MATHÉMATIQUES

De combien de paramètres dépend l'équation générale de degré n ?

Arnaud Beauville[1]

Une équation du quarantième degré !
Elle appartient à ce que les mathématiciens
qui osèrent affronter les ténèbres de l'hypergéométrie
appellent la quatrième dimension. [Ra]

L'équation générale de degré n s'écrit

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \qquad (E_n)$$

où $a_1, \ldots, a_n$ sont des paramètres indépendants ; la réponse à la question posée dans le titre semble donc évidemment n. Cependant nous savons tous que le changement de variable $y = x + \frac{a_1}{n}$ conduit à une équation

$$y^n + b_2 y^{n-2} + \ldots + b_n = 0 \ ,$$

où $b_2, \ldots, b_n$ sont des polynômes en les a_i ; et la résolution de l'une ou l'autre de ces équations est complètement équivalente. De même, remplacer y par $(b_{n-1}/b_n)y$ permet de supposer $b_{n-1} = b_n$, de sorte que notre nouvelle équation, toujours équivalente à (E_n), ne fait plus intervenir que $n-2$ paramètres indépendants. Peut-on aller plus loin ? Après avoir été beaucoup étudiée aux 18e et 19e siècles, cette question est un peu tombée dans l'oubli. Elle en est sortie il y a 15 ans avec l'article de Buhler et Reichstein [BR], qui replacent le problème dans le cadre général de la *dimension essentielle* d'un groupe fini. Je vais essayer de décrire cette formulation, montrer sa relation avec la géométrie algébrique, et expliquer en particulier comment des résultats récents (et difficiles) sur les variétés de dimension 3 permettent de résoudre le cas de l'équation du septième degré.

[1] Laboratoire J.-A. Dieudonné, UMR 7351 du CNRS, université de Nice.

1. Un peu d'histoire

Dans le cas de l'équation $x^2+a_1x+a_2=0$, le changement de variable $y=x+\frac{a_1}{2}$ (qui suffit bien sûr à la résoudre) était connu des babyloniens il y a quelques 4000 ans. Plus près de nous, Cardan consacre une bonne partie de l'*Ars Magna* ([C], chap. 14 à 23) à expliquer son utilisation pour les équations de degré 3. Descartes le décrit en toute généralité, et de façon détaillée, dans le livre III de sa Géométrie [De].

Quarante ans plus tard le mathématicien allemand Ehrenfried von Tschirnhaus a l'idée d'utiliser une transformation plus générale : $y=u_0+u_1x+\ldots+u_{n-1}x^{n-1}$. Il montre que y vérifie une équation

$$y^n+b_1y^{n-1}+\ldots+b_n=0\ ,$$

où b_p est un polynôme homogène de degré p en les u_i. Ainsi, en résolvant une équation quadratique, on peut choisir les u_i de façon que $b_1=b_2=0$; en degré 3, cela suffit à résoudre (E_3). Tschirnhaus fait les calculs complètement et retrouve la formule de Cardan-Tartaglia. À ce point Tschirnhaus, dont la rigueur mathématique n'est pas la qualité dominante, pense avoir obtenu une méthode générale de résolution des équations algébriques ; il l'écrit à Leibniz, qui lui répond assez sèchement qu'en degré supérieur ou égal à 5 sa méthode ne pourra résoudre que des cas particuliers ([L], lettre VIII de Leibniz à Tschirnhaus). Tschirnhaus n'est probablement pas convaincu : dans l'article [T], écrit quelques années plus tard, il semble encore affirmer que sa méthode permet d'éliminer tous les coefficients intermédiaires $b_1,\ldots,b_{n-1}$.

Ehrenfried Walter von Tschirnhaus (1651-1708)

La méthode est reprise un siècle plus tard par le mathématicien suédois Erland Bring, qui réduit ainsi l'équation du cinquième degré à la forme $x^5+px+q=0$ [Br] ; ce résultat est retrouvé et généralisé par un mathématicien anglais, George Jerrard (qui ignorait probablement le travail de Bring) – d'où le nom de Bring-Jerrard associé à cette réduction. Jerrard pense lui aussi pouvoir résoudre ainsi par radicaux l'équation de degré 5 (quelques années après la preuve par Abel de l'impossibilité d'une telle résolution...), et c'est Hamilton qui indique son erreur [H]. La forme de Bring-Jerrard est utilisée de façon essentielle par Hermite lorsqu'il prouve que

l'équation du cinquième degré peut être résolue à l'aide de fonctions elliptiques ([He], voir aussi [K]).

Il faut noter que cette réduction s'éloigne légèrement de la question initiale, dans la mesure où les nouveaux coefficients b_i sont des fonctions *algébriques* (i.e. solutions d'équations algébriques) et non plus polynomiales des a_i ; dans le langage de l'époque, on introduit des « irrationalités accessoires », qui sont considérées comme inessentielles puisqu'elles sont racines d'équations de degré plus petit que celle qu'on cherche à résoudre. Klein semble être le premier à s'en préoccuper : dans [K] il analyse soigneusement ces irrationalités accessoires pour l'équation du cinquième degré, et montre notamment qu'on ne peut réduire le nombre de paramètres à 1 sans les introduire (*théorème de Kronecker*, dernier paragraphe de [K]).

La théorie des équations, devenue théorie de Galois, se déplace ensuite vers des questions plus générales, telles que la théorie du corps de classes, et le problème du nombre de paramètres semble oublié – jusqu'à l'article [BR] dont nous allons essayer d'expliquer les idées essentielles.

2. De la méthode de Tschirnhaus à la dimension essentielle de $\mathfrak{S}_n$

2.1. La transformation de Tschirnhaus en termes modernes

Essayons maintenant de formuler rigoureusement la définition du « nombre minimum de paramètres » de l'équation (E_n), nombre que nous noterons $d(n)$. Il nous faut d'abord un corps de base : pour simplifier je prendrai le corps $\mathbb{C}$ – voir §5 pour quelques remarques sur le cas général. Il nous faut ensuite des indéterminées $a_1, \ldots, a_n$; on va donc considérer le corps $K = \mathbb{C}(a_1, \ldots, a_n)$ des fractions rationnelles en ces n variables. L'étude de l'équation (E_n) revient à celle de l'extension $K \subset L := K[x]/(x^n + a_1 x^{n-1} + \ldots + a_n)$.

Que fait Tschirnhaus ? Il prend un élément quelconque y de L et observe que L peut aussi s'écrire $K[y]/(y^n + b_1 y^{n-1} + \ldots + b_n)$. Notons K_0 le sous-corps de K engendré par $(b_1, \ldots, b_n)$, et posons $L_0 := K_0[y]/(y^n + b_1 y^{n-1} + \ldots + b_n)$; on a un diagramme[2]

$$\begin{array}{ccc} L_0 & \longrightarrow & L \\ \uparrow & & \uparrow \\ K_0 & \longrightarrow & K \end{array}$$

qui est commutatif et même *cartésien* : techniquement, cela veut dire que L est le produit tensoriel $K \otimes_{K_0} L_0$, mais concrètement cela signifie précisément que L peut être défini par une équation à coefficients dans le corps plus petit K_0 (on dit que l'extension L/K est *définie sur* K_0). C'est donc exactement ce que nous cherchons à faire, avec un corps K_0 le plus petit possible. Comment mesurer cette petitesse ? Il n'y a pas de raison de se borner au cas où K_0 est isomorphe à un corps de fractions rationnelles $\mathbb{C}(b_1, \ldots, b_p)$. Mais il est toujours vrai (et pas difficile) que K_0 contient un tel sous-corps de façon que K_0 soit une extension *finie* de $\mathbb{C}(b_1, \ldots, b_p)$ (en particulier, tout élément de K_0 vérifie une équation algébrique à coefficients dans ce sous-corps). Le nombre p est un invariant de K_0 qu'on appelle

[2] Ne pas oublier que tout homomorphisme de corps est injectif, donc peut être vu comme une inclusion.

le *degré de transcendance* de K_0 (sur $\mathbb{C}$) et qu'on note $\deg.\mathrm{tr}(K_0)$. Il est donc raisonnable de le considérer comme le « nombre de paramètres » dont dépendent K_0 et L_0, et de poser

$$d(n) := \min\{\deg.\mathrm{tr}(K_0) \mid K_0 \subset K \text{ et } L/K \text{ est définie sur } K_0\}\,.$$

2.2. Passage à l'extension galoisienne

Les algébristes préfèrent regarder l'*extension galoisienne* associée : au lieu d'adjoindre à K une racine x de l'équation (E_n), on prend toutes ses racines $x_1, \dots, x_n$. Le résultat est le corps des fractions rationnelles en n variables $M = \mathbb{C}(x_1, \dots, x_n)$, le sous-corps $K = \mathbb{C}(a_1, \dots, a_n)$ étant formé des fractions rationnelles symétriques (a_i étant, au signe près, le i-ième polynôme symétrique élémentaire). Ce qu'on gagne dans cette situation c'est que le groupe symétrique $\mathfrak{S}_n$ agit sur M (par permutation de $x_1, \dots, x_n$), et que K est précisément le sous-corps des éléments de M invariants pour cette action. Si L/K est définie sur K_0, il en est de même de M/K, d'où un diagramme

$$\begin{array}{ccc} M_0 & \longrightarrow & M \\ \uparrow & & \uparrow \\ K_0 & \longrightarrow & K\,. \end{array}$$

Le corps $M_0 \subset M$ est stable par l'action de $\mathfrak{S}_n$, et son sous-corps des invariants pour cette action est K_0. Par conséquent *la deuxième ligne est déterminée par la première*, à savoir par le sous-corps M_0 de M stable par $\mathfrak{S}_n$. Le fait que l'extension M/K « provient » de M_0/K_0 se traduit par le fait que leurs degrés sont les mêmes (à savoir $n!$, l'ordre de $\mathfrak{S}_n$), et ceci est équivalent au fait que l'action de $\mathfrak{S}_n$ sur M est *fidèle*. Comme le degré de transcendance ne change pas par extension finie, on peut réécrire notre définition de $d(n)$:

$$d(n) := \min\{\deg.\mathrm{tr}(M_0) \mid M_0 \subset M \text{ stable par } \mathfrak{S}_n\ ,\ \mathfrak{S}_n \subset \mathrm{Aut}(M_0)\}\,.$$

Nous allons maintenant reformuler cette définition en termes de géométrie algébrique. Pour cela nous devons d'abord rappeler la correspondance entre corps et variétés algébriques.

2.3. Des corps aux variétés algébriques

Dans ce qui suit les variétés algébriques sont supposées *irréductibles*, c'est-à-dire qu'elles ne sont pas réunion de deux sous-variétés strictes, comme la courbe $xy = 0$ dans $\mathbb{C}^2$. Une *application rationnelle* $f : X \dashrightarrow Y$ entre deux variétés algébriques est une application algébrique de $X \smallsetminus Z$ dans Y, où Z est une sous-variété stricte de X. Si $Y = \mathbb{C}$, on parle de *fonction rationnelle* ; les fonctions rationnelles sur X forment un corps K_X, extension de type fini de $\mathbb{C}$ (c'est-à-dire engendrée, en tant que corps, par un nombre fini d'éléments). Par exemple $K_{\mathbb{C}^n}$ est le corps des fractions rationnelles $\mathbb{C}(x_1, \dots, x_n)$.

On dit qu'une application rationnelle $f : X \dashrightarrow Y$ est *dominante* si elle est « presque surjective », c'est-à-dire que le complémentaire de son image est contenu dans une sous-variété stricte de Y. Si c'est le cas, pour toute fonction rationnelle $\varphi \in K_Y$ la composée $\varphi \circ f$ est une fonction rationnelle $f^*\varphi$ sur X ; l'application

$f^* : K_Y \to K_X$ est un homomorphisme de corps. En termes savants, on a défini un *foncteur*

$$\{\text{variétés algébriques} + \text{appl. rat. dominantes}\} \longrightarrow \{\text{corps de type fini sur } \mathbb{C}\}\ .$$

Il n'est pas difficile de voir que ce foncteur est une *équivalence de catégories* : toute extension de type fini est isomorphe au corps des fonctions rationnelles sur une variété, et tout homomorphisme $K_Y \to K_X$ provient d'une unique application rationnelle dominante $X \dashrightarrow Y$.

Par exemple, la définition du degré de transcendance du corps K_X se traduit par l'existence d'une application rationnelle dominante $f : X \dashrightarrow \mathbb{C}^p$ qui est génériquement finie, c'est-à-dire que $f^{-1}(v)$ est fini pour v assez général dans $\mathbb{C}^p$. Cela entraîne $\dim(X) = p = \deg.\,\mathrm{tr}(K_X)$.

Dans ce qui suit, nous travaillerons toujours dans la catégorie des variétés algébriques et applications rationnelles dominantes. Il faut prendre garde que des variétés différentes deviennent isomorphes dans cette catégorie (on dit qu'elles sont *birationnelles*) ; ainsi on peut toujours enlever une sous-variété d'une variété donnée sans changer son type birationnel. Plus subtilement, on peut toujours choisir un modèle *lisse* (= sans singularités) et *projectif* dans un type birationnel donné.

2.4. Passage aux variétés algébriques

Appliquons ce dictionnaire à la dernière définition de $d(n)$. Le corps M est le corps des fonctions rationnelles de $\mathbb{C}^n$, le sous-corps M_0 celui d'une variété X, munie d'une action fidèle de $\mathfrak{S}_n$; de plus on a une application rationnelle dominante $\mathbb{C}^n \dashrightarrow X$ compatible avec l'action de $\mathfrak{S}_n$. Nous avons vu ci-dessus que $\deg.\,\mathrm{tr}(M_0) = \dim(X)$. Donc

$$d(n) := \min\{\dim(X) \mid \mathfrak{S}_n \subset \mathrm{Aut}(X)\ ,\ \exists\ \mathbb{C}^n \dashrightarrow X \text{ dominante } \mathfrak{S}_n\text{-équivariante}\}.$$

À ce point, pourquoi se borner au groupe symétrique ? Étant donnés un groupe fini G et une représentation linéaire V de G, posons (provisoirement)

$$\mathrm{ed}(G, V) := \min\{\dim(X) \mid G \subset \mathrm{Aut}(X)\ ,\ \exists\ V \dashrightarrow X \text{ dominante } G\text{-équivariante}\}.$$

En fait, en comparant V à la représentation régulière, Buhler et Reichstein montrent que ce nombre est indépendant du choix de V : ils l'appellent dimension essentielle de G. Donnons une définition précise :

Définition. *Soit G un groupe fini.*

1) *Une G-variété est une variété algébrique irréductible, munie d'une action* fidèle *de G.*

2) *Une G-variété X est* linéarisable *s'il existe une représentation linéaire V de G et une application rationnelle dominante G-équivariante $V \dashrightarrow X$.*

3) *La* dimension essentielle $\mathrm{ed}(G)$ *de G est la dimension minimale d'une G-variété linéarisable.*

Le nombre $d(n)$ qui nous occupe est donc la dimension essentielle $\mathrm{ed}(\mathfrak{S}_n)$; nous allons essayer de le déterminer, ou au moins de l'encadrer. Notons que $\mathrm{ed}(G)$ a une interprétation analogue pour tout groupe fini G : c'est le plus petit nombre de paramètres nécessaire pour définir l'équation générale de groupe de Galois G, voir [BR].

3. Dimension essentielle

3.1. Premiers exemples

Voici quelques exemples de variétés G-linéarisables.

1) Soit V une représentation linéaire fidèle de G ; l'application identique de V est bien évidemment une G-linéarisation. On a donc $\mathrm{ed}(G) \leqslant \dim(V)$. Par conséquent, si l'on note $\mathrm{rd}(G)$ la plus petite dimension d'une représentation fidèle de G (*dimension de représentation* de G), on a $\mathrm{ed}(G) \leqslant \mathrm{rd}(G)$.

2) Plaçons-nous dans la situation de 1). Le groupe G opère sur l'espace projectif $\mathbb{P}(V)$, et l'application rationnelle $V \dashrightarrow \mathbb{P}(V)$ est G-équivariante. L'action de G sur $\mathbb{P}(V)$ est fidèle si et seulement si $G \subset GL(V)$ ne contient pas d'homothétie non triviale. C'est le cas en particulier si le *centre* $Z(G)$ de G est trivial. On a donc dans ce cas $\mathrm{ed}(G) \leqslant \mathrm{rd}(G) - 1$.

3) Donnons un exemple un peu plus élaboré. Partons de l'action de $\mathfrak{S}_n$ sur $\mathbb{C}^n$ par permutation. Elle s'étend à $(\mathbb{P}^1)^n$, où $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ est la droite projective complexe (= sphère de Riemann). Le groupe $H = \mathrm{PGL}(2, \mathbb{C})$ des homographies de $\mathbb{P}^1$ opère sur $(\mathbb{P}^1)^n$; cette action se restreint à la sous-variété ouverte $(\mathbb{P}^1)^n_{\neq}$ formé des points dont les coordonnées sont toutes distinctes (complémentaire des sous-variétés d'équation $x_i = x_j$ dans $(\mathbb{P}^1)^n$). Dès que $n \geqslant 3$, H opère *librement* sur $(\mathbb{P}^1)^n_{\neq}$ – une homographie qui fixe 3 points distincts est l'identité. On peut alors former le *quotient* $X_n = (\mathbb{P}^1)^n_{\neq}/H$, c'est une variété algébrique de dimension $n-3$. L'action de $\mathfrak{S}_n$ sur $(\mathbb{P}^1)^n_{\neq}$ commute avec celle de H, elle passe donc au quotient et définit une action de $\mathfrak{S}_n$ sur X_n. *Cette action est fidèle pour* $n \geqslant 5$: comme dans ce cas le seul sous-groupe distingué non trivial de $\mathfrak{S}_n$ est $\mathfrak{A}_n$, il suffit de prouver que celui-ci n'opère pas trivialement sur X_n ; le lecteur vérifiera que la classe dans X_n de $(0, 1, 2, \ldots, n-1)$ n'est pas fixée par la permutation (123). Donc :

Proposition 1. *Pour* $n \geqslant 5$, *on a* $\mathrm{ed}(\mathfrak{S}_n) \leqslant n - 3$. ■

Notons au passage que l'action de $\mathfrak{S}_4$ sur X_4 n'est *pas* fidèle. En effet le seul invariant projectif de 4 points est le birapport, qui fournit un isomorphisme $X_4 \xrightarrow{\sim} \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$. Or il est bien connu que le birapport est invariant par le sous-groupe distingué $(\mathbb{Z}/2)^2$ de $\mathfrak{S}_4$ (« groupe de Klein »), qui opère donc trivialement sur X_4.

3.2. Propriétés élémentaires

Commençons par deux conséquences immédiates de la définition.

1) On a $\mathrm{ed}(G) \geqslant 0$, et $\mathrm{ed}(G) = 0$ si et seulement si $G = \{1\}$: seul le groupe trivial opère fidèlement sur un point.

2) Si H est un sous-groupe de G, on a $\mathrm{ed}(H) \leqslant \mathrm{ed}(G)$. En effet toute G-linéarisation $V \dashrightarrow X$ est aussi une H-linéarisation.

3.3. Groupes de dimension essentielle 1

Théorème 1. *Les groupes de dimension essentielle* 1 *sont* $\mathbb{Z}/n$ *et les groupes diédraux* $\mathbb{D}_n$ *pour n impair.*

Démonstration. Le groupe $\mathbb{Z}/n$ opère fidèlement sur $\mathbb{C}$; le groupe $\mathbb{D}_n$ a une représentation fidèle de dimension 2, et pour n impair son centre est trivial. Ces groupes sont donc de dimension essentielle 1 par 3.1, exemples 1) et 2).

Soit G un groupe de dimension essentielle 1. Il existe alors une courbe C munie d'une action de G, et une application rationnelle dominante d'un espace vectoriel dans C. Un théorème célèbre (et facile) de Lüroth affirme alors que la courbe C est *rationnelle*, c'est-à-dire birationnelle à $\mathbb{P}^1$ – on peut donc prendre $C = \mathbb{P}^1$. Or les groupes finis d'automorphismes birationnels de $\mathbb{P}^1$ sont bien connus, ce sont les sous-groupes finis de $\mathrm{SO}(3,\mathbb{R})$ (penser à la sphère de Riemann), à savoir $\mathbb{Z}/n$, $\mathbb{D}_n$, et les groupes polyédraux $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$. On remarque alors que $\mathbb{D}_n$ pour n pair et $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$ contiennent tous un sous-groupe isomorphe à $(\mathbb{Z}/2)^2$. Compte tenu de 3.2.2, le théorème résulte du lemme suivant :

Lemme 1. *On a* $\mathrm{ed}((\mathbb{Z}/2)^2) = 2$.

Démonstration. Posons $G = (\mathbb{Z}/2)^2$. On a $\mathrm{ed}(G) \leqslant 2$ puisque G admet une représentation fidèle de dimension 2 ; supposons $\mathrm{ed}(G) = 1$. Il existe alors comme ci-dessus une application rationnelle dominante G-équivariante $f : V \dashrightarrow \mathbb{P}^1$, avec $V = \mathbb{C}^2$ muni de l'action de G donnée par les matrices $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. Notons que f est définie en dehors d'un nombre fini de points : en effet on a $f(x,y) = \dfrac{P(x,y)}{Q(x,y)}$, où P et Q sont des polynômes sans facteur commun ; les points d'indétermination de f sont ceux qui vérifient $P(x,y) = Q(x,y) = 0$, ils sont en nombre fini.

La G-variété V possède un point très particulier, l'origine 0, qui est fixée par tout le groupe. Par contre G ne fixe aucun point de $\mathbb{P}^1$ (pour un choix convenable de la coordonnée z de $\mathbb{P}^1$, G est engendré par les involutions $z \mapsto -z$ et $z \mapsto 1/z$, qui n'ont pas de point fixe commun). De deux choses l'une :

• ou bien f est définie en 0 ; alors le point $f(0)$ de $\mathbb{P}^1$ est fixé par G, impossible ;

• ou bien f n'est pas définie en 0. La géométrie algébrique possède une construction miraculeuse pour traiter ce cas, l'*éclatement* de 0 dans V ; elle fournit une variété $\hat{V}$ et une application birationnelle $\varepsilon : \hat{V} \to V$ qui est un isomorphisme au-dessus de $V \smallsetminus \{0\}$, mais remplace 0 par la droite projective $\mathbb{P}(V)$; elle est facile à décrire : $\hat{V}$ est la sous-variété de $V \times \mathbb{P}^1$ formée des couples $((x,y);z)$ tels que $x = yz$, et ε est la première projection.

La composée $f \circ \varepsilon : \hat{V} \dashrightarrow \mathbb{P}^1$ est de nouveau définie en dehors d'un nombre fini de points ; elle induit donc une application rationnelle $f' : \mathbb{P}(V) \dashrightarrow \mathbb{P}^1$, qui est encore G-équivariante. Or l'élément g de G correspondant à la matrice $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ de $\mathrm{GL}(V)$ opère trivialement sur $\mathbb{P}(V)$, donc sur l'image de f', qui doit être un point de $\mathbb{P}^1$ fixé par g. Mais de nouveau ce point devrait être fixé par G tout entier : cette contradiction prouve le lemme, et donc le théorème. ∎

La même idée, un peu plus développée, conduit au résultat général suivant, dû à Kollár et Szabó ([RY], Appendice) :

Théorème 2. *Soit A un groupe* abélien, *et X une variété lisse projective A-linéarisable. Alors A fixe un point de X.*

Corollaire. *On a* $\mathrm{ed}(A) = \mathrm{rd}(A)$. *En particulier, la dimension essentielle de* $(\mathbb{Z}/n)^r$ *est* r.

Démonstration. Soit X une variété lisse projective A-linéarisable, x un point de X fixé par A. Le groupe A agit sur l'espace tangent $T_x(X)$, et cette action est localement isomorphe à celle de A sur X au voisinage de x. Par conséquent la représentation de A dans $T_x(X)$ est fidèle ; on a donc $\mathrm{rd}(A) \leqslant \dim(X)$, et par suite $\mathrm{rd}(A) \leqslant \mathrm{ed}(A)$. L'inégalité opposée est triviale (exemple 3.1.1). Enfin l'égalité $\mathrm{rd}((\mathbb{Z}/n)^r) = r$ est laissée en exercice (facile !). ■

L'égalité $\mathrm{ed}(G) = \mathrm{rd}(G)$ est encore vraie pour un p-groupe [KM] ; la démonstration utilise des méthodes beaucoup plus sophistiquées.

4. Retour à $\mathfrak{S}_n$

4.1. $\mathrm{ed}(\mathfrak{S}_n)$ pour $n \leqslant 6$

Revenons à notre problème de départ, le calcul de $d(n) = \mathrm{ed}(\mathfrak{S}_n)$.

Proposition 2. *On a* $\left[\frac{n}{2}\right] \leqslant \mathrm{ed}(\mathfrak{S}_n) \leqslant n-3$ *pour* $n \geqslant 5$.

Démonstration. Posons $p = \left[\dfrac{n}{2}\right]$. Le sous-groupe H_n de $\mathfrak{S}_n$ engendré par les transpositions $(12), \dots, (2p-1, 2p)$ est isomorphe à $(\mathbb{Z}/2)^p$, donc $\mathrm{ed}(\mathfrak{S}_n) \geqslant \mathrm{ed}(H_n) = p$ (corollaire du théorème 2). La seconde inégalité a déjà été démontrée (proposition 1). ■

Corollaire.

$$\mathrm{ed}(\mathfrak{S}_2) = \mathrm{ed}(\mathfrak{S}_3) = 1 \qquad \mathrm{ed}(\mathfrak{S}_4) = \mathrm{ed}(\mathfrak{S}_5) = 2 \qquad \mathrm{ed}(\mathfrak{S}_6) = 3\ .$$

Démonstration. Les deux premières égalités, et l'inégalité $\mathrm{ed}(\mathfrak{S}_4) \geqslant 2$, résultent du théorème 1 (noter que $\mathfrak{S}_3 = \mathbb{D}_3$). $\mathfrak{S}_4$ admet une représentation de dimension 3 et son centre est trivial, donc $\mathrm{ed}(\mathfrak{S}_4) = 2$ (3.1.2). Le cas de $\mathfrak{S}_5$ et $\mathfrak{S}_6$ résulte de la proposition. ■

Remarque 1. Les mêmes méthodes donnent $\mathrm{ed}(\mathfrak{A}_3) = 1$ et $\mathrm{ed}(\mathfrak{A}_4) = \mathrm{ed}(\mathfrak{A}_5) = 2$. L'égalité $\mathrm{ed}(\mathfrak{A}_6) = 3$ est plus subtile, voir [S]. On a donc $\mathrm{ed}(\mathfrak{A}_n) = \mathrm{ed}(\mathfrak{S}_n)$ pour $3 \leqslant n \leqslant 6$.

4.2. $\mathrm{ed}(\mathfrak{S}_7)$

À partir de $n = 7$, la proposition ne fournit qu'un encadrement de $d(n)$; on trouve par exemple $d(7) \in \{3, 4\}$. Ce cas a été réglé récemment [D1] grâce à des travaux de Prokhorov [P] :

Théorème 3. $\mathrm{ed}(\mathfrak{A}_7) = \mathrm{ed}(\mathfrak{S}_7) = 4$.

Démonstration. Comme

$$3 = \mathrm{ed}(\mathfrak{A}_6) \leqslant \mathrm{ed}(\mathfrak{A}_7) \leqslant \mathrm{ed}(\mathfrak{S}_7) \leqslant 4$$

il suffit de prouver qu'on a $\mathrm{ed}(\mathfrak{A}_7) \neq 3$. Dans le cas contraire, il existe une $\mathfrak{A}_7$-variété X lisse projective de dimension 3 et une application rationnelle dominante $f : \mathbb{C}^n \dashrightarrow X$. Cette dernière propriété entraîne que deux points généraux x, x' de X peuvent être joints par une courbe rationnelle (l'image de la droite dans $\mathbb{C}^n$ passant par deux points v, v' tels que $f(v) = x$, $f(v') = x'$) : on dit que X est *rationnellement connexe*. Le travail de Prokhorov mentionné ci-dessus classifie toutes les variétés rationnellement connexes de dimension 3 munies de l'action d'un groupe simple. Le groupe $\mathfrak{A}_7$ apparaît deux fois dans cette liste :

- $\mathfrak{A}_7$ opère par permutation des coordonnées sur la variété X d'équations $\sum X_i = \sum X_i^2 = \sum X_i^3 = 0$ dans $\mathbb{P}^6$;
- $\mathfrak{A}_7$ admet un plongement dans $\mathrm{PGL}(4, \mathbb{C})$, donc une action sur $\mathbb{P}^3$.

Dans le premier cas, on vérifie que le sous-groupe $(\mathbb{Z}/2)^2 \times \mathbb{Z}/3 \subset \mathfrak{A}_4 \times \mathfrak{A}_3 \subset \mathfrak{A}_7$ n'a pas de point fixe dans X, de sorte que X n'est pas $\mathfrak{A}_7$-linéarisable par le théorème 2.

Le second cas est plus amusant. On considère les revêtements doubles de groupes de Lie complexes

$$\mathrm{SL}(4) \longrightarrow \mathrm{SO}(6) \longrightarrow \mathrm{PGL}(4)$$

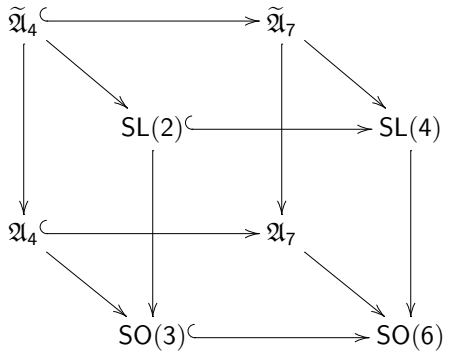
déduits de l'isomorphisme $\mathbb{C}^6 \cong \wedge^2 \mathbb{C}^4$. La représentation standard $\mathfrak{A}_7 \subset \mathrm{SO}(6)$, composée avec la deuxième flèche, fournit le plongement cherché.

L'image réciproque de $\mathfrak{A}_7$ dans $\mathrm{SL}(4)$ apparaît comme une extension centrale

$$1 \to \{\pm 1\} \longrightarrow \widetilde{\mathfrak{A}}_7 \longrightarrow \mathfrak{A}_7 \to 1 \ .$$

Lemme 2. *L'élément central -1 de $\widetilde{\mathfrak{A}}_7$ est un commutateur.*

Démonstration. Considérons le sous-groupe $\mathfrak{A}_4$ de $\mathfrak{A}_7$ qui laisse fixes les 3 dernières lettres. On a un diagramme commutatif



de sorte qu'il suffit de vérifier que -1 est un commutateur dans $\widetilde{\mathfrak{A}}_4$. Or comme $\mathrm{SL}(2)$ ne contient pas d'élément d'ordre 2 autre que -1, le groupe de Klein $(\mathbb{Z}/2)^2 \subset \mathfrak{A}_4$ se relève en le groupe quaternionien $\mathbb{Q}_8 \subset \widetilde{\mathfrak{A}}_4$, dans lequel le commutateur de deux éléments distincts différents de ± 1 est -1. ■

On a donc $-1 = (u, v)$ dans $\widetilde{\mathfrak{A}}_7$. Les éléments u, v de $\widetilde{\mathfrak{A}}_7 \subset \mathrm{SL}(4)$ ne peuvent laisser stable une même droite de $\mathbb{C}^4$, puisqu'ils commuteraient sur cette droite. Par suite leurs images dans $\mathfrak{A}_7$ ne fixent pas un même point de $\mathbb{P}^3$; comme elles commutent, le théorème 2 montre que $\mathbb{P}^3$ n'est pas $\mathfrak{A}_7$-linéarisable. ■

4.3. Peut-on aller plus loin ?

Il est évidemment tentant de conjecturer qu'on a $\mathrm{ed}(\mathfrak{A}_n) = \mathrm{ed}(\mathfrak{S}_n) = n - 3$ pour tout $n \geqslant 5$, mais je ne connais aucun argument en faveur de cette conjecture à part le fait qu'elle est vraie pour $n \leqslant 7$. Le résultat de Prokhorov est un véritable tour de force, qui utilise toute la puissance de la théorie de Mori en dimension 3 ; il semble tout à fait hors de portée d'obtenir une classification analogue en dimension plus grande. Si l'on veut progresser sur $d(n)$, il faut chercher une autre approche – peut-être des variantes plus sophistiquées du théorème 2 ?

4.4. Autres groupes

Pour les autres groupes la situation n'est guère plus brillante. Les groupes de dimension essentielle 2 ont été classifiés par Duncan [D2] ; comme la liste en est assez longue, je me bornerai à citer les deux groupes simples qui apparaissent, $\mathfrak{A}_5$ et $\mathrm{PSL}(2, \mathbb{F}_7)$. On peut déduire du théorème de Prokhorov que les groupes simples de dimension essentielle 3 sont $\mathfrak{A}_6$ et peut-être $\mathrm{PSL}(2, \mathbb{F}_{11})$ [B] – on ignore si la dimension essentielle de ce dernier groupe est 3 ou 4. On a très peu d'informations sur les autres groupes simples.

5. Développements ultérieurs

Je n'ai touché qu'à l'aspect le plus élémentaire de la notion de dimension essentielle, celui qui concerne les groupes finis sur le corps des nombres complexes. Pour finir je vais évoquer très brièvement les développements importants que le sujet a connu depuis [BR].

D'abord je me suis placé sur $\mathbb{C}$, alors que la plupart des articles sur le sujet se placent sur un corps k quelconque. Si l'on suppose que k contient suffisamment de racines de l'unité, la situation est essentiellement la même ; les choses deviennent beaucoup plus délicates si l'on affaiblit cette hypothèse. Le théorème déjà cité de [KM] traite le cas d'un p-groupe lorsque k contient les racines p-ièmes de l'unité (et $\mathrm{car}(k) \neq p$) ; sans cette hypothèse le résultat n'est pas connu, déjà dans le cas d'un groupe cyclique.

La définition de la dimension essentielle a été étendue au cas où G est un groupe algébrique [R] : on doit se borner aux représentations V qui sont « génériquement libres », c'est-à-dire où G opère librement sur un ouvert de V. On pose alors $\mathrm{ed}(G) := \min\{\dim(X) - \dim(G)\}$ pour X G-linéarisable. Sur $\mathbb{C}$, ce nombre est connu pour la plupart des groupes classiques mais pas pour $\mathrm{PGL}(n)$ par exemple.

La notion de dimension essentielle a été reformulée par Merkuriev dans le cadre très général des foncteurs sur la catégorie des extensions du corps de base [BF]. Cela s'applique notamment aux champs algébriques [BRV], dont la dimension essentielle a été calculée dans un certain nombre de cas. Nous voilà loin des essais malheureux de Tschirnhaus...

6. Références

[B] A. Beauville : *On finite simple groups of essential dimension* 3. Preprint arXiv:1101.1372.

[Br] E. Bring : *Meletemata quaedam mathematematica circa transformationem aequationum algebraicarum*. Lund (1786).

[BF] G. Berhuy, G. Favi : *Essential dimension : a functorial point of view (after A. Merkurjev)*. Doc. Math. **8** (2003), 279–330.

[BR] J. Buhler, Z. Reichstein : *On the essential dimension of a finite group*. Compositio Math. **106** (1997), no. 2, 159–179.

[BRV] P. Brosnan, Z. Reichstein, A. Vistoli : *Essential dimension of moduli of curves and other algebraic stacks*. J. Eur. Math. Soc. (JEMS) **13** (2011), no. 4, 1079–1112.

[C] G. Cardano : *Ars Magna or the rules of Algebra* (traduction anglaise). Dover, New York (1993).

[De] R. Descartes : *La Géométrie*. Jan Maire, Leyden (1637) ; disponible sur `http://fr.wikisource.org/wiki/La_Géométrie_(éd._1637)`.

[D1] A. Duncan : *Essential dimension of A_7 and S_7*. Math. Res. Lett. **17** (2010), no. 2, 263–266.

[D2] A. Duncan : *Finite Groups of Essential Dimension* 2. Comment. Math. Helvet., à paraitre.

[H] W.R. Hamilton : *Inquiry into the Validity of a Method recently proposed by George B. Jerrard, Esq. for Transforming and Resolving Equations of Elevated Degrees*. British Association Report, Bristol (1836), p. 295–348. Disponible sur `http://www.maths.tcd.ie/pub/HistMath/People/Hamilton/Jerrard/Jerrard.pdf`

[He] C. Hermite : *Sur l'équation du cinquième degré*. Comptes rendus de l'Académie des Sciences, t. LXI, 1865 (II), pp. 877, 965 et 1073 ; t. LXII, 1866 (I), pp. 65, 167, 245, 715, 919, 959, 1054, 1161 et 1213.

[J] G. B. Jerrard : *Mathematical Researches*. A.B. Strong, Bristol (1832).

[K] F. Klein : *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree* (traduction anglaise). Dover, New York (1956).

[KM] N. Karpenko, A. Merkuriev : *Essential dimension of finite p-groups*. Invent. math. **172**, 491–508 (2008).

[L] G.W. Leibniz : *Leibnizens mathematische schriften*, IV. H.W. Schmidt, Halle (1859) ; disponible sur Google books.

[P] Y. Prokhorov : *Simple finite subgroups of the Cremona group of rank* 3. J. Algebraic Geom., à paraitre.

[Ra] J. Ray : *Les mystérieuses études du docteur Drum* (Les aventures de Harry Dickson). Librio no. **154** (1998), Librio, Paris.

[R] Z. Reichstein : *On the notion of essential dimension for algebraic groups*. Transform. Groups **5** (2000), no. 3, 265–304.

[RY] Z. Reichstein, B. Youssin : *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*. With an appendix by J. Kollár and E. Szabó. Canad. J. Math. **52** (2000), no. 5, 1018–1056.

[S] J.-P. Serre : *Le groupe de Cremona et ses sous-groupes finis*. Séminaire Bourbaki 2008–2009, Exp. 1000. Astérisque **332** (2010), 75–100.

[T] E. Tschirnhaus : *Methodus auferendi omnes terminos intermedios ex data æquatione*. Acta eruditorum **2** (1683), 204–207. Traduction anglaise dans Bull. ACM SIGSAM **37** no. 1 (2003), 1–3.