Groupe projectif (spécial) linéaire et groupe symétrique

Abandonné

Dans tout ce qui suit, $p \in \{2, 3\}$, et G est l'un des groupes de matrices $\mathbb{P}GL_2(\mathbb{F}_p)$ ou $\mathbb{P}SL_2(\mathbb{F}_p)$.

Théorème (Trois isomorphismes exceptionnels)

1. $\mathbb{P}SL_2(\mathbb{F}_2) \simeq S_3$
2. $\mathbb{P}GL_2(\mathbb{F}_3) \simeq S_4$
3. $\mathbb{P}SL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$

Voici le plan de la démonstration:

1. Montrer les Lemmes 1 et 2.
2. A l'aide d'une action fidèle sur $\mathbb{P}(\mathbb{F}_p^2)$ (droites vectorielles du $\mathbb{F}_p-$espace vectoriel $\mathbb{F}_p^2$), montrer les isomorphismes.

Lemme 1

Soit $\mathbb{K}$ un corps et soit $u \in End_{\mathbb{K}}(E)$ (E est un $\mathbb{K}-$espace vectoriel de dimension finie). Si u préserve toute droite de E alors u est une homothétie.

Démonstration. *Soient $x, y \in E$. Comme $x \in Vect\{x\}$ et $y \in Vect\{y\}$, ils existent $\lambda_x, \lambda_y \in \mathbb{K}$ tels que $u(x) = \lambda_x x$ et $u(y) = \lambda_y y$. Or, $u(x+y) = \lambda_x x + \lambda_y y$, et $x + y \in Vect\{x+y\}$ donc il existe $\lambda \in \mathbb{K}$ tel que $u(x+y) = \lambda(x+y)$. Donc $\lambda_x = \lambda_y = \lambda$ et $u = \lambda Id_E$*

■

Lemme 2

Si G agit sur $\mathbb{P}(\mathbb{F}_p^2)$ via l'action:

$$\overline{P} \cdot \mathcal{D} = \{Px, x \in \mathcal{D}\}$$

alors cette action est fidèle, i.e. $\overline{P} \cdot \mathcal{D} = \mathcal{D} \Rightarrow \overline{P} = \overline{I_2}$.

En d'autres termes, le morphisme $\rho : G \longrightarrow S_n$, où $n = |\mathbb{P}(\mathbb{F}_p^2)|$, est injectif.

Démonstration. *Soit $\overline{P}$ un élément de G. Soit $\mathcal{D} \in \mathbb{P}(\mathbb{F}_p^2)$ telle que $\overline{P} \cdot \mathcal{D} = \mathcal{D}$. Alors, pour tout $x \in \mathcal{D} \backslash \left\{0_{\mathbb{F}_p^2}\right\}$, $\overline{P}x \in \mathcal{D} = Vect\{x\}$, donc P conserve toute droite de $\mathbb{F}_p^2$. Par le lemme 1, $\overline{P}$ est une homothétie, mais $G = \frac{GL_2(\mathbb{F}_p)}{\left\{\alpha I_2, \alpha \in \mathbb{F}_p^\times\right\}}$ ou $\frac{SL_2(\mathbb{F}_p)}{\{-I_2, I_2\}}$, donc $\overline{P} = \overline{I_2}$, ce qui conclut.*

■

On prouve maintenant le théorème:

Démonstration. *1. On sait que, puisque $\mathbb{F}_2^\times = \{\overline{1}\}$, alors $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2)$ et $\{-1,1\} = \{1\}$ donc on a:*

$$|\mathbb{P}SL_2(\mathbb{F}_2)| = \frac{|SL_2(\mathbb{F}_2)|}{|\{-1,1\}|} = |SL_2(\mathbb{F}_2)| = |GL_2(\mathbb{F}_2)| = |\left\{Basees\ de\ \mathbb{F}_2^2\right\}| = 3\times 2 = 6$$

De plus, $\mathbb{P}(\mathbb{F}_2^2) = \{\langle(1,0)\rangle, \langle(1,1)\rangle, \langle(0,1)\rangle\}$ donc $|\mathbb{P}(\mathbb{F}_2^2)| = 3$, et, puisque $\mathbb{P}SL_2(\mathbb{F}_2)$ agit sur $\mathbb{P}(\mathbb{F}_2^2)$, on a alors le morphisme:

$$\rho : \mathbb{P}SL_2(\mathbb{F}_2) \longrightarrow S_3$$

Par le lemme 2, ce morphisme est injectif, et $|\mathbb{P}SL_2(\mathbb{F}_2)| = |S_3| = 6$, donc ρ est bijectif.

2. On sait que:

$$|\mathbb{P}GL_2(\mathbb{F}_3)| = \frac{|GL_2(\mathbb{F}_3)|}{|\{I_2, 2I_2\}|} = \frac{|\{Bases\ de\ \mathbb{F}_3^2\}|}{2} = \frac{(9-1)\times(9-3)}{2} = 24$$

De plus, $\mathbb{P}(\mathbb{F}_3^2) = \{\langle(1,0)\rangle, \langle(0,1)\rangle, \langle(1,1)\rangle, \langle(1,2)\rangle\}$ donc $|\mathbb{P}(\mathbb{F}_3^2)| = 4$, et, puisque $\mathbb{P}\mathbb{P}GL_2(\mathbb{F}_3)$ agit sur $\mathbb{P}(\mathbb{F}_3^2)$, on a alors le morphisme:

$$\rho' : \mathbb{P}GL_2(\mathbb{F}_2) \longrightarrow S_4$$

Par le lemme 2, ce morphisme est injectif, et $|\mathbb{P}GL_2(\mathbb{F}_3)| = |S_4| = 24$, donc ρ' est bijectif.

3. Soit $\overline{\det} : \mathbb{P}GL_2(\mathbb{F}_3) \longrightarrow \mathbb{F}_3^\times = \{-1,1\}$. C'est un morphisme de groupes.

- ⋆ *Soit $\overline{P} \in \ker(\overline{\det})$. $\overline{\det}(\overline{P}) = 1$, mais $\mathbb{P}GL_2(\mathbb{F}_3) = \frac{GL_2(\mathbb{F}_3)}{\{-I_2, I_2\}}$, donc $P \in GL_2(\mathbb{F}_3)$ et $\det(P) = 1$, d'où $P \in SL_2(\mathbb{F}_3)$, soit $\overline{P} \in \mathbb{P}SL_2(\mathbb{F}_3)$. Donc $\ker(\overline{\det}) \subset \mathbb{P}SL_2(\mathbb{F}_3)$.*
- ⋆ *Soit $\overline{P} \in \mathbb{P}SL_2(\mathbb{F}_3)$. On a $\overline{\det}(\overline{P}) = 1$ donc $\mathbb{P}SL_2(\mathbb{F}_3) \subset \ker(\overline{\det})$*

D'où $\ker(\overline{\det}) = \mathbb{P}SL_2(\mathbb{F}_3)$. De plus, on a bien $\mathbb{P}SL_2(\mathbb{F}_3) \lhd \mathbb{P}GL_2(\mathbb{F}_3)$.

Ainsi, la propriété universelle du quotient assure que:

$$\frac{\mathbb{P}GL_2(\mathbb{F}_3)}{\mathbb{P}SL_2(\mathbb{F}_3)} \simeq \mathbb{F}_3^\times \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$$

(on fait commuter le diagramme suivant)

$$\begin{tikzcd} \mathbb{P}GL_2(\mathbb{F}_3) \arrow[r, "\overline{\det}"] \arrow[d, "\pi"'] & \frac{\mathbb{Z}}{2\mathbb{Z}} \\ \frac{\mathbb{P}GL_2(\mathbb{F}_3)}{\mathbb{P}SL_2(\mathbb{F}_3)} \arrow[ur] & \end{tikzcd}$$

De plus, on a $\frac{S_4}{\mathcal{A}_4} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$*, donc* $\frac{\mathbb{P}GL_2(\mathbb{F}_3)}{\mathbb{P}SL_2(\mathbb{F}_3)} \simeq \frac{S_4}{\mathcal{A}_4}$*, et puisque* $\mathbb{P}GL_2(\mathbb{F}_3) \simeq S_4$ *et que* $\mathcal{A}_4$ *est le seul sous-groupe d'indice* 2 *dans* S_4*, on a donc* $\mathbb{P}SL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$.

■

Remarque. *On a, pour* $k \in \mathbb{N}^*$: $|GL_k(\mathbb{F}_q)| = (q^k - 1)(q^k - q)\dots(q^k - q^{k-1})$*. En effet, il suffit pour cela de compter le nombre de bases du* $\mathbb{F}_q$*-espace vectoriel* $\mathbb{F}_q^k$*:*

- *Pour choisir le premier vecteur, il suffit qu'il soit non nul, ce qui donne* $q^k - 1$ *solutions.*
- *Pour choisir le second vecteur, il suffit qu'il ne soit pas dans la droite vectorielle engendrée par le premier vecteur, donnant ainsi* $q^k - q^2$ *solutions.*
- ...
- *Pour choisir le* j*-ième vecteur, il suffit qu'il ne soit pas dans le sous-espace vectoriel engendré par les* $j-1$ *premiers vecteurs, donnant ainsi* $q^k - q^{j-1}$ *solutions.*

Finalement, on multiplie le nombre de solutions pour les k vecteurs, donnant $|GL_k(\mathbb{F}_q)| = (q^k - 1)(q^k - q)\dots(q^k - q^{k-1})$

Reférence. *D.Perrin, Cours d'algèbre*