2.2 Isomorphismes exceptionnels

Leçons concernées : 101, 103, 104 (?), 105, 106, 123 (?), 190, 191

Théorème 5. *On a les isomorphismes exceptionnels :*

1. $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$.
2. $PSL2(\mathbb{F}_3) \simeq \mathfrak{A}_4$.
3. $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$.
4. $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5 \simeq PSL_2(\mathbb{F}_5)$.
5. $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$.

Preuve : On a une action naturelle de $GL_2(K)$ sur la droite projective $\mathbb{P}^1(K)$ (l'ensemble des droites vectorielles de K^2), cela donne un morphisme :

$$\varphi : GL_2(K) \longrightarrow \mathfrak{S}\big(\mathbb{P}^1(K)\big)$$

Soit $u \in \mathrm{Ker}(\varphi)$, alors u stabilise toutes les droites vectorielles de K^2. Cela est un résultat classique d'établir que u est alors une homothétie et donc, on a $\mathrm{Ker}(\varphi) = K^*$. Ainsi, on a un isomorphisme

$$PGL_2(K) \simeq GL_2(K)/K^* \xrightarrow{\simeq} \mathbb{P}^1(K)$$

On va appliquer ce résultat aux corps finis $K = \mathbb{F}_q$ et utiliser un argument de dénombrement. D'où :

Lemme 6. *Soit $\mathbb{F}_q$ le corps à q éléments. Alors,*

1. *L'espace projectif $\mathbb{P}^n(\mathbb{F}_q)$ a $\dfrac{q^{n+1}-1}{q-1}$ éléments. En particulier, la droite projective a $q+1$ éléments.*
2. *Le groupe général linéaire $GL_n(\mathbb{F}_q)$ a $(q^n-1)(q^n-q)...(q^n-q^{n-1})$ éléments.*
3. *Le groupe projectif linéaire $PGL_n(\mathbb{F}_q)$ et le groupe spécial linéaire $SL_n(\mathbb{F}_q)$ ont $\dfrac{(q^n-1)(q^n-q)...(q^n-q^{n-1})}{q-1}$ éléments.*
4. *Le groupe projectif spécial linéaire $PSL_n(\mathbb{F}_q)$ a $\dfrac{(q^n-1)(q^n-q)...(q^n-q^{n-1})}{(q-1)\cdot \mathrm{pgcd}(n,q-1)}$ éléments.*

Preuve du lemme :

1. On peut évoquer la décomposition $\mathbb{P}^n(K) \simeq K^n \sqcup K^{n-1} \sqcup ... \sqcup K^1 \sqcup \{0\}$. Mais faisons pluitôt naturellement agir K^* sur $K^{n+1} \setminus \{0\}$ par homothéties. Il s'agit d'une action libre, on en déduit que

$$\mathrm{Card}\big(\mathbb{P}^n(\mathbb{F}_q)\big) = \frac{\mathrm{Card}\big(\mathbb{F}_q^{n+1} \setminus \{0\}\big)}{\mathrm{Card}\big(\mathbb{F}_q^*\big)} = \frac{q^{n+1}-1}{q-1}$$

2. On peut rendre l'argument de dénombrement “je choisis les colonnes de sorte qu'ils forment une base” plus avancé en considérant l'action de $GL_n(K)$ sur $K^n \setminus \{0\}$. Il s'agit d'une action transitive et on a

$$\mathrm{Stab}\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} = \begin{pmatrix}1 & K^{n-1}\\ 0 & GL_{n-1}(K)\end{pmatrix} \simeq K^{n-1} \rtimes GL_{n-1}(K)$$

Et on en déduit que

$$\mathrm{Card}\Big(GL_n(\mathbb{F}_q)/\big(\mathbb{F}_q^{n-1} \rtimes GL_{n-1}(\mathbb{F}_q)\big)\Big) = \mathrm{Card}\big(\mathbb{F}_q^n \setminus \{0\}\big)$$

et donc, on a

$$\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big) = q^{n-1}(q^n-1)\mathrm{Card}\big(GL_{n-1}(\mathbb{F}_q)\big) = (q^n-q^{n-1})\mathrm{Card}\big(GL_{n-1}(\mathbb{F}_q)\big)$$

3. On a

$$PGL_n(\mathbb{F}_q) = GL_n(K)/K^* \qquad \text{et} \qquad GL_n(K)/SL_n(K) \simeq \mathrm{Im}(\det) = K^*$$

D'où les résultats.

4. On rappelle que $PSL_n(\mathbb{F}_q) = SL_n(\mathbb{F}_q)/Z\big(SL_n(\mathbb{F}_q)\big)$ et que $Z\big(SL_n(\mathbb{F}_q)\big)$ est constitué des homothéties dont le rapport est une racine n-ième de l'unité. Il suffit donc de compter le nombre de racines n-ième de l'unité de $\mathbb{F}_q$.
   Soit $d = \text{pgcd}(n, q-1)$, par Bézout, on peut écrire $d = r(q-1) + sn$ avec $r, s \in \mathbb{Z}$. Soit $x \in \mathbb{F}_q^*$, on a $x^{q-1} = 1$, donc si x est une racine n-ième de l'unité, on a
$$x^d = x^{(q-1)r} x^{ns} = 1$$
   Réciproquement, si $x^d = 1$, alors $x^n = 1$. Il y a donc autant de racines n-ièmes de l'unité que de racines d-ième de l'unité dans $\mathbb{F}_q$. Le polynôme $X^{q-1} - 1$ admet $q-1$ racines dans $\mathbb{F}_q$, donc $X^d - 1$ qui en est un diviseur en a d, donc il y a d racines n-ième de l'unité dans $\mathbb{F}_q$. □

Nous pouvons retourner à notre résultat initial et on a alors un morphisme injectif
$$PGL_2(\mathbb{F}_q) \longrightarrow \mathfrak{S}\big(\mathbb{P}^1(\mathbb{F}_q)\big) \simeq \mathfrak{S}_{q+1}$$

1. On a $PGL_2(\mathbb{F}_2) = GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2)$ car det est le morphisme trivial. Étant de cardinal 6, on en déduit que
$$GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$$
2. $PGL_2(\mathbb{F}_3)$ a 24 éléments : autant que $\mathfrak{S}_4$, d'où
$$PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$$
   et de plus $PSL_2(\mathbb{F}_3)$ est d'indice 2 dans $PGL_2(\mathbb{F}_3)$, et comme $\mathfrak{A}_4$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_4$ et donc
$$PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$$
3. $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4)$ car 1 est son unique racine carrée dans $\mathbb{F}_4$. On vérifie alors que $PGL_2(\mathbb{F}_4)$ est d'indice 2 dans $\mathfrak{S}_5$ par cardinalité, donc nécessairement, on a
$$PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$$
4. Par cardinalité, on vérifie que $PGL_2(\mathbb{F}_5)$ est d'indice 6 dans $\mathfrak{S}_6$, donc il est isomorphe à $\mathfrak{S}_5$ et enfin comme $PSL_2(\mathbb{F}_5)$ est d'indice 2 dans $\mathfrak{S}_5$, il est isomorphe à $\mathfrak{A}_5$, d'où
$$PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5 \qquad \text{et} \qquad PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$$

□

Références :

- D. Perrin, Cours d'algèbre.
- H2G2, Tome 1.

Stratégie de présentation : On a pas mal de temps pour présenter ce résultat. Il faut bien connaître les implications de ces résultats (simplicité de $PSL_n(K)$ ainsi que description algébrique/géométrique de $PSL_2(\mathbb{F}_5)$ qui est le plus petit groupe simple).