

JOURNAL
DE
MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

CAMILLE JORDAN

Théorèmes sur les équations algébriques

Journal de mathématiques pures et appliquées 2^e série, tome 14 (1869), p. 139-146.

http://www.numdam.org/item?id=JMPA_1869_2_14__139_0



NUMDAM

Article numérisé dans le cadre du programme
Gallica de la Bibliothèque nationale de France
<http://gallica.bnf.fr/>

et catalogué par Mathdoc
dans le cadre du pôle associé BnF/Mathdoc
<http://www.numdam.org/journals/JMPA>

Théorèmes sur les équations algébriques;

PAR M. CAMILLE JORDAN [*].

1. On peut appeler *ordre* d'une équation algébrique l'ordre (ou nombre des substitutions) de son groupe.

Si le groupe G d'une équation algébrique E a pour ordre O et contient un autre groupe H ayant pour ordre $\frac{O}{l}$, une fonction des racines de E , invariable par les substitutions de H , dépendra d'une équation irréductible de degré l .

Si le groupe G d'une équation algébrique ne contient aucun autre groupe auquel toutes ses substitutions soient permutable (sauf le groupe formé par la substitution *unité*), cette équation est *simple* et ne pourra être résolue par aucune équation auxiliaire, dont l'ordre ne soit pas un multiple du sien.

Si le groupe G ne jouit pas de la propriété ci-dessus, on pourra déterminer (souvent de plusieurs manières) une suite de groupes $G, H, I, \dots$, tels, que chacun d'eux soit contenu dans le précédent et permutable à ses substitutions, et ne soit contenu dans aucun groupe plus général jouissant de cette double propriété. Soient $O, \frac{O}{l}, \frac{O}{lm}, \dots, 1$ les ordres de ces groupes successifs. La résolution de l'équation proposée se ramène à la résolution successive d'équations simples dont les racines sont des fonctions rationnelles de celles de la proposée, et qui ont respectivement pour ordre $l, m, \dots$.

Ces nombres $l, m, \dots$ seront dits les *facteurs de composition* de la

[*] Cet article et le suivant sont extraits d'un *Traité des équations algébriques* en cours de publication.

proposée (ou de son groupe). Ils restent les mêmes, à l'ordre près, de quelque manière qu'on détermine la suite $G, H, I, \dots, 1$ [*].

2. THÉORÈME. — *Soit G' un groupe quelconque contenu dans un autre groupe G ; ses facteurs de composition diviseront ceux de G .*

Soient en effet O l'ordre de G ; $l, m, \dots$ ses facteurs de composition; $G, H, I, \dots$ une suite de groupes ayant respectivement pour ordre $O, \frac{O}{l}, \frac{O}{lm}, \dots$ et tels, que chacun d'eux soit contenu dans le précédent et permutable à ses substitutions. Soient, d'autre part, $G', H', I', \dots$ les groupes respectivement formés par celles des substitutions de G' qui appartiennent à G , à H , à I , etc.; $O', \frac{O'}{l'}, \frac{O'}{l'm'}, \dots$ leurs ordres respectifs. Chacun de ces groupes sera évidemment contenu dans le précédent, et, de plus, permutable à ses substitutions. Car, soient, par exemple, g' et h' deux substitutions quelconques appartenant aux groupes G' et H' : h' appartient à H , auquel les substitutions de G , et notamment g' , sont permutables. Donc $g'^{-1}h'g'$ appartient à H ; mais elle appartient aussi à G' : donc elle appartient à H' ; donc g' est permutable à ce dernier groupe.

Soient $\frac{O'}{\lambda_1}$ l'ordre d'un groupe G'_1 aussi général que possible parmi ceux qui contiennent H' , et sont contenus dans G' et permutables à ses substitutions; $\frac{O'}{\lambda_1 \lambda_2}$ l'ordre d'un groupe G'_2 , aussi général que possible parmi ceux qui contiennent H' et sont contenus dans G'_1 et permutables à ses substitutions, etc. Soient de même $\frac{O'}{\mu_1}$ l'ordre d'un groupe H'_1 aussi général que possible parmi ceux qui contiennent I' , et sont contenus dans H' et permutables à ses substitutions, etc. Les groupes $G', G'_1, G'_2, \dots, H', H'_1, \dots, I', \dots$ formant ainsi par construction une suite telle, que chacun d'eux soit aussi général que possible parmi ceux qui sont contenus dans le précédent et permutables à ses

[*] Pour la démonstration de ces résultats, voir le *Commentaire sur Galois* que nous avons inséré dans les *Mathematische Annalen*, t. I.

substitutions, et ayant respectivement pour ordre $O', \frac{O'}{\lambda_1}, \frac{O'}{\lambda_1 \lambda_2}, \dots, \frac{O'}{l}, \frac{O'}{l' \mu_1}, \dots, \frac{O'}{l' m'}, \dots$, les facteurs de composition de G' seront $\lambda_1, \lambda_2, \dots, \frac{l'}{\lambda_1 \lambda_2 \dots}, \mu_1, \dots, \frac{m'}{\mu_1 \dots}, \dots$. Ils diviseront donc respectivement $l', m', \dots$.

Nous achèverons la démonstration en prouvant que $l', m', \dots$ divisent respectivement $l, m, \dots$.

Soient en effet $h_1, h_2, \dots$ les substitutions de H ; $h'_1, h'_2, \dots$ celles de H' ; celles de G' seront de la forme $g'_\alpha h'_\beta$; $g'_1, g'_2, \dots, g'_l$ étant des substitutions de G' qui ne satisfassent à aucune relation de la forme $g'_\alpha = g'_\alpha h'_\beta$ (SERRET, *Algèbre supérieure*, n° 413). Cela posé, les substitutions de G' , appartenant à G , sont permutables à H . Le groupe K , dérivé de la combinaison de G' et de H , aura donc toutes ses substitutions de la forme $g'_\alpha h'_\beta h_\gamma$. Mais $h'_\beta h_\gamma$, appartenant à H , est de la forme h_δ : les substitutions de K seront donc de la forme $g'_\alpha h_\delta$. Réciproquement, les $l' \frac{O}{l}$ substitutions de cette forme obtenues en faisant varier α et δ appartiennent à G , et sont distinctes: car si l'on avait $g'_\alpha h_\delta = g'_{\alpha'} h_{\delta'}$, sans avoir $\alpha = \alpha'$, d'où $\delta = \delta'$, la substitution $g'^{-1}_{\alpha'} g'_\alpha = h_{\delta'} h^{-1}_\delta$ appartiendrait à H et à G' , et par suite à H' : désignons-la par h'_β ; il viendrait $g'_\alpha = g'_{\alpha'} h'_\beta$, ce qui est impossible.

Donc l'ordre de K est égal à $l' \frac{O}{l}$; mais ce groupe est contenu dans G , dont l'ordre est O ; donc son ordre divise ce dernier nombre: donc l' divise l . De même m' divise m , etc.

3. THÉORÈME. — Soient G un groupe quelconque; H et G' deux groupes contenus dans G ; H' le groupe formé par les substitutions communes aux deux précédents; O, P, O', P' les ordres respectifs de ces quatre groupes; d, d', e, f les valeurs des entiers $\frac{O}{P}, \frac{O'}{P'}, \frac{O}{O'}, \frac{P}{P'}$, δ le plus grand commun diviseur de d et de e : d' sera au plus égal à d , et divisible par $\frac{d}{\delta}$.

Soient en effet $h_1, h_2, \dots$ les substitutions de H ; $h'_1, h'_2, \dots$ celles de H' : celles de G' seront de la forme $g'_\alpha h'_\beta$; $g'_1, \dots, g'_{d'}$ étant des sub-

stitutions convenablement choisies. En outre, le groupe G contiendra au moins les substitutions $g'_\alpha h_\beta$, qui sont toutes distinctes et en nombre Pd' . On aura donc $Pd' \leq O$, d'où $d' \leq d$.

D'autre part, la relation évidente $ed' = df$ montre que d' est divisible par $\frac{d}{\delta}$.

4. THÉORÈME. — *Soit E une équation décomposable en facteurs rationnels $X, Y, \dots$: tout facteur de composition d'une des équations partielles $X, Y, \dots$ sera un facteur de composition de E ; et réciproquement, tout facteur de composition de E sera facteur de composition d'une ou plusieurs de ces équations partielles.*

En effet, on résoudra l'équation E en résolvant successivement les équations partielles $X, Y, \dots$, ce qui pourra se faire pour chacune d'elles à l'aide d'une suite d'équations simples.

Soient $\alpha_1, \alpha_2, \dots$ les racines de l'équation X , lesquelles appartiennent également à E ; l son premier facteur de composition : il existe une équation simple U , d'ordre l , dont la résolution fera connaître des fonctions de $\alpha_1, \alpha_2, \dots$ qui auparavant n'étaient pas rationnelles. Cette résolution abaissera donc l'ordre de X et celui de E en les divisant l'un et l'autre par l . Quant à chacune des autres équations partielles, telle que Y , son ordre ne sera pas réduit par cette résolution, ou il sera divisé par l , auquel cas Y aura l pour facteur de composition.

Si donc on résout l'équation X par l'adjonction des racines d'une suite d'équations simples, on trouvera successivement que chacun des facteurs de composition de X est un facteur de composition de E . Quant aux autres équations partielles $Y, \dots$, leurs groupes pourront perdre par ces adjonctions quelques-uns de leurs facteurs de composition, mais conserveront tous ceux qui ne leur sont pas communs avec le groupe de X . Résolvant maintenant l'équation Y par l'adjonction des racines d'une suite d'équations simples, on verra de même que tous les facteurs de composition qui restent dans le groupe de l'équation Y sont des facteurs de composition de E ; et que les équations partielles restantes $Z, \dots$ conserveront après cette nouvelle adjonction tous ceux de leurs facteurs de composition qui ne leur sont pas communs avec X ou Y . On continuera ainsi jusqu'à ce qu'on ait résolu

successivement toutes les équations $X, Y, \dots$. Mais alors l'équation E sera elle-même résolue, et le théorème sera démontré.

5. THÉORÈME. — Soient ε une équation irréductible et primitive de degré n ; E l'équation de degré $n - 1$ obtenue par l'adjonction d'une de ses racines, a ; $X, Y, \dots$ les diviseurs rationnels de cette dernière équation, supposée réductible. Tout facteur de composition de l'une des équations partielles $X, Y, \dots$ divisera l'un au moins des facteurs de composition de chacune des autres équations partielles.

Supposons, pour fixer les idées, qu'il y ait deux équations partielles, X et Y , et que Y ait un facteur de composition, m , qui ne divise aucun des facteurs de composition de X ; nous allons prouver que l'équation ε , supposée irréductible, n'est pas primitive.

Soit en effet G le groupe de l'équation E : abaissons-le autant que possible par la résolution successive d'équations simples, dont l'ordre ne soit pas divisible par m ; et supposons que ces adjonctions réduisent successivement le groupe de l'équation E à $H, \dots$, à K . L'équation partielle X étant complètement résolue par ces opérations, et l'équation Y ne l'étant pas, le groupe final K contiendra des substitutions différentes de l'unité; mais les racines $x_1, x_2, \dots$ de X , qui sont actuellement connues, ne seront déplacées par aucune de ces substitutions.

La suite des facteurs de composition de K peut être déterminée, soit d'une seule manière, soit de plusieurs manières différentes; mais, dans tous les cas, le premier de ces facteurs sera divisible par m ; car, sans cela, le groupe pourrait être abaissé, contrairement à l'hypothèse, par la résolution d'une équation simple dont l'ordre ne serait pas divisible par m . Réciproquement, K contient tous les groupes contenus dans G et jouissant de cette propriété. Car soit G' un groupe quelconque contenu dans G et non dans K . Supposons, pour fixer les idées, que parmi les groupes de la suite $G, H, \dots, K$, le groupe H soit le premier qui ne contienne pas G' : soit H' le groupe formé par les substitutions communes à H et à G' ; soient enfin $O, \frac{O}{l}, O', \frac{O'}{l'}$ les ordres respectifs de G, H, G', H' . Les premiers facteurs de

composition de G' , $\lambda_1, \lambda_2, \dots$ auront pour produit l' , qui divise l (2) : ils ne sont donc pas divisibles par m .

6. Soient maintenant $a, a_1, \dots, a_{\mu-1}$ celles des racines de E que les substitutions de K laissent immobiles. Cette suite contenant, outre la racine a que l'on s'est adjointe, les racines $x_1, x_2, \dots$ de l'équation X , contient plusieurs racines; d'autre part, elle ne les contient pas toutes.

Cela posé, soient $\mathcal{G}$ le groupe de $\mathcal{E}$; S une de ses substitutions, qui remplace a par une des racines $a, a_1, \dots, a_{\mu-1}$, telle que a_1 : elle remplacera toutes ces racines les unes par les autres. En effet, S transforme le groupe G , formé des substitutions de $\mathcal{G}$ qui ne déplacent pas a , en un groupe analogue G_1 , formé de celles de ces substitutions qui ne déplacent pas a_1 . Ceux des groupes partiels contenus dans G_1 qui jouissent de la propriété d'avoir leur premier facteur de composition nécessairement divisible par m seront évidemment les transformés de ceux des groupes partiels contenus dans G qui jouissent de cette propriété. Ils seront donc tous contenus dans un seul d'entre eux, qui sera le transformé de K , et aura seul le même ordre que ce dernier groupe. Mais G_1 contient K lui-même; ce sera donc là ce groupe d'ordre maximum qui contient tous les autres et qui est le transformé de K . Donc la substitution S transforme K en lui-même : donc elle permute exclusivement entre elles les racines $a, a_1, a_2, \dots$ que les substitutions de K ne déplacent pas.

Toute substitution de $\mathcal{G}$ qui remplace l'une par l'autre deux des racines $a, a_1, \dots, a_{\mu-1}$ permute ces racines exclusivement entre elles. Car soit T une substitution de $\mathcal{G}$ qui remplace, par exemple, a_1 par a_2 ; ST , remplaçant a par a_2 , permutera exclusivement entre elles les racines $a, a_1, \dots, a_{\mu-1}$: il en est de même pour S ; donc il en est de même pour T .

Soient a' une autre racine quelconque; U une substitution de $\mathcal{G}$ qui remplace a par a' : les racines $a', a'_1, \dots, a'_{\mu-1}$ que U fait succéder à $a, a_1, \dots, a_{\mu-1}$ seront, d'après ce qui précède, essentiellement différentes de $a, a_1, \dots, a_{\mu-1}$. D'ailleurs toute substitution de $\mathcal{G}$ qui remplace une des racines $a, a_1, \dots, a_{\mu-1}$ par une des racines $a', a'_1, \dots, a'_{\mu-1}$ remplacera chacune des racines $a, a_1, \dots, a_{\mu-1}$ par quelque une des racines $a', a'_1, \dots, a'_{\mu-1}$. Car soit V une substitution de $\mathcal{G}$ qui remplace,

par exemple, a par a'_1 : VU^{-1} remplace a par a_1 : elle remplacera donc les racines $a, a_1, \dots, a_{\mu-1}$ les unes par les autres; et U les remplaçant par $a', a'_1, \dots, a'_{\mu-1}$, $V = VU^{-1}$. U les remplacera également, à l'ordre près, par $a', a'_1, \dots, a'_{\mu-1}$.

Si les 2μ racines écrites ci-dessus n'épuisent pas le nombre n des racines de $\mathcal{E}$, soient a'' une autre racine, W une substitution de $\mathcal{G}$ qui remplace a par a'' : les racines $a'', a''_1, \dots, a''_{\mu-1}$ que W fait succéder à $a, a_1, \dots, a_{\mu-1}$ sont, d'après ce qui précède, essentiellement différentes de $a, a_1, \dots, a_{\mu-1}$ et de $a', a'_1, \dots, a'_{\mu-1}$.

Si $n > 3\mu$, on continuera de même; et l'on voit ainsi que n est un multiple de μ , et que les racines de la proposée peuvent être groupées en $\frac{n}{\mu}$ systèmes. D'ailleurs chaque substitution de $\mathcal{G}$ remplace les racines de chaque système par celles d'un même système. Car soit R une substitution de $\mathcal{G}$, qui remplace, par exemple, a'' par a'_1 ; et soient $a'_1, \alpha, \dots, \vartheta$ les racines qu'elle fait succéder à $a'', a''_1, \dots, a''_{\mu-1}$. La substitution WR appartient à $\mathcal{G}$, et remplace $a, a_1, \dots, a_{\mu-1}$ par $a'_1, \alpha, \dots, \vartheta$. Mais a'_1 appartient au système $a'_1, a'_2, \dots, a'_{\mu-1}$. Donc $\alpha, \dots, \vartheta$ sont les autres racines de ce système.

Donc l'équation $\mathcal{E}$ n'est pas primitive, ce qu'il fallait démontrer.

7. COROLLAIRE I. — *L'équation $\mathcal{E}$ étant irréductible et primitive, tout nombre premier qui divise l'ordre de E divisera l'ordre de chacune des équations partielles $X, Y, \dots$*

Car soit p un semblable diviseur. Divisant l'ordre de E , il divise un de ses facteurs de composition; mais ce facteur de composition appartient à l'une au moins des équations partielles $X, Y, \dots$ (4). Donc il divise un au moins des facteurs de composition de chacune des autres équations : donc il divise l'ordre de chacune d'elles.

COROLLAIRE II. — *Si l'une des équations partielles $X, Y, \dots$ a tous ses facteurs de composition premiers, il en est de même des autres.*

8. THÉORÈME. — *Si une équation E , irréductible et de degré n , a son ordre divisible par un nombre premier p , supérieur à $\frac{1}{2}n$, son groupe G sera $n - p + 1$ fois transitif.*

Supposons en effet que G soit $n - q + 1$ fois transitif, q étant $< p$. Son ordre sera égal à $n(n-1)\dots(q+1)\Omega$, Ω étant l'ordre du groupe partiel $\mathcal{G}$ formé par celles de ses substitutions qui laissent immobiles $n - q$ racines données $a, a_1, \dots$, lequel est simplement transitif par rapport aux q racines restantes. Mais $n(n-1)\dots(q+1)$ n'est pas divisible par p , n étant $< 2p$ et $q > p$. D'autre part, Ω ne peut être divisible par p . En effet, considérons l'équation $\mathcal{C}$ de degré q à laquelle se réduit la proposée par l'adjonction des racines $a, a_1, \dots$; elle a évidemment pour groupe $\mathcal{G}$. Si elle n'est pas primitive, soit μ le nombre des systèmes entre lesquels se répartissent ses racines : son ordre Ω sera un diviseur de $1.2\dots\mu\left(1.2\dots\frac{q}{\mu}\right)^\mu$, et ne sera pas divisible par p , qui est supérieur à $\frac{q}{2}$, et, par suite, à μ et à $\frac{q}{\mu}$. Si, au contraire, l'équation $\mathcal{C}$ est primitive, son ordre est égal à qO , O étant l'ordre de l'équation E' , de degré $q - 1$, qu'on obtient en s'adjoignant une nouvelle racine b . Mais $\mathcal{G}$ étant simplement transitif, le groupe de E' , formé par celles des substitutions de $\mathcal{G}$ qui laissent b immobile, sera intransitif : l'équation E' se décompose donc en plusieurs facteurs rationnels $X, Y, \dots$. L'une au moins de ces équations partielles sera d'un degré d inférieur à $\frac{q}{2}$, et, par suite, à p ; son ordre, divisant $1.2\dots d$, ne sera pas divisible par p . Mais il est divisible par tout nombre premier qui divise O : donc O , et, par suite, $\Omega = qO$ n'est pas divisible par p .

