Isomorphismes exceptionnels

Achille Méthivier

Théorème 1. *On a les isomorphismes suivants :*

1. $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathscr{S}_3$.
2. $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathscr{S}_4$; $\quad \mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathscr{A}_4$.
3. $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathscr{A}_5$.
4. $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathscr{S}_5$; $\quad \mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathscr{A}_5$.

Lemme 2. *Soit k un corps et E un k-espace vectoriel. On a la suite exacte courte suivante*

$$1 \to \mathrm{PSL}(E) \to \mathrm{PGL}(E) \to k^*/k^{*n} \to 1,$$

où $k^{*n} = \{x \in k^* \ : \ \exists y \in k^* \ x = y^n\}$.

Démonstration. On a la suite exacte suivante :

$$1 \to \mathrm{SL}(E) \to \mathrm{GL}(E) \xrightarrow{\det} k^* \to 1.$$

Or $\det(Z(\mathrm{GL}(E)) = \det(k^*\mathrm{Id}) = k^{*n}$. On a donc un morphisme surjectif $\widetilde{\det} : \mathrm{GL}(E) \to k^*/k^{*n}$ qui vérifie $Z(\mathrm{GL}(E)) \subset \ker(\widetilde{\det})$ et il passe au quotient en $\overline{\det} : \mathrm{PGL}(E) \to k^*/k^{*n}$. Or, $\ker(\overline{\det}) = \{[g] \in \mathrm{PGL}(E) : \det(g) \in k^{*n}\}$, donc pour $[g] \in \ker(\overline{\det})$, on dispose de $x \in k^*$ tel que $\det(g) = x^n$, donc $x^{-1}g \in \mathrm{SL}(E)$ d'où $[g] \in \mathrm{PSL}(E)$. L'inclusion réciproque étant évidente, on a bien la suite exacte voulue. □

Lemme 3. *Les cardinaux des groupes linéaires sur $\mathbb{F}_q$ sont les suivants :*

1. $\#\mathrm{GL}_n(\mathbb{F}_q) = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$.
2. $\#\mathrm{SL}_n(\mathbb{F}_q) = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})q^{n-1} = N$.
3. $\#\mathrm{PGL}_n(\mathbb{F}_q) = \#\mathrm{SL}_n(\mathbb{F}_q) = N$.
4. $\#\mathrm{PSL}_n(\mathbb{F}_q) = N/d$ *où* $d = n \wedge q - 1$

Démonstration. Soit $B = (e_1, \dots, e_n)$ une base de $\mathbb{F}_q^n$. L'application qui à $A \in \mathrm{GL}_n(\mathbb{F}_q)$ associe $Ae_1, \dots Ae_n$, les images par A des vecteurs de la base B est une bijection de $\mathrm{GL}_n(\mathbb{F}_q)$ dans l'ensemble des bases de $\mathbb{F}_q^n$. Pour choisir une base $(a_1, \dots, a_n)$ de $\mathbb{F}_q^n$, on peut prendre n'importe quel vecteur non nul a_1 donc $q^n - 1$ choix. La seule condition pour a_2 et qu'il ne soit pas dans le $\mathrm{Vect}(a_1)$ qui est de cardinal q, donc $q^n - q$ choix. On itérant ce raisonnement, on obtient le résultat 1.. Ensuite, comme $\#\mathbb{F}_q^* = q - 1$, les résultats 2. et 3. s'en suivent. Maintenant on sait que $\#\mathrm{PSL}_n(\mathbb{F}_q) = \#SL_n(\mathbb{F}_q)/\#\mu_n(\mathbb{F}_q)$ où $\mu_n(\mathbb{F}_q)$ est l'ensemble des racines n-èmes de l'unité dans $\mathbb{F}_q$. Comme $d|n$, on $\mu_d(\mathbb{F}_q) \subset \mu_n(\mathbb{F}_q)$. Soit maintenant $x \in \mu_n(\mathbb{F}_q)$, et on dispose de $(u, v) \in \mathbb{Z}^2$ tel que $d = un + v(q-1)$, donc $x^d = (x^n)^u(x^{q-1})^v$ et comme $x^n = x^{q-1} = 1$, on a bien $x^d = 1$ donc $\mu_d(\mathbb{F}_q) = \mu_n(\mathbb{F}_q)$. Or $Z(\mathrm{SL}(\mathbb{F}_q)) = \mu_n(\mathbb{F}_q)I_n$, donc $\#\mathrm{PSL}_n(\mathbb{F}_q) = N/d$. □

Démonstration du théorème. Considérons l'action de $\mathbb{F}_q^*$ par translation sur $\mathbb{F}_q^{n\setminus\{0\}}$

$$\begin{array}{ccc} \mathbb{F}_q^* \times \mathbb{F}_q^{n\setminus\{0\}} & \to & \mathbb{F}_q^{n\setminus\{0\}} \\ (\lambda, x) & \mapsto & \lambda x, \end{array}$$

et notons $\mathbb{P}(\mathbb{F}_q^n) = \mathbb{F}_q^{n\setminus\{0\}}/\mathbb{F}_q^*$ l'ensemble des orbites pour cette action. Le groupe $\mathrm{GL}_n(F_q)$ agit alors aussi sur $\mathbb{P}(\mathbb{F}_q^n)$ comme suit

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{F}_q) \times \mathbb{P}(\mathbb{F}_q^n) & \to & \mathbb{P}(\mathbb{F}_q^n) \\ (g, [x]) & \mapsto & [gx], \end{array}$$

(on vérifie aisément que l'action est bien définie) ce qui donne le morphisme de groupes suivant

$$\varphi : \mathrm{GL}_n(\mathbb{F}_q) \to \mathscr{S}(\mathbb{P}(\mathbb{F}_q)).$$

Regardons le noyau de ce morphisme. Soit $g \in \ker(\varphi)$, alors pour tout $[x] \in \mathbb{P}(\mathbb{F}_q^n)$ on a $[gx] = x$ autrement dit la famille (gx, x) est liée. Il est alors bien connu que g est une homothétie, donc $\ker(\varphi) = \mathbb{F}_q^* I_n$. Par le premier théorème d'isomorphismes, on obtient un morphisme de groupes injectif

$$\tilde{\varphi} : \mathrm{PGL}_n(\mathbb{F}_q) \to \mathscr{S}(\mathbb{P}(\mathbb{F}_q^n)) \simeq \mathscr{S}_{(q^n-1)/(q-1)}.$$

Dans le particuliers qui nous intéresse où $n = 2$, on a

$$\tilde{\varphi} : \mathrm{PGL}_2(\mathbb{F}_q) \to \mathscr{S}_{q+1}.$$

Il est temps de récolter ce que l'on a semé :

1. Pour $q = 2$, on a $\mathbb{F}_2^* = \{1\}$, les groupes linéaires sont donc tous égaux de cardinal 6 et s'injectent dans $\mathscr{S}_3$ et lui sont donc isomorphes.
2. Pour $q = 3$, on a $\#\mathrm{PGL}_2(\mathbb{F}_3) = 24$ et le même raisonnement prouve que $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathscr{S}_4$. De plus $\#\mathrm{PSL}_2(\mathbb{F}_3) = 12$ et donc $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathscr{A}_4$ car c'est le seul sous-groupe d'indice 2 dans $\mathscr{S}_4$.

3. Pour $q = 4$, en appliquant le lemme 2, on obtient la suite exacte suivante :

$$1 \to \mathrm{PSL}_2(\mathbb{F}_4) \to \mathrm{PGL}_2(\mathbb{F}_4) \to \mathbb{F}_4^*/\mathbb{F}_4^{*2} \to 1.$$

   Or, $\mathbb{F}_4 = \mathbb{F}_2[x]$ où x est une racine de $X^2 + X + 1 \in \mathbb{F}_2[X]$. On a donc $\mathbb{F}_4 = \{0, 1, x, x+1\}$ et on voit que $\mathbb{F}_4^{*2} = \{1, x, x+1\} = \mathbb{F}_4^*$ d'où $\mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{PGL}_2(\mathbb{F}_4)$. Et comme $\mu_2(\mathbb{F}_4) = \{1\}$ on a $\mathrm{SL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4)$. Ces trois groupes sont de cardinal 60, donc leur image est d'indice 2 dans $\mathscr{S}_5$, autrement dit, ils sont isomorphes à $\mathscr{A}_5$.

4. Pour $q = 5$, comme $\#\mathrm{PGL}_2(\mathbb{F}_5) = 120$, l'image de $\mathrm{PGL}_2(\mathbb{F}_5)$ par $\tilde{\varphi}$ est un sous-groupe de $\mathscr{S}_6$ d'indice 6, donc isomorphe à $\mathscr{S}_5$. Et comme $\#\mathrm{PSL}_2(\mathbb{F}_5) = 60$, il en découle que $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathscr{A}_5$.

$\square$

I Références

1. Cours d'algèbre, Daniel Perrin (page 106).