Sous-groupes finis de $\mathrm{PGL}_2(\mathbb{C})$

Dans cette note j'énonce (sans démonstration, mais avec une référence) le théorème de Dickson sur les sous-groupes finis de $\mathrm{PGL}_2(\mathbb{C})$, et j'explique (avec démonstration, mais sans référence) comment identifier précisément ces sous-groupes en donnant des générateurs sous forme d'homographies. Les leçons concernées sont :

Groupes finis. Exemples et applications.
Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.
Sous-groupes finis de $\mathrm{O}(2,\mathbb{R})$, de $\mathrm{O}(3,\mathbb{R})$. Applications.
Exemples de parties génératrices d'un groupe.
Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.
Homographies de la droite complexe. Applications.

Notations. Le groupe $\mathrm{PGL}_2(\mathbb{C})$ est le quotient de $\mathrm{GL}_2(\mathbb{C})$ par le sous-groupe des homothéties. On désignera par la même lettre une matrice inversible $(2,2)$ et son image dans $\mathrm{PGL}_2(\mathbb{C})$. Nous notons $\mathbb{D}_n$ le groupe diédral d'ordre $2n$.

1 Le théorème de Dickson

1.1 Énoncé

Rappelons que $\mathrm{PGL}_2(\mathbb{C})$ est un groupe d'une grande importance géométrique car il s'identifie au groupe des homographies de la droite projective $\mathbb{P}^1(\mathbb{C})$ via l'application

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(x \mapsto \frac{ax+b}{cx+d} \right)$$

Il se trouve qu'il a exactement les mêmes sous-groupes finis qu'un autre groupe important en géométrie, à savoir le groupe $\mathrm{SO}_3(\mathbb{R})$ des isométries positives de l'espace euclidien de dimension trois. Ce n'est pas un hasard, comme nous l'expliquerons ci-dessous. Le théorème de Dickson ([Suzuki], theorem 6.17 du chapter 3, § 2) est le suivant :

Théorème 1 *Les sous-groupes finis de* $\mathrm{PGL}_2(\mathbb{C})$ *sont isomorphes à l'un des 5 groupes suivants : un groupe cyclique, un groupe diédral, ou l'un des groupes* $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$.

Remarque 1 Voici comment lire cet énoncé dans le livre de Suzuki - mais lisez ensuite la remarque 2 ci-dessous. Le théorème 6.17 de [Suzuki] concerne les sous-groupes de $\mathrm{SL}_2(k)$ avec k algébriquement clos de caractéristique quelconque. La démonstration est longue et assez technique et je ne vous conseille pas de la lire. Pour retrouver l'énoncé ci-dessus, notez que si k est algébriquement clos on a $\mathrm{PSL}_2(k) \simeq \mathrm{PGL}_2(k)$ (exercice), donc il suffit de lire la partie I du théorème (caractéristique 0) et de quotienter par $\{\pm 1\}$ pour obtenir les sous-groupes de $\mathrm{PSL}_2(k)$. On trouve, dans l'ordre donné par Suzuki : les groupes cycliques, les groupes diédraux, puis $\mathfrak{A}_4$ (vu que $\mathrm{PSL}(2,\mathbb{F}_3) \simeq \mathfrak{A}_4$), $\mathfrak{S}_4$ (en effet le quotient du groupe $\widetilde{\Sigma}_4$ donné par Suzuki est $\mathfrak{S}_4$) et $\mathfrak{A}_5$ (vu que $\mathrm{PSL}(2,\mathbb{F}_5) \simeq \mathfrak{A}_5$).

Remarque 2 Vous n'avez pas besoin de la remarque 1, car il vous sera très facile de retenir le théorème puisque vous connaissez bien la liste des sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$. Si on vous demande une référence, vous n'aurez qu'à citer le livre de Suzuki... on ne vous en demandera pas plus.

1.2 Lien avec $\mathrm{SO}_3(\mathbb{R})$

Ce paragraphe est inclus pour assouvir votre curiosité, mais il n'est pas nécessaire pour lire la partie suivante.

Le lien entre sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$ et de $\mathrm{PGL}_2(\mathbb{C})$ a une explication simple :

Affirmation : *Il existe une injection* $\mathrm{SO}_3(\mathbb{R}) \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$.

Admettant cela, le théorème de Dickson nous redonne les seuls sous-groupes finis possibles de $\mathrm{SO}_3(\mathbb{R})$. En effet, si H est un sous-groupe fini de $\mathrm{SO}_3(\mathbb{R})$, c'est un sous-groupe de $\mathrm{PGL}_2(\mathbb{C})$ via notre injection, et d'après le théorème de Dickson il est isomorphe à l'un des 5 que l'on sait.

Nous allons maintenant construire cette injection à l'aide de l'algèbre des quaternions $\mathbb{H}$ (j'utilise [Perrin], chapitre VII comme référence sur $\mathbb{H}$). Rappelons que $\mathbb{H}$ est la $\mathbb{R}$-algèbre composée des éléments $a + bi + cj + dk$ où $a, b, c, d \in \mathbb{R}$, avec les règles de multiplication bien connues. Le groupe $G \subset \mathbb{H}$ des quaternions de norme 1 est homéomorphe à la sphère S^3.

Preuve : Il y a deux points importants :

(1) On a une injection $\mathbb{H} \hookrightarrow \mathrm{M}_2(\mathbb{C})$. En effet $\mathbb{H}$ a une structure de $\mathbb{C}$-ev de dimension 2 : on peut voir $\mathbb{C}$ comme sous-corps de $\mathbb{H}$ comme l'ensemble des $a+bi$, et puisque $k = ij$ dans $\mathbb{H}$, on peut écrire $a + bi + cj + dk = (a + bi) + (c + di)j$ de sorte que $\{1, j\}$ est une base de $\mathbb{H}$ comme $\mathbb{C}$-ev. (Attention : la loi extérieure est ici $(\lambda, q) = \lambda q$ alors que Perrin (chap. VII, § 4) utilise la loi extérieure $(\lambda, q) = q\lambda$.) Si on fixe un quaternion q, il est facile devoir que la multiplication à droite par q, $D_q(x) = xq$ est $\mathbb{C}$-linéaire. (Ici, Perrin considère la multiplication à gauche à la place.) On obtient donc un morphisme injectif $\mathbb{H} \to \mathrm{End}_{\mathbb{C}\text{-ev}}(\mathbb{H}) \simeq \mathrm{M}_2(\mathbb{C})$, qui à q associe D_q.

(2) On en déduit un morphisme $f : G \to \mathrm{PGL}_2(\mathbb{C})$. En effet on peut faire agir un élément $g \in G$ par la conjugaison par son image dans $\mathrm{M}_2(\mathbb{C})$. Il s'agit d'une action par automorphismes de $\mathbb{C}$-algèbre d'où un morphisme de groupes $G \to \mathrm{Aut}_{\mathbb{C}\text{-alg}}(\mathrm{M}_2(\mathbb{C}))$. Or on connaît ce groupe d'automorphismes : le morphisme $\mathrm{GL}_2(\mathbb{C}) \to \mathrm{Aut}_{\mathbb{C}\text{-alg}}(\mathrm{M}_2(\mathbb{C}))$ qui à P associe la conjugaison par P a pour noyau les homothéties, donc il se factorise en un morphisme injectif $\mathrm{PGL}_2(\mathbb{C}) \to \mathrm{Aut}_{\mathbb{C}\text{-alg}}(\mathrm{M}_2(\mathbb{C}))$. Ce morphisme est aussi surjectif (donc un isomorphisme) car on sait que les automorphismes de $\mathbb{C}$-algèbre de $\mathrm{M}_2(\mathbb{C})$ sont tous intérieurs (voir par exemple [FGN] p. 273).

On conclut en cherchant le noyau de f. Si $g \in \ker(f)$, il agit trivialement sur $\mathrm{M}_2(\mathbb{C})$ et en particulier sur la sous-algèbre $\mathbb{H}$. Or la conjugaison par g est triviale sur $\mathbb{H}$ ssi g est central, donc $g \in \mathbb{R}$, or $G \cap \mathbb{R} = \{\pm 1\}$. Donc $\ker(f) = \{\pm 1\}$, or on sait que $G/\{\pm 1\} \simeq \mathrm{SO}_3(\mathbb{R})$: cela s'obtient en disant que la restriction de la conjugaison par $g \in G$ à l'ensemble des quaternions purs se fait par isométries, voir Perrin chap. VII, § 2. Donc $f : G \to \mathrm{PGL}_2(\mathbb{C})$ se factorise en l'injection qu'on voulait $\mathrm{SO}_3(\mathbb{R}) \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$. $\square$

Remarque 3 Il y a une autre façon de voir cette injection. On peut identifier la sphère unité $S^2 \subset \mathbb{R}^3$ à la droite projective complexe (voir cours d'E. Halberstadt sur la droite projective). Les isométries de $\mathbb{R}^3$ agissent sur la sphère et donc sur $\mathbb{P}^1(\mathbb{C})$, et tout revient alors à vérifier que cette action se fait par homographies.

2 Expliciter les sous-groupes finis de $\mathrm{PGL}_2(\mathbb{C})$

On peut résumer les résultats qui vont suivre en un énoncé un peu imprécis :

Théorème 2 *Soit G l'un des 5 groupes $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{D}_n$, $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$. Alors les sous-groupes de $\mathrm{PGL}_2(\mathbb{C})$ qui sont isomorphes à G sont tous conjugués entre eux. En particulier ils sont tous conjugués à un sous-groupe de $\mathrm{SO}_3(\mathbb{R})$. De plus, on sait produire un sous-groupe explicite de chacun des 5 types.*

2.1 Un résultat clé

Notons $\mu_n^* \subset \mathbb{C}$ le groupe des racines primitives n-èmes de l'unité. On définit une relation d'équivalence dans μ_n^* par $\zeta \sim \zeta'$ ssi $\zeta' \in \{\zeta, \zeta^{-1}\}$. La classe de ζ est notée $[\zeta]$, et l'application $[\zeta] \mapsto \zeta + \zeta^{-1}$ définit une injection $\mu_n^*/\sim \hookrightarrow \mathbb{C}$.

La clé de la démonstration du théorème 2 est le résultat suivant.

Proposition 1 *Soit $A \in \mathrm{PGL}_2(\mathbb{C})$ et $n > 1$. Alors LCSSE* ([1]) *:*

(i) *A est d'ordre n.*

(ii) *Comme homographie de $\mathbb{P}^1(\mathbb{C})$, A est conjugué à $x \mapsto \zeta x$, pour un $[\zeta] \in \mu_n^*/\sim$.*

(iii) *Il existe $[\zeta] \in \mu_n^*/\sim$ tel que $(\zeta + \zeta^{-1} + 2)\det(A) - \mathrm{tr}(A)^2 = 0$.*

En particulier l'ensemble $\mu_n^*/\sim$ classifie les classes de conjugaison d'éléments d'ordre n.

Pour justifier (ii), observez que $x \mapsto \zeta x$ et $x \mapsto \zeta^{-1}x$ sont conjuguées (par l'homographie $x \mapsto 1/x$), de sorte que le fait d'être conjugué à $x \mapsto \zeta x$ ne dépend pas de la classe de ζ pour la relation $\sim$. Quant à (iii), notez que $\det(A)$ et $\mathrm{tr}(A)$ ne sont pas bien définies car A n'est que la classe d'une matrice modulo homothéties. Cependant, si on multiplie A par un scalaire $\lambda \neq 0$, alors $\det(A)$ et $\mathrm{tr}(A)^2$ sont tous deux mutlipliés par λ^2, donc la condition (iii) a un sens indépendant du représentant matriciel choisi pour A.

Preuve : On travaille avec un représentant de A dans $\mathrm{GL}_2(\mathbb{C})$. Le polynôme caractéristique est $\chi(X) = X^2 - \mathrm{tr}(A)X + \det(A)$ et les valeurs propres sont $\lambda^{\pm} = \frac{1}{2}(\mathrm{tr}(A) \pm \delta)$ où $\delta^2 = \mathrm{tr}(A)^2 - 4\det(A)$. Posons $\zeta_A := \lambda^+/\lambda^- \in \mathbb{C}$ de sorte que

$$\zeta_A + \zeta_A^{-1} = \frac{\mathrm{tr}(A) + \delta}{\mathrm{tr}(A) - \delta} + \frac{\mathrm{tr}(A) - \delta}{\mathrm{tr}(A) + \delta} = \frac{\mathrm{tr}(A)^2}{\det(A)} - 2$$

Il est clair que A est d'ordre n (dans $\mathrm{PGL}_2(\mathbb{C})$) ssi $\zeta_A = \zeta \in \mu_n^*$. Ceci équivaut à dire que A est semblable à la matrice diagonale $(\zeta, 1)$, donc (i) $\Leftrightarrow$ (ii). Par ailleurs on a vu que (i) $\Rightarrow$ (iii). Montrons la réciproque. Sous la condition (iii) on a

$$\zeta_A + \zeta_A^{-1} = \frac{\mathrm{tr}(A)^2}{\det(A)} - 2 = \zeta + \zeta^{-1}$$

Ceci entraîne que $\zeta_A = \zeta$ ou ζ^{-1}, d'où on déduit (i). $\square$

Les cas particuliers $n = 2, 3, 4, 6$ sont les seuls cas où $\mu_n^*/\sim$ est réduit à un point : pour $n = 2$ c'est clair, et les autres cas sont ceux pour lesquels $\varphi(n) = 2$, donc $\zeta + \zeta^{-1}$ prend alors une seule valeur. (Les cas $n = 2$ et $n = 3$ seront fondamentaux dans la suite.)

[1] Les conditions suivantes sont équivalentes

Corollaire 1 *A est d'ordre $n = 2, 3, 4, 6$ ssi* $\mathrm{tr}(A)^2 = i \det(A)$ *pour $i = 0, 1, 2, 3$ resp.* $\square$

Preuve : On utilise le (iii) de la proposition 1. Les racines primitives de l'unité correspondantes sont -1, $j = e^{2i\pi/3}$, i et $u = e^{i\pi/3}$. Les polynômes minimaux de j et u sur $\mathbb{Q}$ sont les polynômes cyclotomiques $\Phi_3 = (X - j)(X - \overline{j}) = X^2 + X + 1$ et $\Phi_6 = (X - u)(X - \overline{u}) = X^2 - X + 1$. On en déduit les valeurs correspondantes pour $\zeta + \zeta^{-1} + 2$. $\square$

Corollaire 2 *Soit $A \in \mathrm{PGL}_2(\mathbb{C})$ distinct de l'identité et d'ordre fini. Notons A comme une homographie $A(x) = \frac{ax+b}{cx+d}$. Alors A a deux points fixes sur $\mathbb{P}^1(\mathbb{C})$.*

Preuve : D'après le (iii) de la proposition 1, il existe une racine de l'unité ζ telle que $(\zeta + \zeta^{-1} + 2)\det(A) - \mathrm{tr}(A)^2 = 0$. Si $c = 0$ alors $a \neq d$ car A est d'ordre fini, et alors A a pour points fixes le point ∞ et le point $b/(d - a)$. Si $c \neq 0$, il n'y a pas de point fixe à l'infini, et l'équation donnant les points fixes est $cx^2 + (d - a)x - b = 0$. Le discriminant est $\Delta = \mathrm{tr}(A)^2 - 4\det(A) = (\zeta + \zeta^{-1} - 2)\det(A)$. Or $\zeta + \zeta^{-1} - 2 \neq 0$ pour toute racine n-ième de l'unité, donc il y a deux solutions distinctes. $\square$

2.2 Démonstration du théorème de Dickson

Dans ce paragraphe *qui n'est pas terminé*, je voudrais démontrer le théorème de Dickson en suivant la stratégie de la preuve du théorème de classification des sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$.

Soit maintenant G un sous-groupe de $\mathrm{PGL}_2(\mathbb{C})$, fini de cardinal n. Notons $\mathcal{F}$ l'ensemble des points fixes des éléments de G distincts de l'identité : d'après le corollaire ci-dessus c'est un ensemble fini de cardinal compris entre 2 et $2(n - 1)$. Le groupe G agit sur $\mathcal{F}$ car si x est un point fixe de $g \in G$, et $h \in G$, alors $h(x)$ est un point fixe de hgh^{-1}. D'après la formule de Burnside, le nombre d'orbites pour cette action est

$$k = \frac{1}{n} \sum_{g \in G} |\,\mathrm{Fix}(g)| = \frac{1}{n}(|\mathcal{F}| + 2(n-1))$$

Rappelons ensuite que $\mathrm{PGL}_2(\mathbb{C})$ est simplement 3-transitif sur $\mathbb{P}^1(\mathbb{C})$, ce qui veut dire qu'étant donnés deux triplets (r, s, t) et (r', s', t') d'éléments de $\mathbb{P}^1(\mathbb{C})$ avec r, s, t tous distincts et r', s', t' tous distincts, il existe un unique $F \in \mathrm{PGL}_2(\mathbb{C})$ tel que $F(r) = r'$, $F(s) = s'$, $F(t) = t'$. Maintenant soit... *(à suivre)*

2.3 Démonstration du théorème 2

On prouve le théorème 2 en cherchant un représentant explicite de chaque classe de conjugaison de sous-groupe fini dans $\mathrm{PGL}_2(\mathbb{C})$. Pour cela, on choisit des présentations des groupes finis en question par générateurs et relations, et on exprime ces relations dans $\mathrm{PGL}_2(\mathbb{C})$ à l'aide de la proposition 1 et du corollaire. Pour simplifier les écritures, nous noterons parfois les homographies sous la forme $\frac{ax+b}{cx+d}$.

Proposition 2 *Les sous-groupes cycliques de $\mathrm{PGL}_2(\mathbb{C})$ sont tous conjugués à*

$$C_n := \langle\, \zeta x \,\rangle$$

Notez que ce sous-groupe ne dépend pas du choix de ζ qui apparaît. La preuve de cette proposition est simplement le (ii) de la proposition 1.

Proposition 3 *Les sous-groupes diédraux de* $\mathrm{PGL}_2(\mathbb{C})$ *sont tous conjugués à*

$$D_n := \langle\, \zeta x, \frac{1}{x} \,\rangle$$

Preuve : Soit $\mathbb{D}_n = \langle r, s \,|\, r^n = s^2 = (rs)^2 = 1 \rangle$. Soit $\nu\colon \mathbb{D}_n \to \mathrm{PGL}_2(\mathbb{C})$ un morphisme injectif, $a = \nu(r)$ et $b = \nu(s)$. D'après la proposition 1(ii), quitte à appliquer une première conjugaison dans $\mathrm{PGL}_2(\mathbb{C})$, on peut supposer que $a(x) = \zeta^{-1}x$ pour un $\zeta \in \mu_n^*$. D'après le corollaire, comme b est d'ordre 2 on peut écrire $b(x) = \frac{rx+s}{tx-r}$. En écrivant le fait que $ab = \nu(rs)$ est aussi d'ordre 2 on trouve que $r = 0$, donc $b(x) = \frac{s}{tx}$. Alors, la conjugaison par λ/x (où $\lambda := \sqrt{s/t}$) envoie a sur $x \mapsto \zeta x$ et b sur $x \mapsto 1/x$. On a ainsi montré que l'image de ν est conjuguée au groupe $D_n = \langle\, \zeta x, 1/x \,\rangle$. $\square$

Proposition 4 *Les sous-groupes de* $\mathrm{PGL}_2(\mathbb{C})$ *isomorphes à* $\mathfrak{A}_4$ *sont tous conjugués à*

$$A_4 := \langle\, jx, \frac{x+2}{x-1} \,\rangle \simeq \langle\, (123), (12)(34) \,\rangle$$

avec j *racine primitive troisième de l'unité.*

L'écriture ci-dessus signifie qu'on a choisi pour $\mathfrak{A}_4$ les générateurs (123) et $(12)(34)$, et que l'homographie $x \mapsto jx$ correspond à (123), et $x \mapsto \frac{x+2}{x-1}$ correspond à $(12)(34)$.

Preuve : Soit $\nu\colon \mathfrak{A}_4 \to \mathrm{PGL}_2(\mathbb{C})$ un morphisme injectif. Soit $a = \nu(123)$ et $b = \nu((12)(34))$. Écrivons $b(x) = \frac{rx+s}{tx-r}$. Quitte à appliquer une première conjugaison dans $\mathrm{PGL}_2(\mathbb{C})$, on peut supposer que $a(x) = jx$. En écrivant le fait que $ab = \nu(134)$ est d'ordre 3 on trouve $2r^2 = st$. Donc $t \neq 0$, car sinon on aurait $r = 0$ ce qui est impossible. Alors la conjugation par $\phi(x) = rx/t$ laisse a inchangé et envoie b sur $x \mapsto \frac{x+2}{x-1}$. Donc l'image de ν est conjuguée au groupe annoncé. On n'a utilisé que certaines relations, et on pourrait les utiliser toutes pour montrer que le groupe obtenu est en effet isomorphe à $\mathfrak{A}_4$. Cependant le fait d'admettre le théorème de Dickson nous assure qu'il existe des sous-groupes isomorphes à $\mathfrak{A}_4$, de sorte que le sous-groupe produit ci-dessus *doit* être isomorphe à $\mathfrak{A}_4$. Nous ferons de même ci-dessous. $\square$

Proposition 5 *Les sous-groupes de* $\mathrm{PGL}_2(\mathbb{C})$ *isomorphes à* $\mathfrak{S}_4$ *sont tous conjugués à*

$$S_4 := \langle\, ix, \frac{x+1}{x-1} \,\rangle \simeq \langle\, (1234), (12) \,\rangle$$

Preuve : Soit $\nu\colon \mathfrak{S}_4 \to \mathrm{PGL}_2(\mathbb{C})$ un morphisme injectif. Soit $a = \nu(1234)$ et $b = \nu(12)$, on a $ab = \nu(134)$. Écrivons $b(x) = \frac{rx+s}{tx-r}$. Quitte à appliquer une première conjugaison on peut supposer que $a(x) = ix$. En écrivant le fait que ab est d'ordre 3 on trouve $r^2 = st$. La conjugation par $\phi(x) = rx/t$ laisse a inchangé et envoie b sur $x \mapsto \frac{x+1}{x-1}$. $\square$

Proposition 6 *Les sous-groupes de* $\mathrm{PGL}_2(\mathbb{C})$ *isomorphes à* $\mathfrak{A}_5$ *sont tous conjugués à*

$$A_5 := \langle\, \delta x, \frac{x+1}{\Delta x - 1} \,\rangle \simeq \langle\, (12345), (12)(34) \,\rangle$$

où δ *est une quelconque racine primitive cinquième de l'unité et* $\Delta := 1 - \delta - \delta^{-1}$.

Preuve : Soit $\nu\colon \mathfrak{A}_5 \to \mathrm{PGL}_2(\mathbb{C})$ un morphisme injectif. Soit $a = \nu(12345)$, $b = \nu((12)(34))$, on a $ab = \nu((12345)(12)(34)) = \nu(135)$. Écrivons $b(x) = \frac{rx+s}{tx-r}$. Il existe une racine primitive cinquième de l'unité δ telle qu'après une première conjugaison on ait $a(x) = \delta x$. On écrit que ab est d'ordre 3, ce qui donne $\Delta r^2 = st$. Alors, la conjugaison par $x \mapsto \frac{r\Delta}{t}x$ laisse a inchangé et transforme b en $\frac{x+1}{\Delta x-1}$. $\square$

Bibliographie

[FGN] Francinou, Gianella, Nicolas, Exercices de mathématiques des oraux de l'Ecole polytechnique et des Ecoles normales supérieures : Algèbre, Tome I, *Cassini*.
[Perrin] Perrin, Cours d'Algèbre, *Ellipses*.
[Suzuki] Suzuki, Group Theory I, *Springer*. Le livre n'est pas à la BU, mais il est à la bibliothèque de Chevaleret à la cote 20 SUZ 82.