7. Cas des corps finis

Soit $\mathbb{F}_q$ un corps fini à q éléments, avec $q = p^\alpha$, p premier.(★)

Prop Pour tout entier $n \geq 1$, on a les égalités de cardinaux suivantes :

(1) $|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

(2) $|SL_n(\mathbb{F}_q)| = |PGL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-2})q^{n-1}$.

(3) $|PSL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)|/d$ où $d = pgcd(n, q-1)$.

Dém (1) $GL_n(\mathbb{F}_q)$ est en bijection avec l'ensemble des bases de l'espace vectoriel $E = (\mathbb{F}_q)^n$. Or une base est composée de

un vecteur e_1 non nul : q^n-1 choix,
un vecteur e_2 n'appartenant pas à la droite $Vect(e_1)$: q^n-q choix
⋮
un vecteur e_n ——"—— au $(n-1)$-plan $Vect(e_1,\dots,e_{n-1})$: q^n-q^{n-1} choix.

La valeur de $|GL_n(\mathbb{F}_q)|$ s'en déduit.

(2) Les suites exactes $1 \to SL_n(\mathbb{F}_q) \to GL_n(\mathbb{F}_q) \xrightarrow{det} \mathbb{F}_q^\times \to 1$

$1 \to Z \simeq \mathbb{F}_q^\times \to GL_n(\mathbb{F}_q) \to PGL_n(\mathbb{F}_q) \to 1$

montrent que $|GL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)| \times |\mathbb{F}_q^\times| = |PGL_n(\mathbb{F}_q)| \times |\mathbb{F}_q^\times|$ d'où le résultat.

(3) On a une suite exacte $1 \to Z \to SL_n(\mathbb{F}_q) \to PSL_n(\mathbb{F}_q) \to 1$ où $Z = Z(SL_n)$. Or on sait (voir §4. Générateurs de GL et SL) que Z est isomorphe au groupe $\mu_n(\mathbb{F}_q)$ des racines n-ièmes de l'unité dans $\mathbb{F}_q$. Or on sait que $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$, fixons-en un générateur ω.

(★) Celles et ceux qui s'interrogent sur les raisons de ma prudence (excessive ?) pour dire « un » corps à q éléments plutôt que « le » corps à q éléments pourront lire le paragraphe « La notation $\mathbb{F}q$ et ses dangers » par Michel Demazure (tiré de son livre « Cours d'algèbre » aux éditions Cassini et mis en lien sur la page web du cours). Pour l'essentiel, les subtilités décrites par M. Demazure ne se présenteront pas dans le cours THGG et peuvent être ignorées.

Notons $d = \mathrm{pgcd}(n, q-1)$ et $n = da$, $q-1 = db$ avec $\mathrm{pgcd}(a,b) = 1$.
Un élément $x \in \mu_n(\mathbb{F}_q)$ s'écrit $x = \omega^i$ tel que $\omega^{in} = 1$. Ceci équivaut à $q-1 \mid in$, c'est-à-dire $b \mid ia$ ou encore $b \mid i$ (par Euclide).
On trouve $\mu_n(\mathbb{F}_q) = \langle \omega^b \rangle$ qui est de cardinal $\frac{q-1}{b} = d$, cqfd.

Prop (Isomorphismes exceptionnels)

(1) $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq S_3$

(2) $PGL_2(\mathbb{F}_3) \simeq S_4$ et $PSL_2(\mathbb{F}_3) \simeq A_4$

(3) $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq A_5$

(4) $PGL_2(\mathbb{F}_5) \simeq S_5$ et $PSL_2(\mathbb{F}_5) \simeq A_5$.

en fait seulement la droite projective $\mathbb{P}^1(\mathbb{F}_q) := \mathbb{P}(\mathbb{F}_q^2)$

La démonstration utilise l'espace projectif $\mathbb{P}(E)$, ensemble des droites d'un espace vectoriel. La seule chose dont on a besoin est de le dénombrer, ce qui est facile : toute droite étant dirigée par un vecteur non nul et deux tels vecteurs directeurs étant multiples par un scalaire $\lambda \in k^\times$, on a une bijection

$$E \setminus \{0\} / k^\times \simeq \{\text{vecteurs non nuls}\} / \{\text{homothéties}\} \simeq \mathbb{P}(E).$$

Lorsque $k = \mathbb{F}_q$, en prenant les cardinaux on obtient

$$|\mathbb{P}(E)| = \frac{q^n - 1}{q-1}, \quad n = \dim(E).$$

Dém de la prop : comme déjà mentionné dans le § 6 sur la simplicité de PSL, le noyau de l'action de $GL(E)$ sur $\mathbb{P}(E)$ est exactement le centre. On a donc une injection induite (pour $E = \mathbb{F}_q^2$ i.e. $n=2$) :

$$(\star) \qquad PGL_2(\mathbb{F}_q) \hookrightarrow \mathrm{Bij}(\underbrace{\mathbb{P}(\mathbb{F}_q^2)}_{\text{cardinal } q+1, \text{ cf ci-dessus.}}) \simeq S_{q+1}.$$

Prenons les points de la prop. un par un.

(1) Si $k=\mathbb{F}_2$ on a $k^\times=1$ donc $GL(E)=SL(E)=PGL(E)$ qui pour $E=\mathbb{F}_2^2$ est de cardinal 6 d'après la prop. précédente. Comme S_3 est de cardinal 6 également, l'injection (⋆) est bijective.

(2) De même $PGL_2(\mathbb{F}_3)\hookrightarrow S_4$ et les deux groupes sont de cardinal 24. Comme $PSL_2(\mathbb{F}_3)$ est d'indice 2 et S_4 possède A_4 pour <u>seul</u> sous-groupe d'indice 2, on déduit $PSL_2(\mathbb{F}_3)\simeq A_4$.

(3) Ici $q=4$ et $n=2$ donc $d=\mathrm{pgcd}(n,q-1)=1$. Ceci entraîne $\mu_n(\mathbb{F}_q)$ et $SL_2(\mathbb{F}_4)=PSL_2(\mathbb{F}_4)=PGL_2(\mathbb{F}_4)$. L'injection $PGL_2(\mathbb{F}_4)\hookrightarrow S_5$ (Card = 60 ↑, Card = 120 ↑)

réalise $PGL_2(\mathbb{F}_4)$ comme sous-groupe d'indice 2 de S_5 donc $\simeq A_5$

(4) Ici $k=\mathbb{F}_5$ et l'injection $PGL_2(\mathbb{F}_5)\hookrightarrow S_6$ (120 ↑, ↑ 720) réalise PGL comme un sous-groupe d'indice 6. Un exercice classique montre que les sous-groupes d'indice n de S_n sont isomorphes à S_{n-1} donc $PGL_2(\mathbb{F}_5)\simeq S_5$. Le sous-groupe $PSL_2(\mathbb{F}_5)$, d'indice 2, est nécess. isomorphe à A_5 ☒

Rem Comme S_3 et A_4 ne sont pas simples, on voit que la simplicité de PSL est bien en défaut pour $n=2$, $k=\mathbb{F}_2$ et $n=2$, $k=\mathbb{F}_3$.

<u>Nous allons terminer cette section</u> en observant qu'il est facile de trouver un p-Sylow pour $GL_n(\mathbb{F}_p)$ et que cela permet de démontrer l'existence des p-Sylow pour tout G fini. On rappelle:

<u>Déf</u> Soit p un nombre premier. Soit G un groupe fini d'ordre $n=p^\alpha m$ avec $\alpha\geq 0$ et $p\nmid m$. On appelle p-sous-groupe de Sylow (ou p-Sylow) de G un sous-groupe d'ordre p^α.

Un p-Sylow est donc un sous-groupe $H \subset G$ d'ordre égal à la plus grande puissance de p qui divise $|G|$. Ou encore, un sous-groupe H tel que $\begin{cases} |H| \text{ est puissance de } p, \text{ et} \\ [G:H] \text{ est premier à } p. \end{cases}$

Lemme Dans $GL_n(\mathbb{F}_p)$, le sous-groupe $S = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}$ des matrices triangulaires supérieures unipotentes est un p-Sylow.

Dém : en effet, son ordre est $p^{1+2+\dots+(n-1)}$ qui est égal à la plus grande puissance de p qui divise $|GL_n(\mathbb{F}_p)| =$

$$(p^n-1)(p^n-p)\dots(p^n-p^{n-1}) = p^{1+2+\dots+(n-1)}\left((p^n-1)(p^{n-1}-1)\dots(p-1)\right) \boxtimes$$

Lemme (Perrin, Chapitre I, Lemme 5.5)
Soit G un groupe avec $|G| = n = p^\alpha m$, avec $p \nmid m$ et soit H un sous-groupe de G. Soit 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. Le groupe G opère sur G/S par translation à gauche (cf. §4 Exemple C) et le stabilisateur de aS est aSa^{-1}. Mais H opère lui aussi sur G/S par restriction, avec comme stabilisateur de aS, $aSa^{-1} \cap H$.
Il reste à voir que l'un de ces groupes est un Sylow de H. Ce sont déjà des p-groupes et il suffit donc que, pour un $a \in G$, $|H/(aSa^{-1} \cap H)|$ soit premier à p.
Mais on a, d'après 4.7, $|H/aSa^{-1} \cap H| = |\omega(aS)|$, cardinal de l'orbite de aS dans G/S sous l'action de H. Si tous ces nombres étaient divisibles par p, il en serait de même de $|G/S|$ car G/S est réunion des orbites $\omega(aS)$. Mais ceci contredit le fait que S est un p-Sylow de G.

Théorème : tout groupe fini possède un p-sous-groupe de Sylow.

Dém on considère les morphismes injectifs de groupes ($n = |G|$) :

$$G \xhookrightarrow[\text{de Cayley}]{\text{théorème}} \mathfrak{S}_{|G|} \simeq \mathfrak{S}_n \xhookrightarrow{} GL_n(\mathbb{F}_p)$$

$$g \longmapsto \left(L_g : \begin{array}{c} G \to G \\ x \mapsto gx \end{array}\right) \qquad \sigma \longmapsto \left(\text{Matrice de permutation } M_\sigma\right)$$

Le premier lemme fournit un p-Sylow $S \subset GL_n(\mathbb{F}_p)$ et le second lemme fournit un p-Sylow $aSa^{-1} \cap G$ pour G $\boxtimes$