Rapport de leçon pour le Master

# Groupe opérant sur un ensemble, exemples et applications.

Xavier Arhan et Arthur CHASSANIOL

le 01 avril 2012

# Table des matières

# 1 Définitions et premières propriétés

## 1.1 Actions de groupe

**Définition 1.1.1.** Soient $G$ un groupe noté multiplicativement, $X$ un ensemble et $\mathfrak{S}(X)$ l'ensemble des permutations de cet ensemble. Une action du groupe $G$ sur $X$ est la donnée d'une application :

$$\begin{aligned} \phi : G \times X &\to X \\ (g, x) &\mapsto g.x \end{aligned}$$

avec les propriétés suivantes :
– $\forall x \in X, e.x = x$, où $e$ est le neutre de $G$.
– $\forall g, g' \in G, \forall x \in X, g.(g'.x) = (gg').x$.
Ce qui correspond à la donnée d'un morphisme :

$$\varphi : G \to \mathfrak{S}(X)$$

On dit alors que $G$ agit sur $X$, ou que $X$ est un $G$-ensemble.

Remarquons alors que si $H$ est un sous-groupe de $G$, $H$ agit sur $X$ par restriction du morphisme $\varphi$ à $H$.

**Exemple 1.1.2.**

- action de $G$ sur $G$ et $G/H$ par translation,
- action de $G$ sur $G$ et $\mathfrak{P}(G)$ (ensemble des sous-groupes de $G$) par conjugaison,
- action de $S_n$ sur les groupes à $n$ éléments...

On introduit alors les notions de stabilisateur, d'orbite et d'ensemble des points fixes :

**Définition 1.1.3.**

- On définit l'orbite d'un élément $x$ de $X$ par :

$$O_x = \{g.x \mid g \in G\}.$$

- On définit le stabilisateur d'un élément $x$ de $X$ dans $G$ par :

$$Stab_G(x) = \{g \in G \mid g.x = x\}.$$

- On définit l'ensemble des points fixés par un élément $g$ de $G$ par :

$$Fix_X(g) = \{x \in X \mid g.x = x\}.$$

On notera également $X^G$ l'ensemble des éléments ayant une orbite ponctuelle. On a alors :

$$X^G = \bigcap_{g \in G} Fix_X(g).$$

Un rapide calcul donne alors une relation sur les stabilisateurs d'éléments d'une même orbite : Si $y = g.x$ alors

$$Stab_G(y) = g.Stab_G(x).g^{-1}.$$

De plus si $\varphi : G \to \mathfrak{S}(X)$ définie une action de groupe on a :

$$Ker(\varphi) = \bigcap_{x \in X} Stab_G(x).$$

**Exemple 1.1.4.**

- En considérant l'action par conjugaison de $G$ sur $G$, les orbites sont les classes de conjugaison.
- En particulier, quand $G = S_n$, les orbites sont les différents types de décomposition en cycles à supports disjoints des éléments de $S_n$.

On va maintenant rajouter un peu de vocabulaire, histoire de caractériser les différentes actions de groupe.

**Définition 1.1.5.**

- Une action de groupe est dite **transitive** si elle possède une seule orbite. Autrement dit, deux éléments quelconques de $X$ peuvent être envoyés l'un sur l'autre par l'action d'un élément du groupe : $\forall x, y \in X, \exists g \in G \ / \ y = g.x$.
- Une action de groupe est dite **simplement transitive** si elle est transitive et qu'on a unicité du $g$, i.e. : $\forall x, y \in X, \exists! g \in G \ / \ y = g.x$
- Une action de groupe est dite $n$**-transitive** si :
  $\forall x_1, \dots x_n, y_1, \dots y_n \in X, \exists g \in G \ / \ y_1 = g.x_1, \dots y_n = g.x_n$.
- Une action de groupe est dite **fidèle** si l'intersection de tous les stabilisateurs est réduite au neutre, autrement dit si le morphisme $\varphi$ est injective.

**Exemple 1.1.6.**

- Si $E$ est un espace vectoriel de dimension finie, le groupe général linéaire $GL(E)$ agit simplement transitivement sur l'ensemble des bases de $E$.
- Si $G$ est un groupe fini ($|G| = n \in \mathbb{N}$), alors $G$ agit fidèlement-transitivement sur $G$ par multiplication à gauche.
- $S_n$ (respectivement $A_n$) agit $n$-transitivement (resp. $(n-2)$-transitivement) sur $\{1, ..., n\}$.

Applications :

**Proposition 1.1.7** (Théorème de de Cayley)**.** *: Tout groupe fini $G$ de cardinal $n$ est isomorphe à un sous-groupe de $S_n$.*

*Démonstration.* En effet on considère l'action de $G$ sur lui même par multiplication à gauche, ce qui nous donne un morphisme $\varphi : G \to \mathfrak{S}(G)$ or, via une bijection entre $G$ et $\{1, \ldots, n\}$, on a $\mathfrak{S}(G) \simeq S_n$. De plus l'action est fidèle car si $g_1 g = g$ alors $g_1 = e$ donc on obtient un morphsime injectif de $G$ dans $S_n$ ce qui permet de conclure. □

**Proposition 1.1.8.** *Pour $n \geq 5$ les 3-cycles sont conjugués dans $A_n$.*

*Démonstration.* Soit $(a, b, c)$ et $(a', b', c')$ deux 3-cycles de $A_n$. $A_n$ agit $(n-2)$-transitivement sur $\{1, ..., n\}$ or $n \geq 5$ donc $n - 2 \geq 3$, ainsi il existe $\sigma \in A_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(c) = c'$. On remarque alors que $\sigma(a, b, c)\sigma^{-1} = (a', b', c')$, ce qui permet de conlure. □

**Remarque 1.1.9.** Cette proposition est notamment utile pour montrer que $A_n$ est simple pour $n \geq 5$.

## 1.2 Formule des classes et lemme de Burnside

En considérant la relation d'équivalence $R$ :

$$xRy \iff \exists g \in G \text{ tq } x = g.y,$$

les orbites sont alors les classes d'équivalences pour $R$ : les éléments de l'ensemble quotient qu'on notera $X/G$.

**Proposition 1.2.1.** *Soit $x \in X$, l'application :*

$$f : G/Stab_G(x) \to O_x$$

$$g \mapsto g.x$$

*est bien définie et est une bijection.*

*Démonstration.* Soient $g_1, g_2 \in G$ tels que $g_1 = g_2 g$ avec $g \in Stab_G(x)$, alors $g_1.x = (g_2 g).x = g_2.(g.x) = g_2.x$ donc $g.x$ ne dépend pas de la classe de $g$ modulo $Stab_G(x)$ et $f$ est bien définie. De plus $g_1.x = g_2.x$ implique que $g_2^{-1} g_1 \in Stab_G(x)$ donc $f$ est injective. Et par définition de $O_x$ elle est surjective. C'est donc bien une bijection. □

**Corollaire 1.2.2.** *Soir $G$ un groupe fini, $\forall x \in X$ :*

$$|G| = |O_x| \times |Stab_G(x)|$$

On a alors la proposition suivante, dite "formule des classes" :

**Proposition 1.2.3.**

$$|X| = \sum_{\omega \in X/G} |\omega| = |X^G| + \sum_{|\omega| \geq 2} |\omega|$$

*Démonstration.* Il suffit en effet de remarquer que les éléments d'orbites ponctuelles sont exactements ceux de $X^G$ et que les orbites sont disjointes car la relation $R$ est une relation d'équivalence. □

**Corollaire 1.2.4.** *Soit $G$ un $p$-groupe, on a :*

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

*Démonstration.* En effet si $x \in \omega$ alors $|\omega| = |O_x|$ divise $G$ donc si $G$ est un $p$-groupe et $|\omega| \geq 2$ alors $|\omega| \equiv 0 \mod p$. □

Applications :

**Théorème 1.2.5** (de Wedderburn)**.** *Tout corps fini est commutatif.*

*Démonstration.* Soit $K$ un corps fini de cardinal $p^\alpha$. On note $Z = \{a \in K \mid \forall x \in K \ ax = xa\}$ le centre de $K$.

- $Z$ est un sous-corps de $K$ non trivial de cardinal $q \geq 2$, car $0, 1 \in Z$.
- $K$ est naturellement un $Z$-espace vectoriel fini avec $Z$ commutatif donc $|K| = g^n$, $n \in \mathbb{N}^*$.

Le but à présent est de montrer que $n = 1$ pour conclure. On suppose donc $n > 1$. $K^*$ agit sur lui même par conjugaison et on note $\omega(x)$ l'orbite de $x$ sous cette action et $k_x = \{y \in K \mid yx = xy\} = Stab_{K^*}(x) \cup \{0\}$.

- $k_x$ est un corps contenant $Z$ donc une extension de $Z$, ainsi $|k_x| = q^{d_x}$.
- $|Stab_{K^*}|$ divise $|K^*|$ donc $q^{d_x} - 1 | q^n - 1$ ce qui implique que $d_x | n$ (car une puissance $d_x$-ième de l'unité est une puissance $n$-ième de l'unité si et seulement si $\frac{n}{d_x} \in \mathbb{N}$ i.e. $d_x | n$).
- Ainsi en utilisant le fait que $X^n - 1$ est le produit des polynômes cyclotomiques $\phi_m$ pour $m$ divisant $n$ :

$$|\omega(x)| = \frac{|K^*|}{k_x^*} = \frac{q^n - 1}{q^{d_x} - 1} = \prod_{m|n, m\nmid d} \phi_m(q).$$

Si $|\omega(x)| \geq 2$ cela signifie que $d_x \neq n$ et donc que $\phi_n(q)$ divise $|\omega(x)|$. En utilisant la formule des classes on obtient :

$$|K^*| = |Z^*| + \sum_{|\omega(x)|\geq 2} |\omega(x)|,$$

i.e :

$$q^n - 1 = q - 1 + \sum_{|\omega(x)|\geq 2} |\omega(x)|.$$

Donc par ce qui précède on obtient que $\phi_n(q)|q-1$ ce qui implique $\phi_n(q) \leq q-1$. Montrons que ceci n'est pas possible : $\phi_n(q) = (q-\xi_1)\cdots(q-\xi_r)$ où les $\xi_i$ sont les racines primitives $n$-ième de l'unité. $|\xi_i| = 1$ et $\xi_i \neq 1$ car $n > 1$ par hypothèse. Ainsi on voit graphiquement que $|q - \xi_i| > |q-1|$ donc :

$$|\phi_n(q)| > (q-1)^r \geq q-1,$$

absurde. □

**Proposition 1.2.6** (Lemme de Burnside)**.**

$$|X/G| = \frac{1}{|G|} \sum_{g\in G} |Fix_X(g)|$$

*Démonstration.* Soit $A = \{(g,x) \in G \times X \mid g.x = x\}$. On a alors deux façons de compter le nombre d'éléments de $A$ :

$$|A| = \sum_{g\in G} |Fix_X(g)| = \sum_{x\in X} |Stab_G(x)|,$$

ainsi

$$\begin{aligned}\sum_{g\in G} |Fix_X(g)| &= \sum_{\omega\in X/G} \sum_{x\in\omega} |Stab_G(x)| = \sum_{\omega\in X/G} \sum_{x\in\omega} \frac{|G|}{|O_x|} \\ &= \sum_{\omega\in X/G} |G| \sum_{x\in\omega} \frac{1}{|\omega|} = \sum_{\omega\in X/G} |G| = |G| \times |X/G|.\end{aligned}$$

□

**Proposition 1.2.7** (Cauchy)**.** *Soient $G$ un groupe fini et $p$ un entier premier qui divise le cardinal de $G$, alors il existe $g \in G$ d'ordre $p$.*

*Démonstration.* On est ramené au cas où $G$ est un $p$-groupe grâce à l'existence d'un $p$-Sylow que nous verrons au théorème 2.3.2. Soit $G$ de cardinal $p^\alpha$. On pose $F = \{(g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \ldots g_p = e\}$, $\sigma = (1, 2, \ldots, p) \in S_p$ et $H = \langle \sigma \rangle$. $|F| = |G|^{p-1} = p^{\alpha(p-1)}$ car pour tout $(g_1, \ldots, g_{p-1}) \in G^{p-1}$ le $p$-uplet $(g_1, \ldots, g_{p-1}, (g_1 \ldots g_{p-1})^{-1})$ est dans $F$, $|H| = ordre(\sigma) = p$ et $H$ agit sur $F$ via :

$$\sigma.(g_1, \ldots, g_p) = (g_{\sigma(1)}, \ldots, g_{\sigma(p)}) = (g_2, \ldots, g_p, g_1) \in F.$$

Regardons les éléments de $F$ d'orbite ponctuelle sous l'action de $H$. $(g_1, \ldots, g_p) \in F^H$ est équivalent à $g_1 = g_2 = g_3 = \cdots = g_p$, i.e. :

$$F^H = \{(g, g, \ldots, g) \mid g^p = e\}.$$

D'après le corollaire 1.2.4 on a :

$$|F^H| \equiv |F| \mod p,$$

donc $|F^H| \equiv 0 \mod p$, or $(e, \ldots, e) \in F^H$ donc $|F^H| \geq 2$ ce qui signifie qu'il existe un élément $g \in G$ tel que $g^p = e$ et $g \neq e$, $g$ est donc un élément d'ordre $p$ dans $G$. □

# 2 Applications à la théorie des groupes

## 2.1 Action par conjugaison

**Définition 2.1.1** (Centre)**.** Un groupe $G$ agit sur lui-même par conjugaison et on note $Z(G) = \{g \in G \mid \forall h \in G,\ h.g.h^{-1} = g\}$ l'ensembles des points fixes de cette action, appelé centre de $G$.

**Remarque 2.1.2.** Il s'agit de l'ensemble des éléments qui commutent avec tous les éléments du groupe.

**Proposition 2.1.3.** *Si $G$ est un $p$-groupe alors $|Z(G)| \equiv 0$ $[p]$.*

*Démonstration.* $G$ agit sur $G$ par conjugaison, en appliquant la formule des classes pour les $p$-groupe cela donne imédiatement le résultat. □

Applications :

**Proposition 2.1.4.** *Soit $p$ un entier premier, si $|G| = p^2$ alors $G$ est abélien.*

*Démonstration.* On considère l'action de $G$ sur $G$ par conjugaison. Par la proposition 2.1.3 on obtient $|Z(G)| = 0$, $p$ ou $p^2$. 0 est exclu car $e \in Z(G)$. Supposons que $|Z(G)| = p$ : Soit $x \notin Z(G)$. $x \cup Z(G) \subset Stab_G(x)$, ainsi $|Stab_g(x)| \geq p + 1$, or $|Stab_G(x)|$ divise $|G|$ donc $Stab_G(x) = G$ ce qui signifie que $x \in Z(G)$, absurde. On vient donc de montrer que $Z(G) = G$, donc $G$ est abélien. □

**Proposition 2.1.5.** *Soit $G$ un groupe d'ordre $p^\alpha$, $p$ premier et $\alpha \in \mathbb{N}^*$. Alors $G$ contient des sous-groupes d'ordre $p^i$, $\forall i \leq \alpha$.*

*Démonstration.* Le cas $\alpha = 1$ est trivial (le cas $\alpha = 2$ est immédiat en utilisant le théorème de Cauchy). On suppose le résultat vrai pour $\alpha \leq k$ ($k \geq 1$). Soit $G$ un groupe d'ordre $p^{k+1}$. Le but est de trouver un sous-groupe propre et distingué $F$ de $G$ non trivial. Si $G$ est abélien on prend $F = \langle g \rangle$ où $g$ est un élément d'ordre $p$ dans $G$ (existe par Cauchy). Si $G$ non abélien on prend $F = Z(G)$ qui est non trivial d'après la proposition 2.1.3. Ainsi on a un sous-groupe distingué de $G$ de cardinal $p^\beta$ avec $1 \leq \beta \leq k$. Soit $i \in [\![0, k+1]\!]$ :

- Si $i \leq \beta$ par hypothèse de recurrence $F$ possède un sous-groupe d'ordre $p^i$, a fortiori c'est le cas pour $G$ aussi.
- Si $i > \beta$, $L = G/F$ est un groupe car $F \lhd G$ et $|L| = p^{k+1-\beta}$. $\beta \geq 1$ donc de nouveau par hypothèse de recurrence il existe $L_i$ sous-groupe de $L$ avec $|L_i| = p^{i-\beta}$. $L_i = \{g_j F \mid j \in [\![1, p^{i-\beta}]\!]\}$ avec $g_1 = e$, $g_j \in G \setminus F$ pour $j \geq 2$ et les $g_j$ tous distincts. En utilisant la bijection entre les sous-groupe de $G/F$ et ceux de $G$ contenant $F$ le sous groupe de $G$ associé à $L_i$ est $G_i = \{g_j f \mid f \in F, j \in [\![1, p^{i-k}]\!]\}$ qui est de cardinal $|F|p^{i-k} = p^i$.

□

**Remarque 2.1.6.** En utilisant le théorème 2.3.2 on obtient donc que tout groupe de cardinal $p^\alpha m$, ($p$ premier et premier avec $m$), possède des sous-groupes d'ordres $p^i$, $\forall i \leq \alpha$.

## 2.2 Action par multiplication à gauche

**Proposition 2.2.1.** *Soit $G$ un groupe et $H$ un sous-groupe de $G$. $G$ agit transitivement sur $G/H$ par multiplication à gauche. De plus si $\varphi$ est le morphisme associé à cette action on a :*

$$\ker \varphi = \bigcap_{g \in G} gHg^{-1},$$

*qui est le plus grand sous-groupe distingué de $G$ contenu dans $H$.*

*Démonstration.* $\varphi : G \to \mathfrak{S}(G/H)$ :

$$x \in \ker \varphi \iff \forall g \in G,\ xgH = gH \iff \forall g \in G,\ x \in gHg^{-1},$$

ainsi on a bien $\ker \varphi = \bigcap_{g \in G} gHg^{-1}$. De plus $\ker \varphi$ est distingué dans $G$, en tant que noyau de morphisme, et $\ker \varphi \subset H$ (prendre $g = e$ dans l'intersection). On considère maintenant $N$ un sous-groupe distingué de $G$ contenu dans $H$. Soit $x \in N$. $N \lhd G$ donc $\forall g \in G,\ g^{-1}xg \in A \subset H$. Cela signifie que $\forall g \in G,\ x \in gHg^{-1}$ et par suite $x \in \ker \varphi$ donc $N \subset \ker \varphi$. □

Appplications :

**Proposition 2.2.2.** *Si $H$ est d'indice fini dans $G$ infini, alors $G$ n'est pas simple.*

*Démonstration.* L'action de $G$ sur $G/H$ par multiplication à gauche nous donne un morphisme $\varphi : G \to \mathfrak{S}(G/H) \simeq S_n$.

- Si $\ker \varphi = \{e\}$, absurde car $G$ infini.
- Si $\ker \varphi = G$, absurde car l'action n'est pas trivial.

Donc finalement $\ker \varphi$ est un sous-groupe propre non trivial de $G$ et distingué, ce qui implique que $G$ n'est pas simple. □

**Proposition 2.2.3.** *Soit $p$ le plus diviseur premier de $|G|$, tout sous-groupe d'indice $p$ dans $G$ est distingué.*

*Démonstration.* Soit $H$ d'indice $p$ dans $G$. La proposition 2.2.1 nous donne $N = \bigcap_{g\in G} gHg^{-1} \lhd G$ et $N \subset H$. De plus $G/N$ est isomorphe à un sous-groupe de $\mathfrak{S}(G/H) \simeq S_p$ (voir le morphisme dont $N$ est le noyau). Ainsi $|G/N| \mid p!$ et $|G/N| \mid n$ donc $|G/N| \mid pgcd(p!, n) = p$. Donc $N$ est d'indice $p$ dans $G$ or $N \subset H$ donc $H = N$ et ainsi $H$ est bien distingué dans $G$. □

## 2.3 Théorèmes de Sylow

**Définition 2.3.1.** Soit $G$ un groupe fini. Un $p$-Sylow de $G$ est un $p$ sous-groupe de $G$ d'indice premier avec $p$ (i.e un $p$ sous-groupe d'ordre maximal).

**Théorème 2.3.2.** *Soit $G$ un groupe de cardinal $p^\alpha m$, $p$ premier, $\alpha \in \mathbb{N}^*$ et $p$ et $\alpha$ premier entre eux. Alors :*

1. *Il existe un $p$-Sylow dans $G$.*
2. *Tout $p$ sous-groupe de $G$ est inclus dans un $p$-Sylow de $G$.*
3. *Tous les $p$-Sylow de $G$ sont conjugués.*
4. *Si on note $n_p$ le nombre de $p$-Sylow dans $G$ on a*

$$n_p \equiv 1 \ [p] \quad et \quad n_p | m.$$

Pour démontrer ce théorème on commence par un lemme fondamental qui permet, à partir d'un $p$-Sylow d'un groupe $G$, d'obtenir un $p$-Sylow de ces sous-groupes.

**Lemme 2.3.3.** *Soit $H$ un sous-groupe de $G$ et $S$ un $p$-Sylow de $G$. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un $p$-Sylow de $H$.*

*Démonstration.* $H$ agit par translation à gauche sur $G/S$.

$$\begin{aligned} x \in Stab_H(aS) &\iff x \in H \text{ et } xaS = aS \\ &\iff x \in H \text{ et } x \in aSa^{-1} \\ &\iff x \in H \cap aSa^{-1}. \end{aligned}$$

Ainsi en appliquant la formule des classes on obtient :

$$|G/S| = \sum_{\omega \in (G/S)/H} |\omega| = \sum_{Orbite} \frac{|H|}{|H \cap aSa^{-1}|},$$

or $S$ est un $p$-Sylow de $G$ donc $p \nmid |G/S|$, ainsi il existe $a \in G$ tel que $\frac{|H|}{|H \cap aSa^{-1}|}$ ne soit pas divisible par $p$. Ce qui signifie exactement que $H \cap aSa^{-1}$ est un $p$-Sylow de $H$ car c'est un $p$-sous groupe de $H$ d'indice premier avec $p$. □

Voici donc maintenant la démonstration du théorème de Sylow.

*Démonstration.*

1. $G \hookrightarrow S_n$ par Cayley et $S_n \hookrightarrow \mathrm{GL}_n(\mathbb{F}_q)$ en associant à une permutation de $S_n$ la matrice de permutation des vecteurs d'une base de $(\mathbb{F}_p)^n$. Donc $G$ s'injecte dans $\mathrm{GL}_n(\mathbb{F}_q)$. D'après le lemme il suffit donc de montrer que $\mathrm{GL}_n(\mathbb{F}_q)$ contient un $p$-Sylowpour avoir l'existence d'un $p$-Sylow de $G$.
$$|\mathrm{GL}_n(\mathbb{F}_p)| = \prod_{i=1}^{n-1} (p^n - p^i) = p^{\frac{n(n-1)}{2}} m,$$
où $p \wedge m = 1$. On considère alors le sous-groupe
$$S = \{I_n + T \mid T \text{triangulaire supérieure stricte}\} \subset \mathrm{GL}_n(\mathbb{F}_p)$$
qui est de cardinal $p^{\frac{n(n-1)}{2}}$ donc $S$ est bien un $p$-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.
2. Soient $H$ un $p$-sous groupe de $G$ et $S$ un $p$-Sylow de $G$. D'après le lemme il existe $a \in G$ tel que $H \cap aSa^{-1}$ soit un $p$-Sylow de $H$. Or $H$ est un $p$-groupe donc $H \cap aSa^{-1} = H$. Cela signifie que $H \subset aSa^{-1}$ et $|aSa^{-1}| = |S|$ donc $aSa^{-1}$ est un $p$-Sylow de $G$ qui contient $H$.
3. Soient $S_1$ et $S_2$ deux $p$-Sylow de $G$. $S_1$ est un $p$-groupe donc il existe $a \in G$ tel que $S_1 \subset aS_2a^{-1}$, par le cardinal on a $S_1 = aS_2a^{-1}$. Ainsi les $p$-Sylow de $G$ sont conjugués dans $G$. Cela signifie que l'ensemble des $p$-Sylow de $G$ constitue une orbite pour l'action de $G$ par conjugaison sur l'ensemble de ses sous-groupes. On a donc :
$$n_p \mid p^\alpha m = |G|.$$

4. $G$ agit sur l'ensemble $X$ de ses $p$-Sylow par conjugaison. Un $p$-Sylow $S$ de $G$ agit donc aussi sur $X$ par restriction. Par la formule des classes on a donc :

$$n_p = |X| = |X^S| + \sum_{|orbite|\geq 2} |orbite|,$$

or le cardinal des orbites divise celui de $S$ qui est $p^\alpha$ donc on obtient :

$$n_p \equiv |X^S| \mod p.$$

Le but est donc maintenant de montrer que $|X^S| = 1$. On commence par remarquer que $S \in X^S$ car $\forall s \in S,\ sSs^{-1} = S$. Supposons que l'on a un autre $p$-Sylow $T \in X^S$. Ainsi $\forall s \in S,\ sTs^{-1} = T$. On pose $N = \langle S, T\rangle \subset G$. $T$ et $N$ sont des $p$-sous groupes de $N$ d'ordre maximal donc ceux sont deux $p$-Sylow de $N$. Or $T \in X^S$ donc $T \lhd N$. Les $p$-Sylow de $N$ étant conjugués cela signifie que $T$ est le seul $p$-Sylow de $N$, ainsi $T = S$, absurde. Donc $S$ est le seul élément de $X^S$ qui est donc bien de cardinal 1 et on a $n_p \equiv 1 \mod p$. En particulier $n_p$ et $p$ son premier entre aux donc puisqu'on a vu plus haut que $n_p \mid p^\alpha m$ cela nous permet de conclure que $n_p \mid m$.

□

**Corollaire 2.3.4.** *Un $p$-Sylow de $G$ est distingué si et seulement si il est le seul $p$-Sylow de $G$.*

*Démonstration.* Ceci est immédiat en utilisant le point 3 du théorème de Sylow. □

Applications : Classification et nature des groupes de petits cardinaux

**Exemple 2.3.5.**

- Si $|G| = 255$ alors il n'est pas simple. En effet $255 = 3 \times 5 \times 17$ donc $n_{17} \equiv 1 \mod 17$ et $n_{17} \mid 15$, ce qui implique $n_{17} = 1$ ainsi il y a un unique 17-Sylow (qui est donc distingué) dans $G$.
- Il y a cinq groupe d'ordre 18, cinq d'ordre 12 et cinq d'ordre 8 à isomorphismes près. Pour cela on utilise les $p$-Sylow pour avoir des sous-groupes parfois conjugués qui nous permettent via l'utilisation de produits semi-directs de trouver tous les groupes d'ordres donnés.

On détaille ici le cas des groupes d'ordre 8 pour montrer les raisonnements utilisés bien que dans ce cas Sylow ne soit pas utile car le caractère distingué de certains sous-groupes dont on a besoin s'obtient par un simple argument sur son indice :

**Proposition 2.3.6.** *Tout groupe d'ordre 8 est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $D_4$ ou $\mathbb{Q}_8$.*

*Démonstration.* Notons $r$ le maximum des ordres des éléments de $G$ un groupe d'ordre 8. Soit $g \in G$ d'ordre 8. Le sous-groupe engendré par $g$ est de cardinal $r$ et donc $r$ divise 8. Il faut donc traiter trois cas : $r \in \{2, 4, 8\}$, $r = 1$ impossible car sinon $G$ est le groupe trivial et n'est donc pas d'ordre 8.

- <u>cas $r = 8$</u>
  Forcément, $G \simeq \mathbb{Z}/8\mathbb{Z}$.
- <u>cas $r = 2$</u>
  Dans ce cas, $G$ est abélien (en effet : $(xy)^2 = e = xyxy$ en multipliant à gauche successivement par $x$ puis par $y$, on obtient bien $xy = yx$). $G$ est donc un $\mathbb{F}_2$-espace vectoriel. Comme il est d'ordre 8, c'est un espace vectoriel de dimension 3, et on a $G \simeq \mathbb{F}_2^3 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- <u>cas $r = 4$</u>
  Soit $g_4 \in G$ un élément d'ordre 4.
  On note $H =< g_4 >$ le sous-groupe engendré par $g_4$. $H$ est d'indice 2 dans $G$ donc distingué.
  On étudie alors deux sous-cas : s'il existe un élément dans $G \setminus H$ d'ordre 2 ou non.
  Supposons qu'il existe $x_2 \in G \setminus H$ d'ordre 2, on note $K = \{e, x_2\}$. $K \cap H = \{e\}$, $H \lhd G$ et $|G| = |H|.|K|$ donc $G$ est isomorphe à un produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.
  Or $\#Aut\,(\mathbb{Z}/4\mathbb{Z}) = 2$ (car l'indicateur d'Euler de 4 est 2 puisqu'il y a deux inversibles dans $\mathbb{Z}/4\mathbb{Z}$). Il y a alors deux possibilités : avec l'automorphisme trivial $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, dans le deuxième cas, $G \simeq D_4$ car $D_4$ est un produit semi-direct non trivial de $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$. En effet $D_4 = \{\langle r, s\rangle \mid s^2 = e,\ r^4 = e,\ srs = r^{-1} = r^3\} = \langle r\rangle \rtimes_\varphi \langle s\rangle$ avec $\varphi(s).(r^i) = r^{3i}$.
  Il reste à étudier le cas où tous les éléments de $G \setminus H$ sont d'ordre 4. Soit alors $j \in G \setminus H$, on note $k = g_4 j$ et $i = g_4$.

$$G = H \sqcup Hj = \{e, i, i^2, i^3, j, k, i^2 j, i^2 k\}$$

  où $i^2$ est le seul élément d'ordre 2 (donc $i^2 = j^2 = k^2$).
  En notant $\mathbb{Q}_8 = < x, y | x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} >$ l'ensemble des quaternions, et en vérifiant qu'en posant $x = i$ et $y = j$ on récupère bien $G$, on a $G \simeq \mathbb{Q}_8$.

**Bilan** : Tous les groupes d'ordre 8 sont isomorphes à l'un des groupes suivants :$(\mathbb{Z}/2\mathbb{Z})^3$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $D_4$ et $\mathbb{Q}_8$.

□

# 3 Applications en algèbre linéaire

On définit ici différentes actions de groupes de matrices ainsi que certaines de leurs propriété et/ou applications.

1. $O_n(\mathbb{R})$ agit sur $S_n(\mathbb{R})$ via $O.M = OM^tO$.

   **Proposition 3.0.7.** *$\{Diag(\lambda_1, \dots, \lambda_n) \mid \lambda_1 \leq \cdots \leq \lambda_n\}$ est un système de représentants des orbites pour cette action.*

   *Démonstration.* Tous les éléments $M$ de $O_n(\mathbb{R})$ sont diagonalisables en base orthonormée. Quitte à faire agir une matrice de permutation (qui se trouve bien dans $O_n(\mathbb{R})$) pour ordonner ses valeurs propres on obtient donc un éléments de la forme $Diag(\lambda_1, \dots, \lambda_n)$, $\lambda_1 \leq \cdots \leq \lambda_n$ dans l'orbite de $M$. De plus deux matrices ayant une liste de valeurs propres différentes ne peuvent pas être dans la même orbite car elles ne sont pas semblables, ainsi $\{Diag(\lambda_1, \dots, \lambda_n) \mid \lambda_1 \leq \cdots \leq \lambda_n\}$ est bien un système de représentants des orbites pour cette action. □

   Application : Classification affine des coniques et des quadriques.

2. $GL_n(K)$ agit par conjugaison sur $M_n(K)$.

   La réduction de Frobenius utilisant les invariants de similitudes permet de trouver un représentant des orbites pour cette action.

   Applications au dénombrement :

   **Proposition 3.0.8.** *Soit $n \geq 2$. Le nombre de matrices nilpotentes d'ordre $n$ dans $M_n(\mathbb{F}_q)$ est*

   $$q^{\frac{(n-2)(n-1)}{2}} \prod_{k=2}^{n} (q^k - 1).$$

   *Démonstration.* Les matrices nilpotentes d'ordre $n$ dans $M_n(\mathbb{F}_q)$ sont semblables à la matrice $N_n$ avec des 1 uniquement sur la première diagonale au-dessus de la diagonale principale, en dimension 3 par exemple il s'agit de la matrice suivante : $N_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. Le cardinal recherché est donc celui de l'orbite de $N_n$ pour l'action de $\mathrm{GL}_n(\mathbb{F}_q)$ par conjugaison sur $M_n(\mathbb{F}_q)$. On va alors utiliser la relation orbite-stabilisateur :

   $$|\mathrm{GL}_n(\mathbb{F}_q)| = |Orbite(N_n)| \times |Stab_{\mathrm{GL}_n(\mathbb{F}_q)}(N_n)|.$$

En raisonnant sur l'indépendance des colonnes des matrices inversibles on obtient :

$$|\mathrm{GL}_n(\mathbb{F}_q)| = \prod_{k=0}^{n-1} (q^n - q^k) = q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} (q^k - 1).$$

Il reste donc à trouver le cardinal des éléments qui stabilisent $N_n$, c'est à dire les éléments de $GL_n(\mathbb{F}_q)$ qui commutent avec $N_n$. Soit $M = (m_{i,j})_{1 \leq i,j \leq n} \in \mathrm{GL}_n(\mathbb{F}_q)$, on pose $A = (a_{i,j})_{1 \leq i,j \leq n} = MN_n$ et $B = (b_{i,j})_{1 \leq i,j \leq n} = N_n M$. Ainsi on a :

$$a_{i,j} = \begin{cases} 0 \text{ si } j = 1 \\ m_{i,j-1} \text{ sinon} \end{cases} \qquad b_{i,j} = \begin{cases} 0 \text{ si } i = n \\ m_{i+1,j} \text{ sinon} \end{cases} .$$

Ainsi :

$$M \in Stab_{\mathrm{GL}_n(\mathbb{F}_q)}(N_n) \iff \begin{cases} \forall i \in [\![2, n]\!],\ m_{i,1} = 0 \\ \forall j \in [\![1, n-1]\!],\ m_{n,j} \\ \forall j > 1, i < n,\ m_{i+1,j} = m_{i,j-1} \end{cases} .$$

Ainsi par récurrence on montre facilement que c'est équivalent à ce que $M$ soit de la forme suivante :

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ 0 & a_1 & a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_2 & a_3 \\ \vdots & & \ddots & a_1 & a_2 \\ 0 & \cdots & \cdots & 0 & a_1 \end{pmatrix}.$$

Se donner une matrice de $Stab_{\mathrm{GL}_n(\mathbb{F}_q)}(N_n)$ revient donc à se donner $n$-éléments $a_1, \ldots, a_n$ dans $\mathbb{F}_q$ avec $a_1 \neq 0$. Ainsi on obtient :

$$|Stab_{\mathrm{GL}_n(\mathbb{F}_p)}(N_n)| = (q-1)q^{n-1},$$

et donc

$$|Orbite(N_n)| = \frac{q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} (q^k - 1)}{(q-1)q^{n-1}} = q^{\frac{(n-2)(n-1)}{2}} \prod_{k=2}^{n} (q^k - 1).$$

□

3. $GL_n(K) \times GL_p(K)$ agit sur $M_{n,p}(K)$ via $(P, Q).M = PMQ^{-1}$.

Pour $r \in [\![1, \min(n,p)]\!]$ on note $J_r$ la matrice suivante :

$$J_r = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & \ddots & & \vdots & & \vdots \\ \vdots & \ddots & 1 & 0 & \dots & 0 \\ \vdots & & \ddots & 0 & \dots & 0 \\ 0 & \dots & \dots & 0 & \dots & 0 \end{pmatrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \end{matrix}\right\} \text{r}$$

**Proposition 3.0.9.** *$\{J_r\}_{0 \leq r \leq \min(n,p)}$ est un système de représentants des orbites qui sont donc caractérisées par le rang des matrices.*

**Remarque 3.0.10.** Ce résultat utilise simplement le fait que les orbites pour cette action sont stables par les opérations du type $L_i \leftarrow L_i + \alpha L_j$ sur les lignes ou $C_i \leftarrow C_i + \alpha C_j$. Ainsi en appliquant un pivot de Gauss successivement sur les lignes et les colonnes on obtient la forme voulue.

De nouveau nous avons des applications en dénombrement comme la proposition suivante :

**Proposition 3.0.11.** *Le nombre de matrices de rang $r$ dans $M_{n,p}(\mathbb{F}_q)$ est*

$$\frac{q^{\frac{r(r-1)}{2}} \prod_{k=n-r+1}^{n} (q^k - 1) \prod_{k=p-r+1}^{p} (q^k - 1)}{\prod_{k=1}^{r} (q^k - 1)}$$

*Démonstration.* Le principe est le même que pour la démonstration de la proposition 3.0.8 mais cette fois on utilise l'action de $GL_n(K) \times GL_p(K)$ sur $M_{n,p}(\mathbb{F}_q)$ et le fait que l'ensemble des matrices de rang $r$ de $M_{n,p}(\mathbb{F}_q)$ est l'orbite de $J_r$. Ici, le stabilisateur de $J_r$ est l'ensemble des couples $(P, Q) \in GL_n(K) \times GL_p(K)$ avec :

$$P = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \; Q = \begin{pmatrix} A & 0 \\ C & E \end{pmatrix},$$

avec $A \in \mathrm{GL}_r(\mathbb{F}_q)$, $D$ et $E$ inversible. Ainsi :

$$|Stab(J_r)| = |\mathrm{GL}_r(\mathbb{F}_q)| \times |\mathrm{GL}_{n-r}\mathbb{F}_q)| \times |\mathrm{GL}_{p-r}(\mathbb{F}_q)| \times q^{(n+p-2r)r},$$

et

$$|Orbite(J_r)| = \frac{|\mathrm{GL}_n(\mathbb{F}_q)| \times |\mathrm{GL}_p\mathbb{F}_q)|}{|\mathrm{GL}_r(\mathbb{F}_q)| \times |\mathrm{GL}_{n-r}\mathbb{F}_q)| \times |\mathrm{GL}_{p-r}(\mathbb{F}_q)| \times q^{(n+p-2r)r}},$$

ce qui donne le résultat après simplification. □

4. $PSL_2(\mathbb{Z})$ (ensemble des matrices $2 \times 2$ à coefficients dans $\mathbb{Z}$, de déterminant 1 que l'on quotiente par $\pm\mathrm{Id}$) agit fidèlement sur le demi-plan de Poincarré $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$ par homographie.

   **Proposition 3.0.12.** *$D = \{z \in \mathbb{C} \mid |z| \geq 1,\ |Re(z)| \leq \frac{1}{2}\}$ est un domaine fondamental pour cette action, i.e. toute orbite rencontre $D$ et si deux points de $D$ sont dans la même orbite ils sont sur la frontière de $D$.*

   Application : $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ engendrent $SL_2(\mathbb{Z})$.

5. Si $\dim(E) < +\infty$, $GL(E)$ agit simplement transitivement sur l'ensemble des bases de $E$ et $PGL(E)$ agit fidèlement sur $\mathbb{P}(E)$.

   Applications :

   **Proposition 3.0.13.**

$$PGL(2, \mathbb{F}_q) \simeq \begin{cases} S_3 \text{ si } q = 2 \\ S_4 \text{ si } q = 3 \\ A_5 \text{ si } q = 4 \\ S_5 \text{ si } q = 5 \end{cases} .$$

   *Démonstration.* La démonstration utilise principalement les deux lemmes suivants sur les groupes symétriques :

   **Lemme 3.0.14.** *Pour $n \geq 5$ les seuls sous-groupes distingués de $S_n$ sont $\{\mathrm{Id}\}$, $A_n$ et $S_n$.*

   *Démonstration.* On admet le fait que $A_n$ est simple pour $n \geq 5$. Soit $G \lhd S_n$. On pose $H = A_n \bigcap G$. Comme $A_n$ est distingué dans $S_n$ alors $H \lhd S_n$. De plus $H \subset A_n$ donc $H \lhd A_n$. Par simplicité de $A_n$ deux cas se présentent :
   - $H = A_n$ : cela signifie que $A_n \subset G$ et par cardinalité on a donc $G = S_n$ ou $G = A_n$.
   - $H = \mathrm{Id}$ : Soit $G = Id$ sinon il existe $x \in G \setminus \{Id\}$. Soit $y \in G$ :

$$\begin{aligned} y \in G \setminus \{Id\} \Longrightarrow y \notin A_n &\Longrightarrow yA_n = xA_n \text{ (car } A_n \text{ d'indice 2 dans } S_n) \\ &\Longrightarrow y^{-1}x \in A_n \bigcap G = \{\mathrm{Id}\} \Longrightarrow y = x \end{aligned}$$

     Ainsi on a $G = \{\mathrm{Id}, x\}$ avec $x$ une transposition. Ceci est absurde car $G \lhd S_n$ et $n \geq 5$.

     □

   **Lemme 3.0.15.** *Soit $n \geq 2$, alors tout sous-groupe d'indice $n$ dans $S_n$ est isomorphe à $S_{n-1}$.*

*Démonstration.* Soit $G \subset S_n$ d'indice $n$.

- $n = 2 : G = \{\mathrm{Id}\} \simeq S_1$.
- $n = 3 : |G| = 2$ donc $G \simeq \mathbb{Z}/2\mathbb{Z} \simeq S_2$.
- $n = 4 : G$ d'indice 4 dans $S_4$ donc $|G| = 6$. Les seuls groupes d'ordre 6 sont, à isomorphisme près, $S_3$ et $\mathbb{Z}/6\mathbb{Z}$ or $G \subset S_4$ n'a pas d'élément d'ordre 6 donc $G \simeq S_3$.
- $n \geq 5 : S_n$ agit sur $S_n/G$ par translation, ce qui nous donne un morphisme $\varphi : S_n \to \mathfrak{S}(S_n/G)$. D'après le lemme 3.0.14 $\ker\varphi$ est égal à $S_n$, $A_n$ ou $\{\mathrm{Id}\}$, or $\ker\varphi \subset G$ donc par cardinalité $\ker\varphi = \{\mathrm{Id}\}$. Ainsi $\varphi$ est injective. On restreint alors cette action à $G$ ce qui nous donne un morphisme injectif $\varphi : G \hookrightarrow \mathfrak{S}(S_n/G)$. Or $\forall g \in G$, $g.(eG) = eG$ donc $eG$ est fixé par $G$. Donc finalement $G$ agit sur $S_n/G\backslash\{eG\}$ ce qui nous donne un morphisme injectif $\varphi : G \hookrightarrow \mathfrak{S}(S_n/G\backslash\{eG\})$. $G$ étant d'indice $n$ dans $S_n$ on a $|S_n/G\backslash\{eG\}| = n-1$ et $\mathfrak{S}(S_n/G \setminus \{eG\}) \simeq S_{n-1}$. Ainsi $G$ s'injecte par $\varphi$ dans $S_{n-1}$ donc par cardinalité $G \simeq S_{n-1}$.

□

Nous avons maintenant tous les éléments pour démontrer notre proposition. $PGL(E)$ agit fidèlement sur $\mathbb{P}(E)$, ici $E = \mathbb{F}_q^2$ donc on obtient un morphisme injectif $\varphi : PGL(2,\mathbb{F}_q) \hookrightarrow \mathfrak{S}(\mathbb{P}(\mathbb{F}_q^2))$.

$$|PGL(2,\mathbb{F}_q)| = \frac{(q^2-1)(q^2-q)}{q-1} = q(q^2-1)$$

$$|\mathbb{P}(\mathbb{F}_q^2)| = \frac{q^2-1}{q-1} = q+1$$

Ainsi $\mathfrak{S}(\mathbb{P}(\mathbb{F}_q^2)) \simeq S_{q+1}$.

- Si $q = 2$ on a $|PGL(2,\mathbb{F}_2)| = 6$ donc $\varphi$ est un isomorphisme et $PGL(2,\mathbb{F}_2) \simeq S_3$.
- Si $q = 3$ on a $|PGL(2,\mathbb{F}_3)| = 24$ donc $\varphi$ est un isomorphisme et $PGL(2,\mathbb{F}_3) \simeq S_4$.
- Si $q = 4$ on a $|PGL(2,\mathbb{F}_4)| = 60$ donc il est isomorphe à un sous-groupe de $S_5$ d'indice 2. Tout sous-groupe d'indice 2 est distingué donc par le lemme 3.0.14 on a $PGL(2,\mathbb{F}_4) \simeq A_5$.
- Si $q = 5$ on a $|PGL(2,\mathbb{F}_5)| = 120$ donc il est isomorphe à un sous-groupe d'indice 6 dans $S_6$, par le lemme 3.0.15 on obtient donc $PGL(2,\mathbb{F}_5) \simeq S_5$.

□

**Remarque 3.0.16.** Le dernier isomorphisme peut notamment être utilisé pour montrer que $S_6$ contient un automorphisme non intérieur, ce qui n'est pas le cas de $S_n$ pour $n \neq 6$. En effet $G = PGL(2,\mathbb{F}_5)$ peut être vu dans $S_6$ comme un sous-groupe d'indice 6 qui agit transitivement sur $\{1,..,6\}$

ainsi il n'est pas conjugué à un $S(i) = \{\sigma \in S_n \mid \sigma(i) = i\}$. Le morphisme $\psi : S_6 \to \mathfrak{S}(S_6/G)$ venant de l'action par translation de $S_6$ sur $S_6/G$ est injective (par le lemme 3.0.14 et cardinal de $G$) donc par le cardinal c'est un isomorphisme. De plus on construit un isomorphisme $\gamma : \mathfrak{S}(S_6/G) \to S_6$ en utilisant une bijection de $\{1, .., 6\}$ dans $S_6/G$ qui envoie 1 sur $eG$. On a donc $\gamma \circ \psi : S_6 \to S_6$ qui est un automorphisme de $S_6$ tel que $\gamma \circ \psi(G) = S(1)$, ainsi $\gamma \circ \psi(G)$ n'est pas un automorphisme intérieur car $G$ et $S(1)$ ne sont pas conjugués.

# 4 Applications en géométrie

- Soient $E$ un espace euclidien de dimension $n \geq 2$, $D_0$ l'ensemble des demis-droites de $E$ et $D_1$ l'ensemble des droites de $E$. $O(E)$ et $SO(E)$ agissent sur $D_0^2$ et $D_1^2$ via $g.(d_1, d_2) = (g(d_1), g(d_2))$. Ceci nous permet de définir la notion d'angle orienté ou non orienté :

  **Définition 4.0.17.** Soit $(d_1, d_2) \in D_1^2$, on appelle angle non orienté de $(d_1, d_2)$ l'orbite de $(d_1, d_2)$ sous l'action de $O(E)$. Dans le cas $n = 2$ cette orbite est différente de celle sous l'action de $SO(E)$, on appelle alors angle orienté de $(d_1, d_2)$ l'orbite de $(d_1, d_2)$ sous l'action de $SO(E)$.

- Soit $E$ un $K$-espace vectoriel.
  **Définition 4.0.18.** Un espace affine attaché à $E$ est un ensemble sur lequel le groupe additif de $E$ opère simplement transitivement.

- $SO_3(\mathbb{R})$ agit naturellement sur la sphère $S^2$.

  Applications :
  **Proposition 4.0.19.** *Tout sous-groupe fini de $S0_3(\mathbb{R})$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, $D_n$, $A_4$, $S_4$ ou $A_5$.*
  **Proposition 4.0.20.** *Il n'y a pas de symétrie d'ordre 5 dans un cristal.*

# 5 Action sur $k[X_1, ..., X_n]$

$\sigma \in S_n$ agit sur $k[X_1, \ldots, X_n]$ via :

$$\sigma.P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

**Définition 5.0.21.** $k[X_1, \ldots, X_n]^{S_n}$ est l'ensemble des polynômes symétriques.

**Proposition 5.0.22.** *L'ensemble des polynômes symétriques est engendré, en tant qu'algèbre, par les polynômes symétriques élémentaires $(s_k)_{1\leq k\leq n}$ définis comme suit :*

$$s_k = \sum_{1\leq i_1\leq\cdots\leq i_k\leq n} X_{i_1}\dots X_{i_k}$$

**Exemple 5.0.23.** Pour $n = 3$ les polynômes symétriques élémentaires sont $X_1 + X_2 + X_3$, $X_1X_2 + X_2X_3 + X_1X_3$ et $X_1X_2X_3$.

**Applications 5.0.24.** Soient $\lambda_1, \dots, \lambda_n$ les racines complexes, comptées avec multiplicités, du polynôme $P \in \mathbb{R}_n[X]$, $P = \sum_{k=0}^{n} a_k X^k$, $a_n = 1$.

$$\forall k \in \{1, \dots, n\},\ s_k(\lambda_1, \dots, \lambda_n) = a_{n-k} \in \mathbb{R},$$

ainsi $\forall i \in \mathbb{N}$ :

$$\sum_{k=1}^{n} \lambda_k^i \in \mathbb{R},$$

en effet il suffit d'appliquer la proposition 5.0.22 au polynôme $Q = \sum_{k=1}^{n} X_k^i \in \mathbb{K}[X_1, \dots, X_n]^{S_n}$.

De même, $A_n$ agit sur $P \in \mathbb{K}[T_{\sigma(1)}, \dots, T_{\sigma(n)}]$ par restriction, et on appelle polynômes semi-symétriques, les points fixes pour cette action.

**Proposition 5.0.25.** *Soit $f(T_1, \dots, T_n)$ un polynôme semi-symétrique, alors $f$ se décompose de façon unique sous la forme :*

$$f(T_1, \dots, T_n) = P(T_1, \dots, T_n) + V(T_1, \dots, T_n)Q(T_1, \dots, T_n),$$

*où $P$ et $Q$ sont des polynômes symétriques et $V$ le polynômes de VanderMonde définit par :*

$$V(T_1, \dots, T_n) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ T_1 & T_2 & \cdots & T_n \\ \vdots & \vdots & \ddots & \vdots \\ T_1^{n-1} & T_2^{n-2} & \cdots & T_n^{n-1} \end{vmatrix} = \prod_{1\leq i<j\leq n} (T_j - T_i)$$

*Démonstration.* Tout d'abord, remarquons que si l'on se donne $f$ un polynôme semi-symétrique et $\sigma_1, \sigma_2 \in S_n \setminus A_n$ alors $\sigma_1^{-1}\sigma_2 \in A_n$ et donc $\sigma_1^{-1}\sigma_2.f = f$, soit $\sigma_1.f = \sigma_2.f$. Comme $\tau = (1, 2) \in S_n \setminus A_n$, si on pose $g = \tau.f$, alors on a : $\forall \sigma \in S_n \setminus A_n$, $g = \sigma.f$.

Les transpositions engendrant les permutations, étudions quelques résultats sur les transpositions :

Soient $\tau_1$ et $\tau_2$ deux transpositions.
$\tau_1.g = \tau_1.(\tau.f) = \tau_1\tau.f = f$ et $\tau_1 f = g$

$(\tau_2\tau_1).g = (\tau_2\tau_1\tau).f = g$ et $(\tau\tau_1).f = f$
Ainsi :
$\tau_1(f-g) = g - f = \epsilon(\tau_1)(f-g)$ et $\tau_2\tau_1.(f-g) = f - g = \epsilon(\tau_2\tau_1).(f-g)$.
$\quad \Longrightarrow \forall \sigma \in S_n,\ \sigma(f-g) = \epsilon(\sigma)(f-g)$
$\tau_1(f+g) = g + f$ et $\tau_2\tau_1.(f+g) = f + g$. $\quad \Longrightarrow \forall \sigma \in S_n, \sigma(f+g) = f+g.$

ainsi $f-g$ est alterné et $f+g$ est symétrique

Soient maintenant $i < j \in \{1, \ldots, n\}$ : On fait la division euclidienne de $f-g$ par $T_j - T_i$ vu comme polynôme en $T_j$ :

$$f - g = (T_j - T_i)q + r \qquad \text{avec } r \in \mathbb{K}[T_1, \ldots, T_{j-1}, T_{j+1}, \ldots, T_n]$$

En appliquant $\tau_{i,j}$, on a aussi :

$$-(f-g) = -(T_j - T_i)\tau_{i,j}.q + \tau_{i,j}.r$$

On évalue ces polynômes de variable $T_j$ en $T_i$ : $(f-g)(T_i) = r(T_i)$, et comme $r$ ne dépend pas de $T_j$, $r(T_i) = r$. De plus, $(g-f)(T_i) = (\tau_{i,j}.r)(T_i) = r$ car $\tau_{i,j}$ échange $T_i$ et $T_j$ dans $r$ puis en évaluant $r$ en $T_i$, cela remplace $T_j$ par $T_i$.

Ainsi $(f-g)(T_i) = (g-f)(T_i) = r$ et donc $r = 0$. On a ainsi montré que :

$$\forall i < j, T_j - T_i | f - g \qquad \text{et donc} \quad V(T_1, \ldots, T_n) | f - g$$

On définit alors $Q$ et $P$ tels que :

$$\begin{cases} (f-g)(T_1, \ldots, T_n) = & V(T_1, \ldots, T_n) 2Q(T_1, \ldots, T_n) \\ (f+g)(T_1, \ldots, T_n) = & 2P(T_1, \ldots, T_n) \end{cases}$$

Et on vérifie : comme $f+g$ est symétrique, alors $P$ est symétrique. De plus :

$$\begin{aligned} \sigma.(f-g) &= 2\sigma.V(T_1, \ldots, T_n)\sigma.Q(T_1, \ldots, T_n) \\ &= 2\epsilon(\sigma)V(T_1, \ldots, T_n)\sigma.Q(T_1, \ldots, T_n), \end{aligned}$$

car $V$ est un déterminant donc il est alterné. D'autre part :

$$\begin{aligned} \sigma.(f-g) &= \epsilon(\sigma).(f-g), \quad (\text{car } f-g \text{ est alterné}) \\ &= \epsilon(\sigma)2.V(T_1, \ldots, T_n).Q(T_1, \ldots, T_n) \end{aligned}$$

Comme $\mathbb{K}[T_1, \ldots, T_n]$ est intègre, on obtient : $Q(T_1, \ldots, T_n) = \sigma.Q(T_1, \ldots, T_n)$ et donc $Q$ est symétrique.

En sommant $f+g$ et $f-g$, on récupère $f = P + VQ$ avec $P$ et $Q$ symétriques et $V$ de Vandermond. Il reste à montrer l'unicité :

Supposons qu'on ait également $f = \hat{P} + V\hat{Q}$, on a $g = \tau.f = \hat{P} - V\hat{Q}$, d'où :

$$\begin{cases} f + g = & 2\hat{P} \\ f - g = & 2V\hat{Q} \end{cases}$$

et donc on a l'unicité de $P$ et $Q$. □

# 6 Représentations des groupes finis

Soit $K$ un corps. Une représentation d'un groupe $G$ (fini) est la donnée d'un couple $(\rho, V)$ où $V$ est un espace vectoriel et $\rho$ un morphsime de $G$ dans $GL(V)$. Il s'agit en faite d'une action linéaire de $G$ sur $V$. L'action de $G$ sur $G$ par multiplication à gauche nous donne une représentation naturelle de $G$ sur $K^G$. En effet en tant que $K$-espace vectoriel $K^G$ est de dimension $|G|$ dont une base est $(f_g)_{g\in G}$ avec $f_g(g_1) = \delta_{g,g_1}$. L'action linéaire de $G$ sur $K^G$ est alors donnée par $\rho : G \to GL(K^G)$ avec :

$$\rho(g_1) : \begin{cases} K^G \to K^G \\ f_g \mapsto f_{g_1 g} \end{cases} .$$

Cette action consiste en faite à permuter les éléments de la base de $K^G$ par la permutation de $G$ induite par l'action de $G$ sur lui-même par multiplication à gauche. Les $\rho(g_1)$ sont donc des matrices de permutations.

Cette représentation de $G$, appelé représentations régulière, est importante car en théorie des représentations on montre qu'il y a un nombre fini de représentations dites "irréductibles" $V_1, \ldots, V_h$ de dimension $n_1, \ldots, n_h$. La représentation régulière est alors la somme directe $V_1^{n_1} \oplus \cdots V_h^{n_h}$. Ainsi on a $|G| = \sum n_i^2$.

# 7 Développements

Les développements choisis dans cette leçon sont
- Théorème de Sylow,
- Isomorphisme de $PGL(2, \mathbb{F}_q)$.

car nous avons jugé que les actions de groupe y avait un rôle important mais voici une liste de résultats du plan qui aurait pu être des développements aussi :
- Action de $A_n$ agit sur $k[X_1, \ldots, X_n]$.
- Théorème de Wedderburn,
- Classification des groupes d'ordre 8, 12 ou 18,
- Réduction de Frobenius et facteurs invariants,
- Action de $PSL_2(\mathbb{Z})$ sur le demi-plan de Poincarré,
- Sous-groupe finis de $SO_3(\mathbb{R})$,