Isomorphisme entre $\mathrm{PSL}_2(\mathbb{F}_7)$ et $\mathrm{GL}_3(\mathbb{F}_2)$

Bruno Winckler

L'objet de ce papier est de montrer l'isomorphisme entre $\mathrm{PSL}_2(\mathbb{F}_7)$ et $\mathrm{GL}_3(\mathbb{F}_2)$. Généralement, il est prouvé qu'il existe un unique groupe simple d'ordre 168, isomorphe au groupe des automorphismes du plan de Fano. Comme ils conviennent tous les deux, ils sont isomorphes. Il existe beaucoup d'autres preuves, mais aucune ne construit explicitement l'isomorphisme, peu évident *a priori* : qu'est-ce que des matrices carrées de taille 4 sur un corps à sept éléments ont à voir avec des matrices carrées de taille 9 sur un corps à deux éléments ? En gros, voici les étapes :

- le groupe $\mathrm{GL}_3(\mathbb{F}_2)$ peut être vu comme l'ensemble des endomorphismes $\mathbb{F}_2$-linéaires sur $\mathbb{F}_8$ et inversibles ;
- le cardinal de $\mathbb{F}_8^*$ est $8-1=7$;
- les carrés non nuls de $\mathbb{F}_7$ sont précisément les puissances de 2 modulo 7 ;
- mettre au carré modulo 2 est additif (grâce à Frobenius !).

1 Prérequis

Allez, on y va ! Soit $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$. Le groupe $\mathbb{F}_8^*$ est de cardinal un nombre premier, donc est cyclique et engendré par n'importe quel élément non trivial, par exemple par $x = X \bmod (X^3+X+1)$. Le corps $\mathbb{F}_8$ est un $\mathbb{F}_2$-espace vectoriel de dimension 3 sur $\mathbb{F}_2$, avec pour base $(1, x, x^2)$. L'application $\mathrm{GL}(\mathbb{F}_8) \to \mathrm{GL}_3(\mathbb{F}_2)$ qui, à une application linéaire inversible de $\mathbb{F}_8$ dans $\mathbb{F}_8$, associe sa matrice dans la base citée, est un isomorphisme de groupes. On peut donc identifier ces deux groupes, et je le ferai.

Le groupe $\mathrm{GL}_3(\mathbb{F}_2)$ est de cardinal 168. De plus, ce groupe est engendré par les transvections. Mais, en conjuguant les transvections par des matrices de permutation, on peut toutes les avoir à partir d'une seule, comme je vous laisse le vérifier. En fait, un système minimal de générateurs est donné par $\{E, S_{(23)}, S_{(12)}\}$, où S_τ est la matrice de permutation associée à τ, qui envoie la base canonique (e_1, e_2, e_3) sur $(e_{\tau^{-1}(1)}, e_{\tau^{-1}(2)}, e_{\tau^{-1}(3)})$, et

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

On peut en effet vérifier que les matrices de permutation restantes s'obtiennent à partir de $S_{(12)}$ et $S_{(23)}$ (elles se multiplient « comme on pense » : on a $S_\tau S_{\tau'} = S_{\tau\tau'}$). À présent, considérons les matrices suivantes :

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

On a $E = A_1A_3$, $S_{(12)} = A_2^2A_1A_2^3A_3$ et $S_{(23)} = A_1$, donc $\mathrm{GL}_3(\mathbb{F}_2)$ est engendré par $\{A_1, A_2, A_3\}$.

Passons à $\mathrm{PSL}_2(\mathbb{F}_7)$, en calculant d'abord son cardinal. Le même argument que précédemment montre que $\mathrm{GL}_2(\mathbb{F}_7)$ a $49 \cdot 42 = 2016$ éléments. L'isomorphisme $\mathrm{GL}_2(\mathbb{F}_7)/\ker(\det) \simeq \det(\mathbb{F}_7) = \mathbb{F}_7^*$ montre que le cardinal de $\ker(\det) = \mathrm{SL}_2(\mathbb{F}_7)$ est $\frac{2016}{6} = 336$. Enfin, l'égalité $\mathrm{PSL}_2(\mathbb{F}_7) = \mathrm{SL}_2(\mathbb{F}_7)/Z(\mathrm{SL}_2(\mathbb{F}_7)) = \mathrm{SL}_2(\mathbb{F}_7)/\pm 1$ donne $\mathrm{card}(\mathrm{PSL}_2(\mathbb{F}_7)) = 168$.

Soit $\mathbb{P}^1$ la droite projective sur $\mathbb{F}_7$, c'est-à-dire $\mathbb{F}_7 \cup \{\infty\}$. Le groupe $\mathrm{PSL}_2(\mathbb{F}_7)$ agit sur $\mathbb{P}^1$ librement et transitivement par homographies (*i.e.* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x = \frac{ax+b}{cx+d}$), donc induit un isomorphisme entre $\mathrm{PSL}_2(\mathbb{F}_7)$ et l'ensemble des homographies de $\mathbb{P}^1$. Dorénavant, j'identifie ces deux groupes. Il

est clair que l'ensemble des homographies est engendré par $r : k \mapsto \frac{-1}{k}$, $t : k \mapsto k+1$, $\delta : k \mapsto 2k$. Pour le démontrer sans méthodes calculatoires, on remarque que si f est une homographie, alors on peut supposer que $f(\infty) = \infty$: si $f(\infty) = m \in \mathbb{F}_7$, alors composer par $k \mapsto \frac{1}{k-m} = r \circ t^{-m}(k)$ permet de supposer $f(\infty) = \infty$. Or, une transformation qui fixe l'infini est de la forme $k \mapsto \frac{ak+b}{d}$ avec $ad = 1$, donc de la forme $k \mapsto a^2k + ab$. Les carrés de $\mathbb{F}_7$ sont les puissances de 2, donc $f = t^{ab} \circ \delta^j$ pour un certain j.

2 Preuve de l'isomorphisme

Posons, pour x le générateur de $\mathbb{F}_8^*$ choisi précédemment, $x^\infty = 0$. Alors, le corps $\mathbb{F}_8$ égale $\{x^k, k \in \mathbb{P}^1\}$. Définissons alors une application $T : \begin{cases} \mathrm{PSL}_2(\mathbb{F}_7) & \to & \mathrm{GL}_2(\mathbb{F}_8) \\ f & \mapsto & T_f \end{cases}$, en posant

$$T_f(x^k) = x^{f(k)} + x^{f(\infty)},$$

qui est bien linéaire ; l'apport de $x^{f(\infty)}$ est pour permettre d'avoir effectivement $T_f(0) = 0$ en toute circonstance. Il faut vérifier que $T_f \in \mathrm{GL}(\mathbb{F}_8)$. Pour cela, il suffit de vérifier que T_r, T_t et T_δ sont inversibles, et que $T_{f \circ g} = T_f T_g$. Comme r, t et δ engendrent $\mathrm{PSL}_2(\mathbb{F}_7)$, ceci prouvera que toutes les applications T_f sont inversibles.

On commence par les deux cas les plus aisés, qui sont T_t et T_δ : on a $T_t(0) = 0$ et pour $k \neq \infty$, on a $T_t(x^k) = x^{k+1} + x^\infty = x \cdot x^k$, donc T_t est juste la multiplication par x sur $\mathbb{F}_8$. En se rappelant que $x^3 = x + 1$, la matrice de T_t dans la base $(1, x, x^2)$ est

$$T_t = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = A_2.$$

Donc T_t est bien inversible. Le cas de T_δ est à peine plus compliqué : on a encore $T_\delta(0) = 0$, et pour $k \neq \infty$, on a $T_\delta(x^k) = x^{2k} = (x^k)^2$, donc T_δ n'est rien d'autre que le morphisme de Frobenius sur F_8, qui est bijectif, donc T_δ est inversible. En outre, T_δ a pour matrice A_3 dans la base canonique, en utilisant le fait que $x^4 = x^2 + x$.

Le cas de T_r est légèrement plus pénible. Commençons par calculer les différentes images des éléments de $\mathbb{P}^1$ par r : on a le tableau suivant :

k	0	1	2	3	4	5	6	∞
$r(k)$	∞	6	3	2	5	4	1	0

Sachant cela, on obtient le tableau de valeurs suivant pour T_r :

x^k	1	x	x^2	x^3	x^4	x^5	x^6	0
$T_r(x^k)$	1	x^2	x	x^2+1	x^2+x	x^2+x+1	$x+1$	0

On voit alors, en vérifiant les égalités $x^5 = x^2 + x + 1$ et $x^6 = x^2 + 1$, que T_r échange les coordonnées devant x et x^2, donc la matrice de T_r est la matrice de permutation $S_{(23)} = A_1$. Bref, T_r, T_t et T_δ sont toutes les trois inversibles. Il n'y a plus qu'à vérifier que $T_{f \circ g} = T_f T_g$, mais un calcul facile le montre. Bref, $T_f \in \mathrm{GL}(\mathbb{F}_8)$ pour tout $f \in \mathrm{PSL}_2(\mathbb{F}_7)$, donc l'application T est bien définie, et l'identité précédente assure que c'est un morphisme de groupes. Nos calculs de T_r, T_t et T_δ montrent qu'en fait, T est surjective, puisque son image atteint A_1, A_2 et A_3 qui engendrent $\mathrm{GL}(\mathbb{F}_8)$. Par égalité des cardinaux, on conclut : T est bijective. $\square$