Leçon 108 : Groupe engendré par une réflexion. Applications en algèbre linéaire et en géométrie. Groupes de petit cardinal.

Alexandre Mahfouf
Antoine Bernard
Paul-Elie Tena

Réf : - Algèbre 2, Alvin Sepinglas
- Perrin
- UHLG2
- Calbrix/Lemaire
- Carnet de voyage en Algébrie, Calbrix/Perrin

On note : les a.s.s.e : les assertions suivantes sont équivalentes

Soit $\mathbb{K}$ un corps, E un $\mathbb{K}$-ev ddf n.
On notera $Z(G)$ (resp $D(G)$) le centre (resp le groupe dérivé) d'un groupe G.

I. Premières définitions. Groupe spécial linéaire.

a) $GL(E)$, $SL(E)$: définitions et premières propriétés

Def 1 : on appelle groupe linéaire l'ensemble des $\mathbb{K}$-automorphismes de E, noté $GL(E)$. $GL(E)$ a une structure de groupe pour la composition des endomorphismes.
On définit $GL_n(\mathbb{K})$ comme le groupe des automorphismes de $\mathbb{K}^n$.
Fixer une base donne un isomorphisme entre $GL(E)$ et $GL_n(\mathbb{K})$.

Prop 2 : on a les équivalences entre :
(i) $u \in GL(E)$ (ii) $\ker(u) = \{0\}$ (iii) $\det u \neq 0$ (iv) $\mathrm{Im}(u) = E$

Contre-exemple 3 : le résultat est faux en dim ∞ :
$u : \mathbb{K}[X] \to \mathbb{K}[X]$, $P \mapsto X.P$ $\quad \ker(u) = 0$ mais $u \notin GL(E)$

Def 4 : le noyau de $\det : GL(E) \to (\mathbb{K}^*, \times)$ est appelé groupe spécial linéaire et noté $SL(E)$: $SL(E) = \{u \in GL(E) \mid \det(u) = 1\}$

Rq 5 : $SL(E)$ est un sous-groupe distingué de $GL(E)$.

Prop 6 : on a la suite exacte : $1 \to SL(E) \hookrightarrow GL(E) \xrightarrow{\det} \mathbb{K}^* \to 1$
et $GL(E) \simeq SL(E) \times \mathbb{K}^*$.

b) Générateurs

Prop/def 7 : soit H un hyperplan de E et $u \in GL(E)$ tq $u|_H = id_H$
Alors les a.s.s.e :
(1) $\det u = \lambda \neq 1$ (2) u admet une valeur propre λ et u est diagonalisable
(3) $\mathrm{Im}(u - id) \not\subset H$
(4) dans une base convenable, u a pour matrice $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$ avec $\lambda \in \mathbb{K}^*$, $\lambda \neq 1$
Si une de ces conditions est vérifiée, on dit que u est une dilatation d'hyperplan H, de droite $D = \mathrm{Im}(u - id)$, de rapport λ.

Prop 8 : deux dilatations sont conjuguées dans $GL(E)$ si et seulement si elles ont le même rapport λ.

Prop/def 9 : soit H un hyperplan de E d'équation $f \in E^*$ (i.e. $H = \mathrm{Ker} f$, $f \neq 0$). Soit $u \in GL(E)$, $u \neq id$, $u|_H = id_H$. les a.s.s.e :
(1) $\det u = 1$ (i.e. $u \in SL(E)$) (2) u n'est pas diagonalisable
(3) $D = \mathrm{Im}(u - id) \subset H$
(4) $\exists a \in H$, $a \neq 0$ tq : $\forall x \in E$, $u(x) = x + f(x)a$
(5) Dans une base convenable, u a pour matrice : $\begin{pmatrix} 1 & \ddots & 0 \\ \ddots & \ddots & 1 \\ 0 & \ddots & 1 \end{pmatrix}$
Si une de ces conditions est vérifiée, on dit que u est une transvection d'hyperplan H et de droite D.

Prop 10 : soit t transvection de droite D, d'hyperplan H, $u \in GL(E)$, alors $u \circ t \circ u^{-1}$ est une transvection de droite $u(D)$, d'hyperplan $u(H)$

Prop 11 : deux transvections sont conjuguées dans $GL(E)$.
Si $\dim E \geq 3$, deux transvections sont conjuguées dans $SL(E)$

Contre-exemple 12 : dans $SL_2(\mathbb{K})$, les transvections $s = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $t = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ sont conjuguées si et seulement si $\frac{\lambda}{\mu} \in (\mathbb{K}^*)^2$.

Théorème 13 : $SL(E)$ est engendré par les transvections.
$GL(E)$ est engendré par les transvections et les dilatations.

c) Centres et groupes dérivés :

Prop 14 : $Z(GL(E)) = \{\lambda id, \lambda \in \mathbb{K}^*\}$
$Z(SL(E)) = \{\lambda id, \lambda^n = 1\}$

Application/définition 15 :
$\frac{GL(E)}{Z(GL(E))} = PGL(E)$ est appelé groupe projectif linéaire
$\frac{SL(E)}{Z(SL(E))} = PSL(E)$ est appelé groupe projectif spécial linéaire.

App 16 : si $|\mathbb{K}| > 4$ ou $n \geq 3$: $D(GL(E)) = SL(E)$
$D(SL(E)) = SL(E)$

Prop 17 : $PSL_n(\mathbb{K})$ est simple sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{F}_3$

d) Cas des corps finis :

Prop 18 : $\#GL_n(\mathbb{F}_q) = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\dots(q-1)$

App 19 :

$\#SL_n(\mathbb{F}_q) = \#PGL_n(\mathbb{F}_q) = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\dots(q^2-1)$

et $\#PSL_n(\mathbb{F}_q) = \frac{1}{u_n}\#SL_n(\mathbb{F}_q)$ où u_n est le nombre de racines n-ièmes de l'unité dans $\mathbb{F}_q$.

App 20 : On a les isomorphismes suivants :

$GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$

$PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4 \quad PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$

$PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$

$PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5 \quad PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$

} Dev 1

II Le groupe orthogonal :

Dans cette partie : $\mathrm{car}(\mathbb{K}) \neq 2$, q est une forme quadratique non dégénérée, b sa forme bilinéaire associée et on considère l'action de congruence de $GL(E)$.

a) Premières définitions et propriétés :

Def 21 : On appelle groupe orthogonal associé à la forme quadratique q l'ensemble : $\{u \in GL(E) \mid q(u(x)) = q(x) \ \forall x \in E\}$ et on le note $O(q)$.

C'est aussi, en notant M la matrice de q dans une base fixée :

$O(q) = \mathrm{Stab}(M) = \{P \in GL_n(\mathbb{K}),\ PM{}^tP = M\}$.

Rq 22 : Si deux formes quadratiques q et q' sont dans la même orbite pour l'action de congruence de $GL(E)$, alors $O(q)$ et $O(q')$ sont isomorphes (et même conjugués).

Contre-exemple 23 : (par la réciproque de Rq 22)

Si $PA{}^tP = A$, alors $P(-1){}^tP = -A$ donc $O(p,s) = O(s,p)$ où $O(p,s)$ est le stabilisateur de $I_{p,s} = \begin{pmatrix} I_p & 0 \\ 0 & -I_s \end{pmatrix}$.

Prop 24 : $u \in O(q) \Rightarrow \det(u) = \pm 1$

Def 25 : Le sous-groupe de $O(q)$ formé des isométries de déterminant 1 est appelé groupe spécial orthogonal et noté $SO(q)$.

Rq 26 : $SO(q)$ est distingué dans $O(q)$.

Ex 27 : si, dans $E = \mathbb{R}^2$, $q\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1^2 - x_2^2$, alors

$$SO(q) = \left\{ \begin{pmatrix} \varepsilon\sqrt{1+b^2} & b \\ b & \varepsilon\sqrt{1+b^2} \end{pmatrix} \mid b \in \mathbb{R},\ \varepsilon = \pm 1 \right\}$$

b) Générateurs et centres

Def/Prop 28 : Si $u \in GL(E)$ et $u^2 = id$, on dit que u est une symétrie. Pour un tel u, il existe deux sous-ev supplémentaires E^+ et E^- tels que $u_{|E^+} = id$, $u_{|E^-} = -id$. Lorsque $\dim(E^-) = 1$ on dit que u est une réflexion. Lorsque $\dim(E^-) = 2$ on dit que u est un renversement.

Prop 29 : une symétrie u est orthogonale si et seulement si E^+ et E^- sont orthogonaux (pour q).

Prop 30 : soit s symétrie orthogonale par rapport à E^+. Soit $u \in O(q)$. Alors $usou^{-1}$ est une symétrie orthogonale par rapport à $u(E^+)$.

Th 34 (Cartan) : $O(q)$ est engendré par les réflexions orthogonales.

Th 35 : $SO(q)$ est engendré par les renversements orthogonaux.

Th 36 : $Z(O(q)) = \{\mathrm{Id}, -\mathrm{Id}\}$ $\quad Z(SO(q)) = \{id, (-1)^{n+1} id\}$

c) Cas des corps finis :

Prop 37 : $|O_{2k}(\mathbb{F}_q)| = 2(q^k - (-1)^{\frac{k(q-1)}{2}}) \prod_{i=1}^{k-1}(q^{2k} - q^{2i})$

$|O_{2k+1}(\mathbb{F}_q)| = 2q^k \prod_{i=0}^{k-1}(q^{2k} - q^{2i})$

Th 38 :

$$SO_2(\mathbb{F}_p) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } (-1) \text{ est un carré} \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon} \end{cases}$$

} Dev 2

III Matrices triangulaires / diagonales par blocs, drapeaux :

Def 39 : soit $k \in [\![1, n-1]\!]$ et $p \in \mathbb{N}^n$. On définit :
$S_k = \{(F,G) / F \oplus G = E, \dim(F) = k\}$ et $\mathcal{F}_p = \{\text{drapeaux de type } p\}$

App 40 : $GL(E) \curvearrowright S_k$ et $GL(E) \curvearrowright \mathcal{F}_p$ par image directe transitivement $\forall k, p$.

Def / prop 41 : $\mathrm{Stab}(S_k) \simeq \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in GL_n(\mathbb{K}) \mid A \in GL_k(\mathbb{K}), B \in GL_{n-k}(\mathbb{K}) \right\}$

$\mathrm{Stab}(\mathcal{F}_p) \simeq \{\text{ens. des matrices } \Delta \text{ sup par blocs suivant le type } p\}$

Rq 42 : comme la transposition laisse fixe $GL(E)$, on a de même pour les matrices Δ inf.

Prop 43 : Il y a bijection entre $\mathcal{F}_n$ et l'ensemble des p. Sylow de $GL(E)$. } cor 3

IV Résultats topologiques :

Ici $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

a) $GL(E)$, $SL(E)$

Prop 44 : $GL_n(\mathbb{K})$ est un ouvert dense de $M_n(\mathbb{K})$.
Si $\mathbb{K} = \mathbb{C}$, $GL_n(\mathbb{K})$ est de plus connexe.
$GL_n^+(\mathbb{R}) = \{g \in GL_n(\mathbb{R}), \det g > 0\}$ est connexe. De même $GL_n^-(\mathbb{R})$.

Prop 45 : $SL_n(\mathbb{C})$ est connexe.

Prop 46 : On a les homéomorphismes suivants :
$GL_n(\mathbb{C}) \simeq \mathbb{C}^* \times SL_n(\mathbb{C})$
$GL_n^+(\mathbb{C}) \simeq \mathbb{R}^{+*} \times SL_n(\mathbb{C})$

b) Groupes orthogonaux canoniques, décomposition polaire

On considère à nouveau l'action par congruence.

Def 47 : On note :
$O(n, \mathbb{R}) = \mathrm{Stab}(I_n) = \{P \in GL_n(\mathbb{R}), {}^tP P = I_n\}$
et $O_{(p,q,\mathbb{R})} = O_{(p,q)} = \mathrm{Stab}(I_{p,q})$
où $I_{p,q} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$ avec $p+q = n$

Prop 48 : $O(n, \mathbb{R})$ est compact.

Th 49 : (Décomposition polaire) } deux
La multiplication matricielle induit l'homéomorphisme :
$\mu : O(n, \mathbb{R}) \times S_n^{++}(\mathbb{R}) \xrightarrow{\sim} GL_n(\mathbb{R})$
$(O, S) \longmapsto OS$

App 48 : Il existe un homéomorphisme :
$O_{(p,q)} \xrightarrow{\sim} O_p \times O_q \times \mathbb{R}^{pq}$ } cor 5

App 49 : $O_{(p,q)}$ n'est pas compact.

CVA p 148

Développement : Le groupe $SO_2(\mathbb{F}_p)$

Leçon 110 · 121 · 150 · 104 · 106 · 152 · 101

Théorème : Soit p un nombre premier impair.

$$SO_2(\mathbb{F}_p) \simeq \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} & \text{si } p \equiv 1[4] \\ \mathbb{Z}/(p+1)\mathbb{Z} & \text{si } p \equiv 3[4] \end{cases}$$

Rappel : $SO_2(\mathbb{F}_p) := \{A \in GL_2(\mathbb{F}_p) \,;\, \det A = 1,\ {}^tAA = I_2\}$

Montrons que $SO_2(\mathbb{F}_p) = \left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix},\ a^2+b^2 = 1,\ a,b \in \mathbb{F}_p\right\}$

Le groupe $SO_2(\mathbb{F}_p)$ est décrit par : $SO_2(\mathbb{F}_p) = \left\{\begin{pmatrix} a & c \\ b & d \end{pmatrix} : ad-bc = 1,\ a^2+b^2=1,\ c^2+d^2=1,\ ac+bd=0\right\}$

Fixons (a,b) tel que $a^2+b^2 = 1$. Les équations d'inconnue (c,d) :

$\begin{cases} ac+bd = 0 \\ -bc+ad = 1 \end{cases}$ forment un système de déterminant $a^2+b^2 = 1 \neq 0$

La solution évidente est $(c,d) = (-b,a)$, c'est donc la seule et on a bien : $c^2+d^2 = 1$

On en déduit : $SO_2(\mathbb{F}_p) = \left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{matrix} a,b \in \mathbb{F}_p \\ a^2+b^2=1 \end{matrix}\right\}$

Premier cas : On suppose ici $p \equiv 1[4]$

Montrons que -1 possède une racine carrée w dans $\mathbb{F}_p$ et montrons que l'équation $x^2+y^2 = 1$ possède $p-1$ solutions dans $\mathbb{F}_p^2$

On sait, que dans ce cas, le symbole de Legendre $\left(\frac{-1}{p}\right)$ vaut $(-1)^{\frac{p-1}{2}} = 1$

On peut donc écrire $-1 = w^2$, avec $w \in \mathbb{F}_p^*$

Pour résoudre $x^2+y^2 = 1$, on peut factoriser : $x^2+y^2 = (x-wy)(x+wy)$ et faire un changement de variables :

$$\begin{cases} x' = x+wy \\ y' = x-wy \end{cases} \Leftrightarrow \begin{cases} x = \frac{x'+y'}{2} \\ y = \frac{x'-y'}{2w} \end{cases}$$

Notons que l'on a bien une bijection $(x,y) \mapsto (x',y')$ justifiée, car p est impair et donc $2 \neq 0$.

Par ce changement de variables, on obtient :

$$|SO_2(\mathbb{F}_p)| = |\{(x',y') \in \mathbb{F}_p^2,\ x'y' = 1\}|$$

À le choix de x' dans $\mathbb{F}_p^*$ détermine un et un seul couple, d'où $|SO_2(\mathbb{F}_p)| = p-1$

Montrons qu'on a l'isomorphisme suivant : $SO_2(\mathbb{F}_p) \simeq \mathbb{F}_p^*$

On vérifie que $\Psi : SO_2(\mathbb{F}_p) \to \mathbb{F}_p^*$ fournit l'isomorphisme désiré. En effet :

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a+wb$$

- $a+wb$ est non nul puisque $(a+wb)(a-wb) = 1$

• Ψ est bien un morphisme

• Ψ est injectif : en effet, si $\Psi(A) = 1$ alors $x = a + ib = 1$, puis $y = a - ib = \frac{a^2+b^2}{a+ib} = 1$

enfin $a = 1$ et $b = 0$

• Ψ est surjectif : par égalité des coordonnées.

Conclusion : Ψ est un isomorphisme de $SO_2(\mathbb{F}_p)$ sur le groupe cyclique $\mathbb{F}_p^*$.

Deuxième cas : On suppose ici que $p \equiv 3[4]$

Montrons que -1 ne possède pas de racine carrée dans $\mathbb{F}_p$ et en déduire que l'équation $x^2 + y^2 = 1$ possède $p+1$ solutions dans $\mathbb{F}_p^2$

On sait, que dans ce cas le symbole de Legendre $\left(\frac{-1}{p}\right)$ vaut $(-1)^{\frac{p-1}{2}} = -1$

Donc -1 n'est pas un carré.

Maintenant raisonnons par analogie avec des réels.

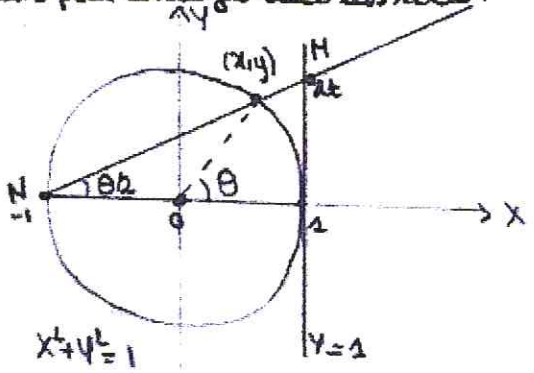

FIGURE : Paramétrage du cercle par une droite

Soit $N = (-1,0)$ dans le plan $\mathbb{F}_p^2$ et l'on note $(x;y)$ les coordonnées. Soit $t \in \mathbb{F}_p$ et $M = (1, 2t)$. La droite (NM) coupe le "cercle" :

$$S^1(\mathbb{F}_p) := \{(x,y),\ x^2 + y^2 = 1,\ x,y \in \mathbb{F}_p\}$$

en N et en un deuxième point $\pi(t)$ (sur les réels, cela revient à paramétrer le point $(x;y)$ par t).

(NM) admet pour équation $y = t(x+1)$ (on utilise $t \neq 0$), d'où l'équation aux abscisses $(1+t^2)x^2 + 2t^2 x + t^2 - 1 = 0$. C'est une équation de degré 2, car $1+t^2 \neq 0$ (-1 n'est pas un carré). La solution évidente -1 étant supprimée (elle correspond au point N), l'autre s'obtient sans calcul par le produit des racines

$x = (1-t^2)/(1+t^2)$

$y = t(x+1) = 2t/(1+t^2)$.

Inversement, pour tout point $M' = (x;y)$ de $S(\mathbb{F}_p)$ autre que N, on a : $x \neq -1$, donc la droite (NM') coupe la droite $x = 1$ en un point. Ainsi, π établit une bijection de $\mathbb{F}_p$ sur $S(\mathbb{F}_p) \setminus \{N\}$. On en déduit : $|SO_2(\mathbb{F}_p)| = |S^1(\mathbb{F}_p)| = p+1$

Soit $\mathbb{K} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, a^2+b^2 = 1, a,b \in \mathbb{F}_p \right\}$ montrons que l'équation quadratique $x^2+y^2=0$ juste une solution triviale et déduire que $\mathbb{K}$ est un corps pour les opérations usuelle des matrices.

Supposons par l'absurde $x^2+y^2=0$, avec x non nul. On a donc x inversible et une manipulation facile donne : $(x^{-1}y)^2 = -1$, ce qui est impossible car -1 n'est pas un carré. Donc x est nul et y l'est également.
On voit facilement que $\mathbb{K}$ est stable par addition et par multiplication. De plus, si une matrice de $\mathbb{K}$ est non nulle, alors $(a,b) \neq (0,0)$ et donc $a^2+b^2 \neq 0$. Si l'on sait inverser une matrice de taille 2, on trouve :

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{K}^*$$

Donc $\mathbb{K}$ est bien un corps.

Conclusion

On sait, que tout sous groupe fini du groupe multiplicatif d'un corps est cyclique cela achève la preuve, puisque dans le premier cas, $SO_2(\mathbb{F}_p) \simeq \mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ et dans le second cas, le groupe $SO_2(\mathbb{F}_p)$ est un sous groupe du groupe multiplicatif $\mathbb{K}^*$, d'ordre $p+1$.

Dev Correspondance entre $\tilde{\mathcal{F}} = \{$ drapeaux complets de $E\}$ et $\{$ p-Sylow de $GL_n(\mathbb{F}_p)\}$
où $E \simeq \mathbb{F}_p^n$

Etape 1 : Introduction

$GL(E) \curvearrowright \tilde{\mathcal{F}}$ par image directe, transitivement.
Soit $F_* := (F_0 \subset F_1 \subset \dots \subset F_n) \;/\; F_k$ sev de E de dim k.
F_* est appelé drapeau complet de E.
Comme $GL(E)$ respecte les dim et les inclusions,
$g \cdot F_* = (g(F_0) \subset \dots \subset g(F_n)) \in \tilde{\mathcal{F}}$
$id \cdot F_* = F_*$ et $g \cdot (h \cdot F_*) = (g \circ h) \cdot F_*$ st vraies
On dit que $\underline{e} = (e_1, \dots, e_n)$ est une base adaptée à F_*
lorsque $\mathrm{vect}(e_1, \dots, e_k) = F_k \;\forall k$.
Soient F_* et F_*' 2 d.c. et $\underline{e}$ et $\underline{e}'$ leur base adaptée respective.
Par conséquent $\exists\, g \in GL(E) \;/\; g(e_i) = e_i'$ et donc $g(F_k) = F_k' \;\forall k$
et donc $g \cdot F_* = F_*'$

$$GL(E) \twoheadrightarrow \tilde{\mathcal{F}}$$

Etape 2 : Stabilisateur

Considérons F_* et $\underline{e}$ une base adaptée
$g \in \mathrm{Stab}(F_*) \iff g \in GL(E)$ et $g(F_k) = F_k \;\forall k$
$\iff$ ——— $g(e_k) \in \mathrm{Vect}(e_1, \dots, e_k) \;\forall k$
$\iff$ ——— et $\mathrm{mat}_{\underline{e}}(g)$ est Δ^+ sup.
$\mathrm{Stab}(F_*) \simeq T_n^{*p}(\mathbb{F}_p) \cap GL_n(\mathbb{F}_p)$

$|\mathrm{Stab}(F_*)| = (p-1)^n \, p^{\frac{n(n-1)}{2}}$
$|\tilde{\mathcal{F}}| = |GL_n(\mathbb{F}_p)| \,/\, |\mathrm{Stab}(F_*)| = \dfrac{p^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (p^i - 1)}{p^{\frac{n(n-1)}{2}} (p-1)^n} = (p^{n-1} + \dots + 1)(p^{n-2} + \dots + 1)(\dots)(p+1)$
$= \prod_{k=1}^{n-1} \sum_{i=0}^{k} p^i$

Etape 3 : la correspondance

Soit $F_* \in \widetilde{\mathcal{F}}$. Notons $U_{F_*} \subset GL(E)$ l'ens des elem^t du stab de F_* qui s^t unipotent, ie d^t le spectre est reduit à $\{1\}$.

Mq $\widetilde{\mathcal{F}} \xrightarrow{\varphi} \{p\text{-Sylow } GL_n(\mathbb{F}_p)\}$ est une bijection.

$F_* \longmapsto U_{F_*}$

(a) Mq U_{F_*} est un p-Sylow de $GL_n(\mathbb{F}_p)$

L'ens des matrices triangulaires sup de spectre 1, ont des 1 sur leur diagonale. On voit rapidem^t que c'est bien un groupe.

$|U_{F_*}| = p^{\frac{n(n-1)}{2}}$ c'est donc un p-gp.

Comme $p \nmid p^k - 1$ $\forall k$ et p premier par Euclide $p \nmid \prod_{i=1}^{n} (p^i - 1)$

Comme $GL_n(\mathbb{F}_p)$ est un gp d'ordre $p^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (p^i - 1)$

U_{F_*} est bien un p-Sylow.

(b) Montrons l'injectivité : Mq $F_k = \bigcap_{g \in U_{F_*}} \ker((g - \mathrm{id})^k)$

Soit $g \in U_{F_*}$: $g(F_k) = F_k$, $(g - \mathrm{id})(F_k) \subset F_{k-1}$

par une récurrence immédiate $(g - \mathrm{id})^k(F_k) = \{0\}$

Donc $F_k \subset \ker((g - \mathrm{id})^k)$ $\forall g \in U_{F_*}$

Donc $F_k \subset \bigcap_{g \in U_{F_*}} \ker(g - \mathrm{id})^k$

Mq $F_k \supset \ker(g - \mathrm{id})^k$: Soit $\underline{e}$ une base adaptée à F_*

Soit g / $g(e_i) = e_i + e_{i-1}$ $\forall i$ en posant $e_0 = 0$

$(g - \mathrm{id})(e_i) = e_{i-1}$ $\forall i$ et par une nouvelle récurrence

$(g - \mathrm{id})^k(e_i) = \begin{cases} e_{i-k} & \text{si } i > k \\ 0 & \text{sinon} \end{cases}$

Soit $x \in E$, $x = \sum_{i=1}^{n} x_i e_i$

$x \in \ker((g-\mathrm{id})^k) \Rightarrow \sum_{i>k} x_i e_{i-k} = 0$

$\Rightarrow x_i = 0 \quad \forall i > k$.

$\Rightarrow x \in F_k$

$\Rightarrow \bigcap_{g \in U_{F_*}} \ker((g-\mathrm{id})^k) \subset \ker((g-\mathrm{id})^k) \subset F_k$

On a bien $F_k = \bigcap_{g \in U_{F_*}} \ker((g-\mathrm{id})^k)$

Sq $U_{F_*} = U_{F_*'} \Rightarrow \bigcap_{g \in U_{F_*}} \ker = \bigcap_{g \in U_{F_*'}} \ker \quad \forall k$

$\Rightarrow F_k = F_k' \quad \forall k \Rightarrow F_* = F_*'$

$\Rightarrow \Psi$ est inj.

© Surjectivité : Soit S un p-Sylow on veut trouver F_*^S / $U_{F_*^S} = S$

Soit $F_* \in \widetilde{\mathcal{F}}$ et U_{F_*} son p-sylow associé.
Comme les p-Sylows st conj : $\exists g \in GL(E)$ / $S = g U_{F_*} g^{-1}$

Posons $F_*^S = g \cdot F_*$. $\mathrm{Stab}(F_*^S) = g\,\mathrm{Stab}(F_*)\,g^{-1}$

Comme 2 matrices conjuguées ont le m spectre :

$U_{F_*^S} = g U_{F_*} g^{-1} = S$ □

Rmq : $|\{p\text{-Sylow}\}| = 1 \mid \widetilde{\mathcal{F}}| = (p^{n-1}+\dots+1)(\dots)(p+1) \equiv 1 [p]$.

- Tous les p-sylows st conjugués car GL_n θ transitivement

Leçons : 101 . 104 - 105 . 120

Théorème de Sylow

Réf : Perrin, Cours d'Algèbre

Théorème : (Cayley) Si G est fini de cardinal n, G est isomorphe à un sous groupe de S_n

Déf Soit G un groupe fini de cardinal n et p un diviseur premier de n. Si $n = p^k m$ avec $p \wedge m = 1$, on appelle p-Sylow de G un sous groupe de cardinal p^k.

Théorème de Sylow : Soit G un groupe fini et p un diviseur (premier) de $|G| = p^k m$ avec $p \wedge m = 1$, alors :

(i) G contient au moins un p-Sylow

(ii) Si H est un sous groupe de G qui est un p-groupe, il existe un p-Sylow S avec $H \subset S$

(iii) Les p-Sylow sont tous conjugués (et donc leur nombre $k | n$)

Démonstration = Pour montrer le (i) du théorème, nous avons besoin de deux lemmes :

Lemme 1 = Soit G un groupe avec $|G| = n = p^k m$ avec $p \wedge m = 1$ et 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

Démo du Lemme 1 : Le groupe G opère sur G/S par translation à gauche et le stabilisateur de aS est aSa^{-1}. Mais H opère lui aussi sur G/S par restriction et on a :

$$\begin{aligned} \mathrm{Stab}_H(aS) &= \{h \in H,\ haS = aS\} \\ &= \{h \in H,\ a^{-1}haS = S\} \\ &= \{h \in H\ \ a^{-1}ha \in S\} \\ &= a\,Sa^{-1} \cap H \end{aligned}$$

Il reste à voir que l'un de ces groupes est un Sylow de H. Ce sont déjà des p-groupes, il suffit donc que pour $a \in G$, $|H/(aSa^{-1} \cap H)|$ soit premier avec p.

Mais on a $|H/aSa^{-1} \cap H| = |\omega(aS)|$, cardinal de l'orbite aS dans G/S sous l'action de H. Si tous ces nombres étaient divisibles par p, il en serait de même pour $|G/S|$ car $|G/S|$ est la réunion des orbites $\omega(aS)$ (d'après l'équation des classes). Mais ceci contredit le fait que S est un p-Sylow de G. Donc p est premier avec $|H/H \cap aSa^{-1}|$ donc $H \cap aSa^{-1}$ est un p-Sylow de H ■

Lemme 2 : Soit $n \in \mathbb{N}^*$. Alors $Gl_n(\mathbb{Z}/p\mathbb{Z})$ possède un p-Sylow

Démo du Lemme 2 : Pour connaître le cardinal de $Gl_n(\mathbb{Z}/p\mathbb{Z})$ il suffit de connaître le nombre de bases du $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^n$. On a donc :

- Pour e_1, on peut choisir tout le monde sauf 0, soit $p^1 - 1$ c
- Pour e_2, _____ Vect(e_1), soit $p^2 - p$
  choix

• Pour e_n on peut choisir tout le monde sauf $Vect(e_1, \dots, e_{n-1})$, soit $p^n - p^{n-1}$ choix.

Ainsi, on a : $|Gl_n(\mathbb{Z}/p\mathbb{Z})| = (p^n-1)(p^n-p)\dots(p^n-p^{n-1})$

$= (p^n-1)\,p(p^{n-1}-1)\dots p^{n-1}(p-1)$

$= p\,p^2\dots p^{n-1}\underbrace{(p^n-1)(p^{n-1}-1)\dots(p-1)}_{m \text{ avec } p\wedge m = 1}$

$= p^{\sum_{k=1}^{n-1} k}\, m$

$= p^{\frac{n(n-1)}{2}}\, m$

On exhibe alors un p-Sylow P de $Gl_n(\mathbb{Z}/p\mathbb{Z})$. C'est l'ensemble des matrices triangulaires supérieures strictes :

$$P = \{A = (a_{ij}),\ a_{ij} = 0 \quad i > j,\ a_{ii} = 1\}$$

En effet, comme les a_{ij} pour $i<j$ sont quelconques on a :

$$|P| = p \times p^2 \times \dots \times p^{n-1} = p^{\frac{n(n-1)}{2}}$$

■

Revenons à la preuve du théorème. Soit G un groupe et p un diviseur de $|G| = n$. On plonge d'abord G dans S_n par le théorème de Cayley puis on plonge S_n dans $Gl_n(\mathbb{Z}/p\mathbb{Z})$ à l'aide de l'application suivante : $S_n \longrightarrow Gl_n(\mathbb{Z}/p\mathbb{Z})$, $\sigma \longmapsto M_\sigma$

où e_σ est défini dans la base canonique par $M_\sigma e_i = e_{\sigma(i)}$

Finalement, on a réalisé G comme sous groupe de $Gl_n(\mathbb{Z}/p\mathbb{Z})$ qui possède un p-Sylow (Lemme 2). Ainsi G possède un p-Sylow (Lemme 1).

Nous allons montrer le ii) et iii) ensemble.

Si H est un p-sous-groupe et S un p-Sylow de G, il existe en vertu du lemme 1, $a \in G$ tel que $aSa^{-1} \cap H$, soit un p-Sylow de H. Mais comme H est un p-groupe, on a $aSa^{-1} \cap H = H$ donc $H \subset aSa^{-1}$ qui est un Sylow.

Si de plus H est un Sylow, on a exactement $H = aSa^{-1}$.

Questions posées =

- Qu'est ce qu'un p-Sylow ?
- Comment appelle t-on G/S ? → ensemble des classes à gauche
- Est ce qu'un sous groupe quotienté par un p-Sylow a toujours une structure de groupe ? → Non il faut que le sous groupe par lequel on quotiente soit distingué ! Si le p-Sylow est unique alors c'est vrai.
- Quels sont les p-Sylow de $G = \mathbb{Z}/n\mathbb{Z}$ avec $n = p^k m$?
  → Si p ne divise pas m, alors G n'admet pas de p-Sylow
  → Sinon soient S_1 et S_2 deux p-Sylow de G, alors d'après le thm de Sylow, ils sont conjugués $\Leftrightarrow \exists a \in G$ tq $S_1 = a + S_2 - a = S_2$ donc il y a un unique p-Sylow dans G qui est $\{k \text{ m. } k \in [\![0, p-1]\!]\}$
- Quels sont les p-Sylow de S_p ? → S_p est de cardinal $p!$ Un p-Sylow de S_p est donc de cardinal p. C'est donc le sous groupe engendré par un p-cycle.
- Quel groupe peut un sous groupe de $Gl_n(\mathbb{Z}/p\mathbb{Z})$? → Si on effectue la multiplication de deux matrices de P, on reste dans P. Pour calculer l'inverse, on résout un système échelonnée.