INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus
Mathématique

Pierre Deligne

Le critère d'Abel pour la résolubilité par radicaux d'une équation irréductible de degré premier

Volume 359, issue 7 (2021), p. 919-921

Published online: 17 September 2021

https://doi.org/10.5802/crmath.242

Les Comptes Rendus. Mathématique *sont membres du Centre Mersenne pour l'édition scientifique ouverte*
www.centre-mersenne.org
e-ISSN : 1778-3569

Comptes Rendus
Mathématique
2021, 359, nº 7, p. 919-921
https://doi.org/10.5802/crmath.242

Théorie des Groupes / *Group theory*

Le critère d'Abel pour la résolubilité par radicaux d'une équation irréductible de degré premier

Abel's criterion for the solvability by radicals of an irreducible equation of prime degree

Pierre Deligne[*, a]

[a] Institute for Advanced Study, Princeton, NJ 08540, USA.
Courriel : deligne@math.ias.edu

Résumé. Dans sa dernière lettre à Crelle, Abel énonce un critère pour déterminer si une équation irréductible de degré premier est résoluble par radicaux. Sylow dit cet énoncé ambigu et devant être modifié. Nous montrons que le critère donné par Abel est correct tel quel.

Abstract. In his last letter to Crelle, Abel states a criterion for the solvability by radicals of an irreducible equation of prime degree. Sylow finds Abel's statement ambiguous, and writes that it should be modified. We show the correctness of Abel's original statement.

Manuscrit reçu le 21 août 2020, révisé le 1er juin 2021, accepté le 5 juillet 2021.

Dans sa dernière lettre à Crelle, datée du 18 Octobre 1828 et reproduite dans [1], Abel énonce le critère suivant pour qu'une équation irréductible de degré premier soit résoluble par radicaux :

> « Si trois racines d'une équation quelconque irréductible d'un degré marqué par un nombre premier, sont liées entre elles de la manière que l'on pourra exprimer l'une de ces racines rationnellement en les deux autres, l'équation sera toujours résoluble par radicaux. »

La théorie de Galois fournit du critère d'Abel la traduction suivante.

Théorème. *Soient p un nombre premier et G un groupe transitif de permutations d'un ensemble E à p éléments. Pour que le groupe G soit résoluble il (faut et il) suffit que quel que soit le choix de trois éléments dans E, il existe un de ces trois éléments qui est fixé par tous les éléments de G qui fixent les deux autres.*

* Auteur correspondant.

Dans l'article [3] à l'occasion du centenaire de la naissance d'Abel, Sylow écrit page 18 :

> « Abel s'est toutefois exprimé inexactement ou au moins peu clairement, et a sans doute voulu dire que toutes les racines devaient pouvoir s'exprimer rationnellement en fonction de deux d'entre elles, toujours les mêmes. Prise rigoureusement à la lettre, la proposition est inexacte, car il existe une classe d'équations à laquelle elle ne s'applique pas, tout ou moins lorsque le degré est de la forme $2^k - 1$. »

Nous montrons que, nonobstant ce que dit Sylow, l'énoncé d'Abel est correct. Nous n'avons toutefois aucune idée de quelle était sa preuve.

La preuve du lemme qui suit est due à Galois [2, propositions VI, VII et VIII].

Lemme. *Avec les hypothèses et notations du théorème, les conditions suivantes sont équivalentes :*

(i) *Il existe deux éléments de E tels que le seul élément de G qui les fixe soit l'identité.*
(ii) $|G| < p^2$.
(iii) *G contient un sous-groupe distingué A d'ordre p.*
(iv) *Une indexation $\mathbb{Z}/p \xrightarrow{\sim} E$ transforme G en un sous-groupe du groupe des affinités $x \mapsto ax + b$, contenant les translations.*
(v) *G est résoluble.*

Démonstration.

(i) ⇒ (ii). En effet, (i) implique que $|G| \leq p\,(p-1)$, le nombre de paires ordonnées d'éléments de E.

(ii) ⇒ (iii). Puisque G agit transitivement sur E, p divise l'ordre $|G|$ de G et, d'après un théorème de Cauchy, G contient un sous-groupe cyclique A d'ordre p. Il ne peut en contenir un deuxième, B, car on aurait dans ce cas $|AB| = p^2 \leq |G|$. Le sous-groupe A, étant unique, est distingué.

(iii) ⇒ (iv). Identifions E à $\mathbb{Z}/p$ de sorte que A soit le groupe des translations. Le groupe G est alors contenu dans le groupe affine des $x \mapsto ax + b$, qui est le normalisateur de A dans le groupe symétrique S_E.

(iv) ⇒ (i) et (v). Clair.

(v) ⇒ (iv). Soit $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ une suite strictement croissante de sous-groupes de G, avec G_i distingué dans G_{i+1} et G_{i+1}/G_i cyclique. Par hypothèse, l'action de G sur E est transitive et fidèle. Si $H \subset G$ est un sous-groupe distingué, ses orbites dans E ont toutes le même nombre d'éléments. Si $H \neq \{e\}$, H est donc transitif. Appliquant cet argument aux G_i, on voit par récurrence descendante que les G_i $(i > 0)$ sont transitifs. Le groupe G_1 est commutatif et agit fidèlement. Il est donc cyclique d'ordre p. Comme dans la preuve de (iii) ⇒ (iv), on peut identifier E à $\mathbb{Z}/p$ de sorte que G_1 soit le groupe des translations. Puisque G_2 normalise G_1, il est contenu dans le groupe affine, et G_1 est l'unique sous-groupe d'ordre p de G_2. Puisque G_2 est distingué dans G_3, G_3 normalise le sous-groupe caractéristique G_1 de G_2, et est contenu dans le groupe affine. Répétant l'argument jusqu'à atteindre G_n, on obtient (iv). □

Preuve du théorème. Si G est résoluble, on applique la partie (v) ⇒ (iv) du lemme. Réciproquement, supposons que G vérifie la condition énoncée par Abel. Nous prouverons (i) du lemme.

Puisque G agit transitivement sur E, $p = |E|$ divise l'ordre de G, et G contient une permutation h de E d'ordre p. Identifions E à $\mathbb{Z}/p$, de sorte que h soit la permutation $n \mapsto n + 1$ de $\mathbb{Z}/p$. Pour vérifier (i) du lemme, nous n'aurons à utiliser la condition énoncée par Abel que pour les triplets $\{a, b, c\}$ en progression arithmétique.

Pour $p = 2$, l'énoncé est trivial. Supposons $p > 2$. Supposons d'abord que pour un $k \neq 0$ et un triplet de la forme $\{a, a + k, a + 2k\}$, tout g dans G fixant a et $a + k$ fixe aussi $a + 2k$. Conjuguant par une puissance de h, on obtient le même énoncé pour tout a. Si g fixe a et $a + k$, il fixe $(a + k)$

et $(a+k)+k$, et donc $a+3k$. Itérant l'argument, on voit que g fixe tous les $a+nk$, c'est à dire E tout entier. La clause (i) du lemme est donc vérifiée par a et $a+k$.

Appliquant ceci à - k et au triplet $\{a+2k, a+k, a\}$, on voit que si tout g dans G fixant $a+2k$ et $a+k$ fixe aussi a, la clause (i) du lemme est vérifiée par $a+2k$ et $a+k$.

Si pour aucun triplet en progression arithmétique ces arguments ne permettent de conclure, alors, quels que soient a et b distincts, si g dans G fixe a et b, g fixe aussi $\frac{1}{2}(a+b)$. Sous cette hypothèse, montrons par récurrence sur n que si g fixe 0 et b, g fixe aussi les $2^{-n}.i.b$ pour $0 \leq i \leq 2^n$. Considérant deux i consécutifs, et leur moyenne, on obtient en effet les $2^{-(n+1)}i.b$ (i impair) à partir des $2^{-n}.i.b$. Dès que $2^n \geq p$, E entier est atteint de sorte que la clause (i) du lemme est vérifiée par 0 et b. □

Références

[1] N. H. Abel, *Oeuvres complètes. Nouvelle édition publiée aux frais de l'État Norvégien par MM. L. Sylow et S. Lie.*, Christiania. Grøndahl et Søn, 1881, Tome 2, XXII, p. 270.

[2] É. Galois, « Mémoire sur les conditions de résolubilité des équations par radicaux », *J. Math. Pures et Appl.* **11** (1846), p. 417-433.

[3] L. Sylow, « Les études d'Abel et ses découvertes », in *Niels Henrik Abel, Mémorial publié à l'occasion du centenaire de sa naissance*, Christiania. Grøndahl et Søn, 1902.