

Isomorphismes exceptionnels des groupes linéaires projectifs et un cas fini.

[PER] p105

Recherches: 101, 102, 104, 106, 103, 190, 191, 105

Proposition:

①

- (1) $|GL_n(\mathbb{F}_q)| = (q^n - 1) \dots (q^n - q^{n-1})$;
- (2) $|SL_n(\mathbb{F}_q)| = (q^n - 1) \dots (q^n - q^{n-2}) q^{n-1} = N$;
- (3) $|PGL_n(\mathbb{F}_q)| = N$
- (4) $|PSL_n(\mathbb{F}_q)| = N/d$, $d = \text{pgcd}(n, q-1)$.

Preuve:

(1) Soit $B = (e_1, \dots, e_n)$ base de $\mathbb{F}_q^n$.

L'application qui à $A \in GL_n(\mathbb{F}_q)$ associe $Ae_1, \dots, Ae_n$ réalise une bijection de $GL_n(\mathbb{F}_q)$ dans l'ensemble des bases de $\mathbb{F}_q^n$.

(On compte donc le nombre de bases de $\mathbb{F}_q^n$)

$(a_1, \dots, a_n)$ une base de $\mathbb{F}_q^n$. On prend a_1 non nul, $q^n - 1$ choix.

On prend a_2 dans le droite (dimension 1) engendrée par a_1 , $q^n - q$ choix.

Jusqu'à prendre $a_n \notin \text{Vect}(a_1, \dots, a_{n-1})$, $q^n - q^{n-1}$ choix.

D'où le résultat

$$|\mathbb{F}_q^{\times}| = q-1 \text{ donne 2) et 3)}$$

Par 4, on démontre le lemme suivant:

②

Lemme:

$$|\mu_n(\mathbb{F}_q)| = d, \quad d = \text{pgcd}(n, q-1)$$

Preuve:

$$\text{M}_q \mu_n(\mathbb{F}_q) = \text{Ord}(\mathbb{F}_q).$$

">": Clair.

"<": Soit $\lambda \in \mu_n(\mathbb{F}_q)$ $\lambda^n = 1$.

Par Lagrange, $\lambda^{q-1} = 1$

D'après Bézout, $\exists (u, v) \in \mathbb{Z}^2$ tq $un + v(q-1) = d$.

$$\text{Puis on a: } \lambda^d = \lambda^{un + v(q-1)} = (\lambda^n)^u (\lambda^{q-1})^v = 1.$$

D'où l'égalité.

$$\text{D'où } |\mu_n(\mathbb{F}_q)| = |\text{Ord}(\mathbb{F}_q)| = d.$$

Iq comme ça dans les leçons de groupe

2.6

$$\text{Posons } d = \text{pgcd}(n, q-1) \\ a = |\mu_n(\mathbb{F}_q)|$$

a | d:
 $a \mid n$ par construction
 $\mu_n(\mathbb{F}_q) \subseteq \mathbb{F}_q^{\times}$ il est donc cyclique d'ordre $a \mid q-1$.
Donc $a \mid d$.

Soit $x \in \mathbb{F}_q^{\times}$ d'ordre $q-1$.
Alors $x^{(q-1)/d}$ est d'ordre d .

On $z^{(q-1)/d} \in \mu_n(\mathbb{F}_q)$ donc
 $\langle z^{(q-1)/d} \rangle \subseteq \mu_n(\mathbb{F}_q)$ donc

$$d \mid |\mu_n(\mathbb{F}_q)| = a.$$

Donc $a = d$

On revient à 4/ :

$$|PSL_n(\mathbb{F}_q)| = \frac{|SL_n(\mathbb{F}_q)|}{|\mu_n(\mathbb{F}_q)|} = N/d$$

□

* Groupe cyclique dans le groupe des racines de $X^n - 1$.

Remarque :

$m=2$ $q=$	2	3	4	5
$GL_2(\mathbb{F}_q)$	6	48	180	480
$SL_2(\mathbb{F}_q)$	6	24	60	120
$PGL_2(\mathbb{F}_q)$	6	24	60	120
$PSL_2(\mathbb{F}_q)$	6	12	60	60

Inomorphismes.	2	3	4	5
$GL_2(\mathbb{F}_q)$	G_3	X	X	X
$SL_2(\mathbb{F}_q)$	G_3	X	X	X
$PGL_2(\mathbb{F}_q)$	G_3	G_4	G_5	G_5
$PSL_2(\mathbb{F}_q)$	G_3	G_4	G_5	G_5

(5)

Proposition

- 1) $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PGL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \cong G_3$;
- 2) $PGL_2(\mathbb{F}_3) \cong G_4$, $PSL_2(\mathbb{F}_3) \cong 2G_4$;
- 3) $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \cong 2G_5$;
- 4) $PGL_2(\mathbb{F}_5) \cong G_5$, $PSL_2(\mathbb{F}_5) \cong 2G_5$.

Preuve :

On considère l'action $\mathbb{F}_q^* \times \mathbb{F}_q^n \setminus \{0\} \rightarrow \mathbb{F}_q^n \setminus \{0\}$
 $(\lambda, x) \mapsto \lambda x$
 et on note $P(\mathbb{F}_q^n) = (\mathbb{F}_q^n \setminus \{0\}) / \mathbb{F}_q^*$ l'ensemble des orbites pour cette action.

On considère l'action de $GL_n(\mathbb{F}_q) \times P(\mathbb{F}_q^n) \rightarrow P(\mathbb{F}_q^n)$
 $(g, [x]) \mapsto [gx]$

qui induit le morphisme $\Psi : GL_n(\mathbb{F}_q) \rightarrow G(P(\mathbb{F}_q^n)) \cong G_{q^n-1}^{n-1}$

On étudie $\text{Ker}(\Psi)$.

$g \in \text{Ker} \Psi$ si $\forall x \in \mathbb{F}_q^n$, (x, gx) est l'orbite, i.e. : g est une homothétie.

Donc $\text{Ker} \Psi = Z(GL_n(\mathbb{F}_q))$. Cela induit $\tilde{\Psi} : PGL_n(\mathbb{F}_q) \hookrightarrow G(P(\mathbb{F}_q^n))$ par le 1^{er} thm d'isomorphisme.

Ici $n=2$ et on a $PGL_2(\mathbb{F}_q) \hookrightarrow G_{q+1}$
 injection

On conclut :

1) $\mathbb{F}_2^* = \{1\}$ donc les groupes sont égaux de cardinal 6 et s'injectent dans G_3 , d'où le résultat.

2) $PGL_2(\mathbb{F}_3) \hookrightarrow G_4$ et est de cardinal 24, d'où le résultat.
 $|PSL_2(\mathbb{F}_3)| = 12$, il est donc isomorphe à un sous-groupe d'indice 2 de G_4 , $2G_4$ étant le seul tel π -groupe, on a le résultat.

3) $\mathbb{F}_4 = \mathbb{F}_2[x]$ avec x racine de $X^2 + X + 1 \in \mathbb{F}_2[X]$. Donc on a :
 $\mathbb{F}_4^* = \{1, x, 1+x\} = \mathbb{F}_4^{*2}$ et on a la suite exacte :

$$1 \rightarrow PSL_2(\mathbb{F}_4) \rightarrow PGL_2(\mathbb{F}_4) \rightarrow \mathbb{F}_4^* / \mathbb{F}_4^{*2} \rightarrow 1$$

Donc $PSL_2(\mathbb{F}_4) = PGL_2(\mathbb{F}_4) \hookrightarrow G_5$ de cardinal 60, d'où le résultat.

4) $PGL_2(\mathbb{F}_5) \hookrightarrow G_6$ d'indice 6 donc isomorphe à G_5 par la proposition.
 $PSL_2(\mathbb{F}_5)$ est isomorphe à un π -groupe d'indice 2 de G_5 , donc à $2G_5$.

□

③ Théorème:
 Soit $H < G_m$ d'indice m .
 $H \cong G_{m-1}$.

Perrin. Page 30

Preuve:

~~G opère sur G/H transitivement~~

Pour $m = 2$ et $m = 3$, l'assertion est évidente.

Pour $m = 4$, $|G/H| = 6$ donc $H \cong G_3$ ou $H \cong \mathbb{Z}/6\mathbb{Z}$.

La seconde étant impossible car G_3 n'a pas d'éléments d'ordre 6, nécessairement $H \cong G_3$.

Supposons $m \geq 5$. On pose $G = G_m$.

Alors G opère transitivement sur G/H , avec $|G/H| = m$.

Cela induit le morphisme $\varphi: G \rightarrow G(G/H) \cong G_m$.

Montrons que φ est injectif.

On a $\text{Ker } \varphi = \bigcap_{a \in G} aHa^{-1} \in H$ donc $|\text{Ker } \varphi| \leq (m-1)!$

Or $\text{Ker } \varphi \triangleleft G$ et $|G| = \frac{m!}{2}$ et

$(m-1)! < \frac{m!}{2}$ donc $\text{Ker } \varphi = \{1\}$

Par égalité des cardinaux, φ est un isomorphisme.

Finalement, H est le stabilisateur de $\bar{1} = H$.

Donc $\varphi(H)$ est le stabilisateur d'un point dans G_m , il est donc isomorphe à G_{m-1} .

Finalement, $H \cong \varphi(H) \cong G_{m-1}$.

④

Lemme:

Pemir p 98

Gm a la suite exacte:

$$1 \rightarrow \mathrm{PSL}(E) \rightarrow \mathrm{PGL}(E) \xrightarrow{\det} k^*/(k^*)^n \rightarrow 1$$

Preuve: