + \ker\varphi$ est un sous-espace affine, où $\varphi(u_0) = 1$.

   Exercice 11. Le démontrer

Remarque 8. Soient $X, Y \in \mathcal{E}$ et F, G des sous-espace vectoriels de E tels que $X + F = Y + G$, alors $F = G$.

$X \in X + F = Y + G$, alors $\overrightarrow{XY} \in G$, symétriquement on montre $\overrightarrow{YX} \in F$ et donc $\overrightarrow{XY} = -\overrightarrow{YX} \in F$, on en déduit $\overrightarrow{XY} \in F \cap G$.

Soit $u \in F$, on a $X + u \in X + F = Y + G$.

Il existe $v \in G$ tel que

$$X + u = X + v$$

$$X + (u - v) = X$$

$$\overrightarrow{XY} = u - v$$

$$u = \overrightarrow{XY} + v \in G$$

Donc $F \subseteq G$, symétriquement $G \subseteq F$ donc $F = G$.

Remarque 9. Soit $X \in \mathcal{E}$ soit F un sous-espace vectoriel de E, alors pour tout $M \in \mathcal{E}$, $M \in X + F \iff \overrightarrow{XM} \in F$

Exercice 12. Remontrer la remarque précédente à l'aide de cette propriété.

Définition 15. Soit $\mathcal{F}$ un sous-espace affine de $\mathcal{E}$, il existe un unique sous-espace vectoriel F de E tel qu'il existe $M \in \mathcal{E}$ vérifiant $\mathcal{F} = M + F$, on l'appelle direction de $\mathcal{F}$.

Si $\dim F$ est finie, on dit que $\mathcal{F}$ est de dimension $\dim F$.

Propriété 6.

- *Soit I un ensemble et $(\mathcal{F}_i)_{i\in I}$ une famille de sous-espace affine de $\mathcal{E}$ de directions respectives (F_i).*

  Si $\bigcap_{i\in I} \mathcal{F}_i \neq \emptyset$, alors il est un sous-espace affine de direction $\bigcap_{i\in I} F_i$.

- *Soient $\mathcal{F}, \mathcal{G}$ deux sous-espaces affines de $\mathcal{E}$ de directions supplémentaires dans E, alors $\mathcal{F} \cap \mathcal{G}$ est réduite à un point.*

- *Soient $\mathcal{F}$ et $\mathcal{G}$ de directions respectives F et G, si $\mathcal{F} \subseteq \mathcal{G}$ alors $F \subseteq G$.*

Preuve 7.

1. On se restreint au cas ou I est de cardinal 2, soient $\mathcal{F}$ et $\mathcal{G}$ deux sous-espaces affines de directions F et G.
2. Soient $\mathcal{A}, \mathcal{B}$ deux sous-espaces affines de directions supplémentaires.

   Il existe $A, B \in \mathcal{E}$ tels que $\mathcal{F} = A + F$ et $\mathcal{G} = B + G$.

   $F \oplus G = E$, on peut alors décomposer $\overrightarrow{AB} = f + g$ avec $(f, g) \in F \times G$

$$A + \overrightarrow{AB} = B$$

$$\underbrace{A + f}_{\in \mathcal{F}} = A + (\overrightarrow{AB} - g) = \underbrace{B - g}_{\in \mathcal{G}}$$

   Donc $X := A + f \in \mathcal{F} \cap \mathcal{G}$.

   Ce point est de plus unique car si $Y \in \mathcal{F} \cap \mathcal{G}$, alors $\overrightarrow{XY} \in F \cap G = \{0\}$, c'est-à-dire $\overrightarrow{XY} = 0$ et donc $X = Y$.

Exemple 14.

Soit S un système d'équations linéaires à n inconnues, soit S_h son système homogène.

Soit $\mathcal{F} \subseteq \mathbb{K}^n$ l'ensemble des solutions de S, et $F \subseteq \mathbb{K}^n$ l'ensemble de solutions de S_h.

Si $F \neq \emptyset$, alors $\mathcal{F}$ est un sous-espace affine de direction F.

Remarque 10. On suppose $\dim E = 2$, deux droites affines de $\mathcal{E}$ vérifient une et une seule des trois conditions suivantes :

- Elles sont égales
- Elles sont disjointes de même direction
- Leur intersection est réduite à un point

Exercice 13. Le démontrer

Définition 16. Deux sous-espaces affines sont *parallèles* s'ils sont de même direction.

Remarque 11. Deux sous-espace affines parallèles sont soit égaux, soit disjoints.

En effet s'ils ne sont pas disjoints, alors il existe $M \in \mathcal{F} \cap \mathcal{G}$ et donc $\mathcal{F} = M + \overrightarrow{\mathcal{F}} = \mathcal{F} = M + \overrightarrow{\mathcal{G}} = \mathcal{G}$

8.3 Applications affines

Définition 17. Soient $\mathcal{E}, \mathcal{F}$ deux espaces affines de directions E et F et $f : \mathcal{E} \longrightarrow \mathcal{F}$, f est *une application affine* s'il existe application linéaire l de E à F telle que :

$$\forall A, B \in \mathcal{E}, \overrightarrow{f(A)f(B)} = l(\overrightarrow{AB})$$

ou de manière équivalente

$$\forall (M, u) \in \mathcal{E} \times E,\ f(M + u) = f(M) + l(u)$$

Preuve 8.

$$\forall A, B \in \mathcal{E},\ \overrightarrow{f(A)f(B)} = l(\overrightarrow{AB}) \Longleftrightarrow \forall A, B \in \mathcal{E},\ f(A) + l(\overrightarrow{AB}) = f(B)$$

$$\forall A, B \in \mathcal{E},\ \overrightarrow{f(A)f(B)} = l(\overrightarrow{AB}) \Longleftrightarrow \forall (A, u) \in \mathcal{E} \times E,\ f(A) + l(u) = f(A + u)$$

Exemple 15.

1. Soit $u \in E$, on pose $\tau_u : \left\{ \begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{E} \\ x & \longmapsto & x + u \end{array} \right.$, c'est une application affine d'application linéaire associée id_E.
2. Soit $\Omega \in \mathcal{E}$ et $\lambda \in \mathbb{K}^\times$, on note $h_{\Omega,\lambda}$ de $\mathcal{E}$ dans $\mathcal{E}$ définie par $h_{\Omega\lambda}(M) = \Omega + \lambda\overrightarrow{\Omega M}$, c'est une application affine d'application linéaire associée λid_E.

   Pour tout $(M, u) \in \mathcal{E} \times E$:

$$\begin{aligned} h(M + u) &= \Omega + \lambda\overrightarrow{\Omega(M + u)} \\ &= \Omega + \left(\overrightarrow{\Omega M} + \overrightarrow{M(M + u)}\right) \\ &= \Omega + \lambda\overrightarrow{\Omega M} + \lambda u \\ &= h(M) + \lambda u \\ &= h(M) + (\lambda id_E)(u) \end{aligned}$$

Remarque 12. Soient $X, Y \in \mathcal{E}$ et $u, v \in \mathcal{E}$, on a $\overrightarrow{(X+u)(Y+v)} = \overrightarrow{XY} + v - u$ car

$$\begin{aligned}\overrightarrow{(X+u)(Y+v)} &= \overrightarrow{(X+u)X} + \overrightarrow{XY} + \overrightarrow{Y(Y+v)} \\ &= -u + \overrightarrow{XY} + v\end{aligned}$$

Proposition 8. *Soient $\mathcal{F}$ et $\mathcal{G}$ des espaces affines, alors :*

1. $\left\{ \begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{E} \\ X & \longmapsto & X \end{array} \right.$ *est une application affine d'application linéaire associée id_E.*
2. *Si $f : \mathcal{E} \longrightarrow \mathcal{F}$ et $f : \mathcal{F} \longrightarrow \mathcal{G}$ sont des applications affines, alors $g \circ f$ l'est aussi, et son application linéaire associée est la composée de celle de f avec celle de g.*
3. *Soit $f : \mathcal{E} \longrightarrow \mathcal{F}$ une application affine, on note L son application linéaire associée, alors f est bijective si et seulement si L bijective, dans ce cas f^{-1} est affine, d'application linéaire associée L^{-1}.*

Preuve 9.

1. ✓
2. Soient $A, B \in \mathcal{E}$
$$\overrightarrow{g(f(A))g(f(B))} = L_g(\overrightarrow{f(A)f(B)}) = L_g(L_f(\overrightarrow{AB})) = (L_g \circ L_f)(\overrightarrow{AB})$$
3. ***f* bijective $\Longrightarrow$ *L* bijective**
   Soit $A \in \mathcal{E}$, et $u \in E$ tel que $L(u) = 0$, on a $f(A+u) = f(A) + L(u) = f(A)$
   or f est injective, alors $A + u = A$, donc $u = 0$, ainsi $\ker L = \{0\}$, L est donc injective.
   Soit $v \in F$ et $u \in E$ tel que $A + u = f^{-1}(f(A) + v)$ alors
   $$L(u) = \overrightarrow{f(A)f(A+u)} = \overrightarrow{f(A)(f(A)+v)} = v$$
   donc L est surjective.
   L est donc bijective.
   ✓
   ***L* bijective $\Longrightarrow$ *f* bijective**
   Réciproquement, si L est bijective, soit $M, X \in \mathcal{E}$ fixés et un point quelconque $A \in \mathcal{E}$, on a
   $$f(M) = X \Longleftrightarrow f(A + \overrightarrow{AM}) = f(A) + L(\overrightarrow{AM}) = X$$
   $$f(M) = X \Longleftrightarrow L(\overrightarrow{AM}) = \overrightarrow{f(A)X}$$
   $$\overrightarrow{AM} = L^{-1}(\overrightarrow{f(A)X})$$
   On pose $f' : \left\{ \begin{array}{ccc} \mathcal{F} & \longrightarrow & \mathcal{E} \\ X & \longmapsto & A + L^{-1}(\overrightarrow{f(A)X}) \end{array} \right.$

On a bien $f' \circ f = id_{\mathcal{E}}$ et $f \circ f' = id_{\mathcal{F}}$:

Soit $X \in \mathcal{E}$, on a :

$$\begin{aligned}(f' \circ f)(X) &= f'\left(f(A) + L\left(\overrightarrow{AX}\right)\right) \\ &= A + L^{-1}\left(\overrightarrow{f(A)\left(f(A) + L\left(\overrightarrow{AX}\right)\right)}\right) \\ &= A + L^{-1}\left(L\left(\overrightarrow{AX}\right)\right) \\ &= A + \overrightarrow{AX} \\ &= X\end{aligned}$$

De même pour $(f \circ f')(Y)$. ✓

On suppose à présent que f et l sont bijectives.

f^{-1} est affine, d'application linéaire associée L^{-1}

Soient $X, Y \in \mathcal{F}$, on montre que $\overrightarrow{f^{-1}(X)f^{-1}(Y)} = L^{-1}(\overrightarrow{XY})$

$L(\overrightarrow{f^{-1}(X)f{-}1(Y)}) = \overrightarrow{f(f^{-1}(X)f(f^{-1}(Y))} = \overrightarrow{XY}$

Or L est injective, donc $\overrightarrow{f^{-1}(X)f^{-1}(Y)} = L^{-1}(\overrightarrow{XY})$

Comme $L : E \longrightarrow F$ est linéaire injective, on a que L^{-1} est linéaire.

✓

Corollaire 2.

- *L'ensemble des applications affines bijectives de $\mathcal{E}$ est un sous-groupe de $\mathfrak{S}_{\mathcal{E}}$, il est appelé groupe affine de $\mathcal{E}$ et est noté $GA(\mathcal{E})$.*
- *L'ensemble des translations est un sous-groupe de $GA(\mathcal{E})$.*
- *L'ensemble G des translations et des homothéties de rapport non-nul est un sous-groupe de $GA(\mathcal{E})$.*

Exercice 14. Soit f d'application linéaire associée $L = \phi(f)$, f est une translation ou une homothétie si et seulement s'il existe $\lambda \in \mathbb{K}^\times$: $L = \lambda id_E$.

Montrons que s'il existe $\lambda \neq 0$ tel que $L = \lambda id_E$, alors f est une homothétie ou une translation :

Si $\boldsymbol{\lambda = 1}$

Soient $M, N \in \mathcal{E}$:

$$\begin{aligned}\overrightarrow{Mf(M)} &= \overrightarrow{Mf(N)} + \overrightarrow{f(N)f(M)} \\ &= \overrightarrow{Mf(N)} + L\left(\overrightarrow{NM}\right) \\ &= \overrightarrow{Mf(N)} + \overrightarrow{NM} \\ &= \overrightarrow{Nf(N)}\end{aligned}$$

il existe donc un certain $u \in \mathcal{E}$ tel que $\forall M \in \mathcal{E},\ f(M) = M + u$.

✓

Si $\boldsymbol{\lambda \neq 1}$

Soit $M \in \mathcal{E}$, on pose $\Omega \in \mathcal{E}$ tel que $\overrightarrow{M\Omega} = \dfrac{\overrightarrow{Mf(M)}}{1-\lambda}$

Ω est un point fixe de f :

$$\begin{aligned} f(\Omega) &= f(M + \overrightarrow{M\Omega}) \\ &= f(M) + \lambda\overrightarrow{M\Omega} \\ &= f(M) + \frac{\lambda}{1-\lambda}\overrightarrow{Mf(M)} \\ &= \Omega + \overrightarrow{\Omega M} + \overrightarrow{Mf(M)} + \frac{\lambda}{1-\lambda}\overrightarrow{Mf(M)} \\ &= \Omega - \frac{\overrightarrow{Mf(M)}}{1-\lambda} + \overrightarrow{Mf(M)} + \frac{\lambda}{1-\lambda}\overrightarrow{Mf(M)} \\ &= \Omega + \frac{-1+(1-\lambda)+\lambda}{1-\lambda}\overrightarrow{Mf(M)} \\ &= \Omega + 0 \cdot \overrightarrow{Mf(M)} \\ &= \Omega \end{aligned}$$

On a ainsi pour tout $M \in \mathcal{E}$:

$$f(M) = f(\Omega + \overrightarrow{\Omega M}) = f(\Omega) + \lambda\overrightarrow{\Omega M} = \Omega + \lambda\overrightarrow{\Omega M}$$

✓

G est alors l'image réciproque du sous-groupe $\{\lambda id_E \mid \lambda \neq 0\}$ par ϕ.

Part III
Groupes symétriques

Exercice 15. Soient E et F deux ensembles, f une bijection de E dans F, l'application

$$\left\{ \begin{array}{ccc} \mathcal{S}_E & \longrightarrow & \mathcal{S}_F \\ \sigma & \longmapsto & f^{-1} \circ \sigma \circ f \end{array} \right.$$

est un isomorphisme de groupes et elle est bien définie.

Définition 18. Soit $n \geqslant 1$, on appelle n-ième groupe symétrique, noté $\mathcal{S}_n$ le groupe $\mathcal{S}_{\{1,2,\dots n\}}$.

Proposition 9. *Soit $n \geqslant 1$, on a $|\mathcal{S}_n| = n!$*

Définition 19.

- Soient $i, j \leqslant n$ distincts, on note $(i\ j)$ la *transposition* définie par

$$\left\{ \begin{array}{ccc} i & \longmapsto & j \\ j & \longmapsto & i \\ k & \longmapsto & k, \quad \text{où } k \neq i, j \end{array} \right.$$

  Celle-ci est d'ordre 2.

- Soient $a_1, ...a_l$ distincts avec $2 \leqslant l \leqslant n$, on note $(a_1\ a_2 ... a_l)$ le *l-cycle* défini par

$$\begin{cases} a_1 & \longmapsto & a_2 \\ a_2 & \longmapsto & a_3 \\ & ... & \\ a_i & \longmapsto & a_{i+1}, \text{ où } i \leqslant k-1 \\ a_k & \longmapsto & a_1, \text{ où } k \neq i, j \end{cases}$$

Définition 20. On définit le *support* de σ par

$$supp(\sigma) = \{i \leqslant n \mid \sigma(i) \neq i\}$$

9 Propriétés de calcul élémentaires

Proposition 10. *Soient $\sigma, \omega \in \mathscr{S}_n$, si $supp(\sigma) \cap supp(\omega) = \emptyset$ alors $\sigma\omega = \omega\sigma$*

Preuve 10. Soit $x \in \{1, ...n\}$

- Si $x \notin supp(\sigma)$ et $x \notin supp(\omega)$, alors $\sigma(\omega(x)) = \sigma(x) = x$ et $\omega(\sigma(x)) = \omega(x) = x$.
- Si $x \in supp(\omega)$, alors
  - $\omega(x) \in supp(\omega)$ et donc $\omega(x) \notin supp(\sigma)$, ainsi $\sigma(\omega(x)) = \sigma(x)$
  - $\omega(\sigma(x)) = \sigma(x)$ car $\sigma(x) \notin supp(\omega)$
- Le cas où $x \in supp(\sigma)$ est symétrique

On a utilisé le fait que $\sigma(supp(\sigma)) = supp(\sigma)$, on le vérifie en rapidement : si $x \in supp(\sigma)$ alors $\sigma(x) \neq x$ et donc $\sigma(\sigma(x)) \neq \sigma(x)$ par injectivité, d'où $\sigma(x) \in supp(\sigma)$, c'est-à-dire $\sigma(supp(\sigma)) \subseteq supp(\sigma)$ et comme σ est bijective, $\sigma(supp(\sigma)) = supp(\sigma)$.

□

Proposition 11. *Soient $x_1, x_2, ...x_l$ des éléments de $\{1, ..n\}$ deux à deux distincts, alors :*

$$(x_1\ x_2)(x_2\ x_3)...(x_{l-1}\ x_l) = (x_1\ x_2\ ...\ x_l)$$

et pour tous $\sigma \in \mathscr{S}_n$: $\sigma(x_1\ x_2\ ...\ x_l)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ ...\ \sigma(x_l))$

Preuve 11. Pour toute suite d'éléments distincts $a_1, a_2, ...a_k$ et tout $i \leqslant k$, on pose $c = (a_1\ a_2\ ...\ a_i)$ et $c' = (a_i\ a_{i+1}\ ...\ a_k)$ et on a :

- $(c \circ c')(a_1) = c(a_1) = a_1$
- $(c \circ c')(a_2) = c(a_2) = a_2$

  ...
- $(c \circ c')(a_i) = c(a_{i+1}) = a_{i+1}$
- $(c \circ c')(a_{i+1}) = c(a_{i+2}) = a_{i+2}$

  ...

- $(c \circ c')(a_k) = c(a_i) = a_1$

Donc $(a_1\ a_2\ ...\ a_i)(a_i\ a_{i+1}\ ...\ a_n)$

On utilise ce résultat pour montrer par récurrence la première égalité :

$$\begin{aligned}
(x_1\ x_2)(x_2\ x_3)...(x_{l-1}\ x_l) &= (x_1\ x_2\ x_3)(x_3\ x_4)...(x_{l-1}x_l) \\
&= (x_1\ x_2\ x_3\ x_4)...(x_{l-1}\ x_l) \\
&... \\
&= (x_1\ x_2\ ...x_i)(x_i\ x_{i+1})(x_{i+1}\ x_{i+2})...(x_{l-1}\ x_l) \\
&= (x_1\ x_2\ ...\ x_{i+1})(x_{i+1}\ x_{i+2})...(x_{l-1}\ x_l) \\
&... \\
&= (x_1\ x_2\ x_3\ ...\ x_l)
\end{aligned}$$

De cette égalité on déduit la seconde, on peut facilement vérifier que pour toute transposition $(a\ b)$ on a $\sigma(a\ b)\sigma^{-1} = (\sigma(a)\ \sigma(b))$, et on en déduit immédiatement

$$\begin{aligned}
\sigma(x_1\ x_2\ ...\ x_l)\sigma^{-1} &= \sigma(x_1\ x_2)(x_2\ x_3)...(x_{l-1}\ x_l)\sigma^{-1} \\
&= \sigma(x_1\ x_2)\sigma^{-1}\sigma(x_2\ x_3)...\sigma^{-1}\sigma(x_{l-1}\ x_l)\sigma^{-1} \\
&= (\sigma(x_1)\ \sigma(x_2))(\sigma(x_2)\ \sigma(x_3))...(\sigma(x_{l-1})\ \sigma(x_l)) \\
&= (\sigma(x_1)\ \sigma(x_2)\ \sigma(x_2)\ ...\ \sigma(x_l))
\end{aligned}$$

□

Proposition 12. *Soit $c = (x_1\ x_2...x_l)$ un l-cycle, c est d'ordre l.*

Preuve 12. Soit i tel que $1 \leqslant i \leqslant l$, on montre que pour tout $0 \leqslant k \leqslant l$: $c^k(x_{1+(i \mod l)}) = x_{1+(i+k \mod l)}$

$$\begin{aligned}
c^0(x_{1+(i \mod l)}) &= x_1 \\
c^1(x_{1+(i \mod l)}) &= x_{1+(i \mod l)} = x_{1+(i+1 \mod l)} \\
&... \\
c^{k+1}(x_{1+(i \mod l)}) &= c\left(c^k(x_{1+(i \mod l)})\right) = c(x_{1+(i+k \mod l)}) = x_{1+(i+k+1 \mod l)} \\
&... \\
c^{l-1}(x_{1+(i \mod l)}) &= x_{1+(i+l-1 \mod l)} \\
\text{et } c^l(x_{1+(i \mod l)}) &= x_{1+(i+l \mod l)} = x_{1+(i \mod l)}
\end{aligned}$$

Ainsi pour tout $0 < k \leqslant l$, $c^k(x_{1+(i \mod l)}) = x_{1+(i+k \mod l)}$ et $1+(i \mod l) = 1+(i+k \mod l)$ si et seulement k est un multiple de l, donc si $k = l$, l, on a ainsi montré que le plus petit $d > 0$ vérifiant pour tout $1 \leqslant k \leqslant l$ $c^d(x_k) = x_k$ est $d = l$, donc l'ordre de c est l.

10 Décomposition en cycles

10.1 Étude

Soit $\sigma \in \mathscr{S}_n$ avec $n \geqslant n$, alors on a une action naturelle de $\langle\sigma\rangle$ sur $\{1, ...n\}$ donnée par

$$\begin{cases} \langle\sigma\rangle \times \{1, ...n\} & \longrightarrow & \{1, ...n\} \\ (g, i) & \longmapsto & g(i) \end{cases}$$

Remarque 13. $\forall i \leqslant n,\ (\langle\sigma\rangle \cdot i = \{i\} \iff i \notin supp(\sigma))$

Soit $x \in \{1, ..n\}$, on supposera que $\sigma(x) \neq x$, à quoi ressemble $\langle\sigma\rangle \cdot x$?

On note $l := \min\{d > 0 \mid \sigma^d(x) = x\}$, il existe car cet ensemble est minoré par 1 et non-vide puisqu'il contient l'odre de σ.

Exercice 16. On montre que $l \mid k$ où k est l'ordre de σ, on considère la division euclidienne de k par l :

$$k = ql + r,\ 0 \leqslant r < l$$

alors $x = \sigma^k(x) = \sigma^r(\sigma^{ql}(x)) = \sigma^r(x)$ alors par minimalité de l, on en déduit $r = 0$ et donc $l \mid k$.

L'orbite de x sous l'action de $\langle x\rangle$ est donc l'ensemble $\{x, \sigma(x), ...\sigma^{k-1}(x)\}$, en effet $x, \sigma(x), ...\sigma^{k-1}(x)$ sont tous distincts car si $i \leqslant j < l$ vérifient $\sigma^i(x) = \sigma^j(x)$ alors $\sigma^{j-i}(x) = x$ et donc $0 \leqslant j - i < l$ et par minimalité de l on déduit $j - i = 0$.

Pour conclure cette étude, on montre que les restrictions de σ et $c = (x\ \sigma(x)\ \sigma^2(x)\ ...\ \sigma^{l-1}(x))$ à $\langle\sigma\rangle \cdot x$ sont égales :

- $\sigma^i(x) \overset{\sigma}{\longmapsto} \sigma^{i+1}(x)$
- $\sigma^i(x) \overset{c}{\longmapsto} \sigma^{i+1}(x)$

10.2 Existence

Soit $\sigma \in \mathscr{S}_n$ telle que $\sigma \neq id$, $\omega_1, ...\omega_r$ une énumération ds orbites à au moins deux éléments et pour tout $i \leqslant r$ on pose $l_i := \text{Card}(\omega_i)$ et $x_i \in \omega_i$.

Remarque 14. $supp(\sigma) = \omega_1 \sqcup \omega_2 ... \sqcup \omega_r$

On note pour tout k, $c_k := (x_k\ \sigma(x_k)\ \sigma^2(x_k)\ ...\ \sigma^{l-1}(x_k))$

Pour tout $i \leqslant r$, σ et c_i coïncident sur ω_i, et pour tout $j \leqslant r$ tel que $i \neq j$, c_j et id coïncident sur ω_i, donc $c_1 \circ c_2 ... \circ c_r$ coïncide avec σ sur ω_i.

Ainsi, $c_1 \circ c_2 ... \circ c_r$ coïncide avec σ sur la réunion des orbites $\omega_1 \sqcup \omega_2 ... \sqcup \omega_r = supp(\sigma)$, de plus pour tout $x \in \{1, ...n\} \backslash supp(\sigma) : \sigma(x) = x$ et $(c_1 \circ c_2 ... \circ c_r)(x) = x$ car $x \notin \omega_1, ..\omega_r$.

10.3 Unicité

Soit $\sigma \in \mathscr{S}_n$ telle que $\sigma \neq id$ et une décomposition en cycles à supports disjoint $\sigma = c_1 \circ c_2 ... \circ c_r$, montrons que cette décomposition est la même que l'on a construit précédemment.

Pour commencer, montrons que les orbites à au moins deux éléments de σ sont les supports des cycles $c_1, c_2, ...c_r$.

Soit $i \leqslant r$, $x_i \in supp(c_i)$ et l_i sa longueur, alors pour tout $k \geqslant 0$ on a que $\sigma^k(x_i) = c_i^k(x_i)$ car les supports sont stables par application des cycles (pour tout i, j : $c_i(supp(c_j)) = supp(c_j)$, le cas $i = j$ est une conséquence d'une remarque précédente, mais si $i \neq j$ alors chaque élément de $supp(c_j)$ est laissé fixe par c_i car les supports sont disjoints) alors $\forall k \geqslant 0,\ \sigma^k(x_i) = c_i^k(x_i)$, donc $\langle\sigma\rangle \cdot x_i = \{x_i, c(x_i), ...c^{l_i-1}(x_i)\}$

Ainsi tous les supports $supp(c_1), supp(c_2) ... supp(c_r)$ sont des orbites à au moins deux éléments de l'action de $\langle\sigma\rangle$ sur $\{1, ...n\}$, et réciproquement toute orbite à au moins deux éléments est le support d'un cycle : soit x tel que $\sigma(x) \neq x$, alors nécessairement x appartient à un support $supp(c_i)$, sinon il serait laissé fixe par tous les cycles et donc par σ.

Pour finir, soient $i \leqslant r$ et $x \in supp(c_i)$, montrons que $\sigma_{|supp(c_i)} = c_{i|supp(c_i)} = (x, \sigma(x), ...\sigma^{l-1}(x))$: pour $y \in \langle\sigma\rangle \cdot x$, il existe k tel que $y = \sigma^k(x)$, alors $\sigma(y) = \sigma^{k+1}(x)$ et $\sigma(y) = (c_1 \circ c_2 .. \circ c_r)(y) = c_i(y)$ car les supports des cycles sont disjoints.

Corollaire 3.

1. *Si $\sigma \neq id$, et que sa décomposition en cycles à supports disjoints est $\sigma = c_1 \circ ...c_r$ alors l'ordre de σ est le PPCM des longueurs des cycles.*
2. *L'ensemble des transpositions engendre $\mathscr{S}_n$*

On rappelle, comme montré en TD, que dans un groupe G, si deux éléments g et g' sont tels que

- g est d'ordre fini d
- g' est d'ordre fini d'
- $\langle g\rangle \cap \langle g'\rangle = \{e\}$

alors $g \star g'$ est d'ordre $PPCM(d, d')$.

11 La signature

Soit $n \geqslant 2$, la signature ε est un homomorphisme de $\mathscr{S}_n$ dans $\{-1, 1\}$ défini par

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Elle est bien définie car

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} = \frac{\prod_{i<j} \sigma(j) - \sigma(i)}{\prod_{i<j} j - i}$$

et en notant $\varepsilon_{i,j} \in \{-1, 1\}$ le signe de $\sigma(j) - \sigma(i)$ on peut réécrire

$$\begin{aligned}
\varepsilon(\sigma) &= \frac{\prod_{i<j} \varepsilon_{i,j} |\sigma(j) - \sigma(i)|}{\prod_{i<j} j - i} \\
&= \prod_{i<j} \varepsilon_{i,j} \cdot \frac{\prod_{i<j} |\sigma(j) - \sigma(i)|}{\prod_{i<j} j - i} \\
&= \prod_{i<j} \varepsilon_{i,j} \cdot \frac{\prod_{i<j} \max(\sigma(i), \sigma(j)) - \min(\sigma(i), \sigma(j))}{\prod_{i<j} j - i}
\end{aligned}$$

et en effectuant le changement de variable $(i', j') = (\min(\sigma(i), \sigma(j)), \max(\sigma(i), \sigma(j)))$ (qui est autorisé car il définit une bijection dans l'ensemble des paires ordonnées $\{(i, j) \mid 1 \leqslant i < j \leqslant n\}$) on a enfin :

$$\begin{aligned}\varepsilon(\sigma) &= \prod_{i<j} \varepsilon_{i,j} \cdot \frac{\prod_{i<j} \max(\sigma(i), \sigma(j)) - \min(\sigma(i), \sigma(j))}{\prod_{i<j} j - i} \\ &= \prod_{i<j} \varepsilon_{i,j} \cdot \frac{\prod_{i'<j'} j' - i'}{\prod_{i<j} j - i} \\ &= \prod_{i<j} \varepsilon_{i,j} \in \{-1, 1\}\end{aligned}$$

Proposition 13. *Si $n \geqslant 2$, alors*

- *Si $\tau = (a\ b)$ est une transposition, (on peut supposer $a < b$), alors*

$$\varepsilon(\tau) = \prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i} = 1 \cdot 1 \cdot ... \cdot \underbrace{\frac{\tau(b) - \tau(a)}{b - a}}_{\frac{a-b}{b-a} = -1} \cdot 1 \cdot ... \cdot 1 = -1$$

- *ε est l'unique homomorphisme non trivial de $\mathscr{S}_n$ dans $\mathbb{C}^\times$*

en effet $\mathscr{S}_n$ est engendré par les transpositions alors tout homomorphisme sur ce groupe est déterminé par la valeur qu'il prend sur les transpositions.

Toutes les transpositions sont conjuguées, alors et pour toutes permutations σ, ω et tout homomorphisme $\varphi : \mathscr{S}_n \longrightarrow \{-1, 1\}$:

$$\varphi(\sigma \circ \omega \circ \sigma^{-1}) = \varphi(\sigma)\varphi(\omega)\varphi(\sigma)^{-1} = \varphi(\omega)$$

Ainsi, si φ vaut 1 sur une (et donc toutes) les transpositions, alors sachant que toute permutation se décompose en produit de transpositions, ε vaut 1 sur toute permutation. Si au contraire elle vaut -1 sur une (et donc toutes) les transpositions, alors elle est égale à la signature.

Définition 21. Soit $n \geqslant 2$, on appelle *n-ième groupe alterné* $\mathcal{A}_n$ le noyau de la signature.

Proposition 14.

1. *Si $l \geqslant 2$ et σ est un l -cycle, alors $\varepsilon(\sigma) = (-1)^{l-1}$.*
2. *Soit $\sigma \in \mathscr{S}_n$ et $\sigma = c_1 \circ ...c_r$ une décomposition en cycles à supports disjoints de longueurs $l_1, l_2, ...l_r$, alors $\varepsilon(\sigma) = (-1)^{l_1+l-1+...l_r-r}$.*

   Et en considérant chaque l_i comme le cardinal d'une orbite non-ponctuelle de l'opération, sachant $n = l_1 + l_2 + ... + l_r + f$ où f est le nombre de points fixes, alors $l_1 + l_2 + ...l_r - r = n - (f + r)$ et donc $\varepsilon(\sigma) = (-1)^{n-(f+r)}$ et comme $f + r = Card\left(\langle\sigma\rangle \backslash [n]\right) := o$ alors $\varepsilon(\sigma) = (-1)^{n-o}$
3. *$\mathcal{A}_5$ est constitué de :*

- *id (1 élément)*
- *doubles transpositions* ($\binom{5}{2}\binom{3}{2}/2 = 15$ *éléments)*
- *de 3-cycles (20)*
- *de 5-cycles (24)*

4. *Card*$(\mathcal{A}_n) = \frac{(n-1)!}{2}$ *car* $\mathscr{S}_n = \mathcal{A}_n \sqcup (1\ 2) \circ \mathcal{A}_n$*, ou bien car* $_{\ker \varepsilon}\backslash\mathscr{S}_n$ *est en bijection avec* $Im(\varepsilon)$

Part IV
Sous-groupes distingués et groupes quotient

12 Sous-groupes distingués

Proposition 15. *Soit* $(G, \star)$ *un groupe et* $G \leqslant G$*, les conditions suivantes sont équivalentes :*

1. $\forall g \in G,\ gH = Hg$
2. $\forall g \in G,\ gHg^{-1} \subseteq H$
3. $\forall g \in G,\ gHg^{-1} = H$

Définition 22. On dit que H est *distingué dans* G, noté $H \lhd G$ si :$\forall g \in G,\ gHg^{-1} = H$.

Exemple 16.

1. Si g est abélien, $H \lhd G$
2. $\{e\} \lhd G$
3. $Z(G) \lhd G$

Proposition 16. *Si* H *est le noyau d'un homomorphisme de groupe défini sur* G*, alors* $H \lhd G$.

En effet φ est un homomorphisme tel que $H = \ker\varphi$, pour tout $h \in H$ et tout $g \in G$, $\varphi(g \star h \star g^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e$, donc $gHg^{-1} = H$.

Exemple 17.

- $\mathcal{A}_n \lhd \mathscr{S}_n$
- $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$
- $SO_n(\mathbb{R}) \lhd O_n(\mathbb{R})$
- $SU_n(\mathbb{C}) \lhd U_n(\mathbb{C})$

13 Groupes quotients

On note $\pi : G \longrightarrow G/H$ la surjection canonique.

Proposition 17. *On suppose $H \lhd G$, alors il existe une et une seule loi de composition interne $*$ sur G/H telle que G/H est un groupe pour cette loi et que π soit un homomorphisme de groupes de G dans G/H*

Exercice 17. S'il existe une loi $*$ de G/H vérifiant les proposition précédentes soient vraies, alors $H \lhd G$.

Remarque 15.

- $H = \pi(e)$ est l'élément neutre de G/H
- $\ker \pi = H$

Corollaire 4. *$H \lhd G$ si et seulement s'il existe un homomorphisme de groupes de domaine G tel que $H = \ker \varphi$*

Exemple 18.

Exercice 18. Soit $n \in \mathbb{Z}$ il existe une application bijective $\varphi : \mathbb{U}_n \longrightarrow \mathbb{Z}/n\mathbb{Z}$ telle que $\varphi(e^{\frac{2ik\pi}{n}}) = \overline{k}$, c'est alors un homomorphisme de groupes et donc un isomorphisme, et sa bijection réciproque ψ est définie par $\psi(\overline{k}) = e^{\frac{2ik\pi}{n}}$.

Exemple 19.

- Soit $n \geqslant 2$, $\mathcal{A}_n \lhd \mathscr{S}_n$ et $\mathscr{S}_n/\mathcal{A}_n \cong \mathbb{Z}/n\mathbb{Z}$
- Soit $n \geqslant 1$, $SO_n(\mathbb{R}) \lhd O_n(\mathbb{R})$ et $O_n(\mathbb{R})/SO_n(\mathbb{R}) = \{\text{classes de } I_n \text{ et classes de } diag(-1, 1, ...1)\}$

Exercice 19. Soit $K = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ est un sous-groupe de $\mathcal{A}_4$ et c'est une réunion de classes de conjugaisons.

L'ensemble quotient est de cardinal 3, donc $\mathcal{A}_4/K \cong \mathbb{U}_3$

14 Passage au quotient des homomorphismes

Théorème 7. *Soient deux groupe $(G, \star)$ et $(G', \star)$, $H \lhd G$ et φ un homomorphisme de groupes de G dans G'.*
Si $H \subseteq \ker \varphi$ alors il existe un unique homomorphisme $\psi : G/H \longrightarrow G'$ tel que $\psi \circ \pi = \varphi$

Preuve 13. **Unicité**
Soient $\psi, \psi' : G/H \longrightarrow G'$ deux homomorphismes tels que $\psi \circ \pi = \psi' \circ \pi = \varphi$
Soit $x \in G/H$, il existe $g \in G$ tel que $pi(g) = x$ par surjectivité de π alors $\psi(x) = \psi(\pi(g)) = \varphi(g)$
(TODO) ✓

On vérifie que φ est constante sur les classes d'équivalence de $\sim$ définie par $\forall g, g' \in G,\ \exists h \in H\ :\ g' = gh$
Donc $\varphi(g') = \varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$
Il existe donc $psi : G/H \longrightarrow arG'$ telle que $\psi \circ \pi = \varphi$.
On vérifie que ψ est un homomorphisme de groupes :
Soient $x, x' \in G/H$ il existe $g, g' \in G$ tels que $x = \pi(g)$ et $x' = \pi(g')$
Alors $xx' = \pi(g)\pi(g') = \pi(gg')$ donc $\psi(xx') = \psi(\pi(gg')) = \varphi(gg') = \varphi(g)\varphi(g') = \psi(x)\psi(x')$ ✓

Propriété 7. *Soient deux groupes G et G', H un sous-groupe distingué de G et f un homomorphisme de G dans G' tel que $H \subseteq \ker f$, alors il existe un unique homomorphisme φ de G/H dans G' tel que $\varphi \circ \pi = f$.*
De plus $Im(f) = Im(\varphi)$ et $\ker \varphi = \ker f/H$.

Corollaire 5.

1. *Il existe un unique homomorphisme injectif* $\varphi : G/_{\ker f} \longrightarrow G'$ *tel que* $\varphi \circ \pi = f$.
2. *Les groupes* $G/_{\ker f}$ *et* $Im(f)$ *sont isomorphes.*
3. *Si de plus,* f *est surjective, alors* f *induit un isomorphisme de groupes* $\varphi : G/_{\ker f} \longrightarrow G'$ *tel que* $\varphi \circ \pi = f$.

Exercice 20. Soit $g \in GL_n(\mathbb{R})$, si pour tout $u \in \mathbb{K}^n \setminus \{0\}$ on a que gu est proportionnel à u, alors il existe $\lambda \neq 0$ tel que $g = \lambda I_n$.

Définition 23. Soit $H = \{\lambda I_n \mid \lambda \neq 0\} \leqslant GL_n(\mathbb{K})$, on note le groupe projectif linéaire

$$PGL_n(\mathbb{K}) = GL_n(\mathbb{K})/_H$$

15 Un théorème d'isomorphisme

Théorème 8. *Soit* G *un groupe,* H *et* K *des sous-groupes distingués de* G *tels que* $K \subseteq H$*, alors*

1. $K \lhd H$
2. $H/_K \lhd G/_K$
3. *Les groupes* $(G/_K)/_{(H/_K)}$ *et* $G/_H$ *sont isomorphes.*

Preuve 14.

1. $\begin{cases} K \lhd G \text{ donc } K \lhd H \\ K \subseteq H \end{cases}$
2. $H/_K = \{hK \mid h \in H\} \subseteq \{gK \mid g \in G\} = G/_K$
   On note π_K la surjection canonique de G dans $G/_K$, on vérifie que $\forall \alpha \in G/_K, \forall \beta \in H/_K,\ \alpha\beta\alpha^{-1} \in H/_K$
   alors $\alpha\beta\alpha^{-1} = \pi_K(g)\pi_K(h)\pi_K(g)^{-1} = \pi_K(ghg^{-1}) \in H/_K$ (car $H/_K = \pi_K(H)$)
   Donc $H/_K \lhd G/_K$
3. On note $\pi : G/_K \longrightarrow (G/_K)/_{(H/_K)}$ la surjection canonique, $\pi \circ \pi_K = f : G \longrightarrow (G/_K)/_{(H/_K)}$
   f est surjective comme composée d'applications surjectives.
   f est une composée d'homomorphismes de groupes, donc c'est un homomorphisme de groupes.
   On vérifie que $H = \ker f$
   $\boldsymbol{H \subseteq \ker f}$ Soit $h \in H$, alors $f(h) = \pi(\pi_K(h))$, or $\pi_K(h) \in \pi_K(H) = H/_K = \ker pi$, donc $f(h) = e$. ✓
   $\boldsymbol{\ker f \subseteq H}$ Soit $g \in \ker f$, donc $e = \pi(\pi_K(g))$ et donc $\pi_K(g) \in \ker \pi = H/_K = \pi_K(H)$.
   Ainsi, il existe $h \in$ tel que $\pi_K(g) = \pi_K(h)$, en particulier $\pi_K(g^{-1}h) = e$, donc $g^{-1}h \in \ker \pi_K = K \subseteq H$ car $h \in h$. ✓

Exemple 20. $G = \mathbb{Z}$, $m, n \in \mathbb{Z}$ tels que $m|n$ et $H = m\mathbb{Z}$ et $K = n\mathbb{Z}$
On a $K \subseteq H$, alors $\mathbb{Z}$ tant abélien on a $H \lhd G$ et $K \lhd G$, alors

$$\mathbb{Z}/_{m\mathbb{Z}} \simeq (\mathbb{Z}/_{n\mathbb{Z}})/_{(m\mathbb{Z}/_{n\mathbb{Z}})}$$

Part V
Théorème de Sylow

16 Théorèmes de Sylow

Théorème 9. *Soit G un groupe d'ordre fini et p un entier premier divisant l'ordre de G. Soit H un sous-groupe de G d'ordre une puissance de p alors il existe un sous-groupe p-Sylow de G contenant H.*

En particulier, il existe un sous-groupe p-Sylow dans G.

Remarque 16. Si H est un sous-groupe p-Sylow et si $g \in G$ alors gHg^{-1}est un sous-groupe p-Sylow de G.

L'opération de G sur ses sous groupes p-Sylow définie par $g \cdot H = gHg^{-1} =^g H$ est une opération de groupe.

Théorème 10. *Soit G un groupe fini d'ordre $p^\alpha m$ avec p un diviseur premier de CardG, on note n_p le nombre de sous-groupes p-Sylow de G, alors*

- *L'opération par conjugaison de G sur l'ensemble de ses sous-groupes est transitive, donc $n_p | p^\alpha m$*
- *$n_p \equiv 1 \mod p$ et $n_p | m$*

Corollaire 6.

- *Si $n_p = 1$ alors l'unique p-Sylow de G est distingué*
- *Si au moins un sous-groupe p-Sylow est distingué dans G, alors il est l'unique p-Sylow de G*

TODO: montrer (1) à l'aide de l'action de G sur ses p-Sylow

Exemple 21. On considère $\mathcal{A}_4$, ses sous-groupes 2-Sylow sont d'ordre 4, et leur nombre n_2 vérifie :

$$\begin{cases} n_2 \equiv 1[2] \\ n_2 | 3 \end{cases}$$

donc $n_2 \in \{1, 3\}$.

Si S est un 2-Sylow et $\sigma \in S$, alors σ est d'ordre 1, 2 ou 4, or les 4-cycles ne sont pas de signature pair, donc S contient l'identité et les doubles transpositions.

Il n'existe donc q'un seul 2-Sylow, c'est le sous-groupe de Klein.

Remarque 17. Si un groupe H est une réunion de classes de conjugaison de G, alors il est distingué.

Exemple 22. On considère $\mathcal{A}_4$, ses sous-groupes 3-Sylow sont d'ordre 3, et leur nombre n_3 vérifie :

$$\begin{cases} n_3 \equiv 1[3] \\ n_2 | 4 \end{cases}$$

donc $n_3 \in \{1, 4\}$.

Or $\langle (1\ 2\ 3) \rangle$ et $\langle (1\ 2\ 4) \rangle$ sont des 2-Sylow, donc $n_3 = 4$.

Exemple 23. On considère $\mathscr{S}_4$ et on pose n_2 le nombre de sous-groupes 2-Sylow; $n_2 \in \{1, 3\}$ les sous-groupes 2-Sylow sont d'ordre 8.

Dans un sous-groupe d'ordre 8 on peut trouver :

- ordre 1 : L'identité

- ordre 2 : Les transpositions et les doubles-transpositions

- ordre 4 : Les 4-cycles

- ordre 8 : Aucun

Soit $S := \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4) \rangle$, S contient les 3 doubles transpositions, l'identité, (1 2 3 4) et (1 4 3 2), donc au moins 6 éléments.

$|S|$ est un multiple de 4, donc $|S| \in \{4, 8, 12, 24\}$. On peut éliminer 4 et 24, $|S| \in \{8, 12\}$

De plus, en considérant l'action de conjugaison de $\mathscr{S}_4$ sur l'ensemble de ses sous-groupes, on obtient que le stabilisateur de $H = \langle (1\ 2\ 3\ 4) \rangle$ est de cardinal 8.

Enfin, $H = S$, en effet les générateurs de S sont dans le stabilisateur, d'où $H \subseteq S$, et on conclut par un argument de cardinalité.

Exercice 21.

1. Décrire tous les sous-groupes de $\mathcal{A}_4$ et pour chacun décrire son stabilisateur pour l'opération de conjugaison
2. De même pour S_4.

Part VI
Solutions des exercices

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

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

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

$$\dots$$

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

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

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

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

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

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

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

Solution de l'exercice 11 φ est non-nulle alors il existe $u_0 \in V$ tel que $\varphi(u_0) \neq 0$, on pose $u_1 = \frac{u_0}{\varphi(u_0)}$ afin d'avoir $\varphi(u_1) = 1$.

Montrons $\mathcal{F} = \{M \in V \mid \varphi(M) = 1\} = u_1 + \ker \varphi$.

$u_1 + \ker \varphi = \{w = u_1 + v \mid v \in \ker f\}$

$u_1 + \ker \varphi = \{w = u_1 + v \mid \varphi(v) = 0\}$

$u_1 + \ker \varphi = \{w = u_1 + v \mid \varphi(w - u_1) = 0\}$

$u_1 + \ker \varphi = \{w \in V \mid \varphi(w - u_1) = 0\}$

$u_1 + \ker \varphi = \{w \in V \mid \varphi(w) = \varphi(u_1) = 1\}$

$u_1 + \ker \varphi = \mathcal{F}$

Solution de l'exercice 12 Soient $X, Y \in \mathcal{E}$

$$u \in F \iff X + u \in X + F$$

$$u \in F \iff X + u \in Y + G$$

$$u \in F \iff \exists v \in G \ : \ X + u = Y + v$$

$$u \in F \iff \exists v \in G \ : \ Y + (v - u) = X \in X + F = Y + G$$

$$u \in F \iff (v - u) \in G$$

$$u \in F \iff u \in G$$