JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

CAMILLE JORDAN

Sur l'équation aux vingt-sept droites des surfaces du troisième degré

Journal de mathématiques pures et appliquées 2^e série, tome 14 (1869), p. 147-166.
<http://www.numdam.org/item?id=JMPA_1869_2_14__147_0>

Sur l'équation aux vingt-sept droites des surfaces du troisième degré;

PAR M. CAMILLE JORDAN.

1. Steiner a fait connaître (*Journal de M. Borchardt*, t. LIII) les théorèmes suivants :

Toute surface du troisième degré contient vingt-sept droites.

L'une quelconque d'entre elles, a, en rencontre dix autres, se coupant elles-mêmes deux à deux, et formant ainsi avec a cinq triangles. Le nombre total des triangles ainsi formés sur la surface par les vingt-sept droites est de quarante-cinq.

Si deux triangles abc, a'b'c' n'ont aucun côté commun, on peut leur en associer un troisième a''b''c'' tel, que les côtés correspondants de ces trois triangles se coupent, et forment trois nouveaux triangles aa'a'', bb'b'', cc'c''.

D'après cela, désignons par les lettres a, b, c, d, e, f, g, h, i, k, l, m, n, p, q, r, s, t, u, m', n', p', q', r', s', t', u' les vingt-sept droites : on formera sans peine le tableau suivant des quarante-cinq triangles, où la désignation des droites reste seule arbitraire :

abc, ade, afg, ahi, akl, bmn, bpq, brs, btu, $cm'n'$, $cp'q'$, $cr's'$, $ct'u'$, dmm', dpp', drr', dtt', enn', eqq', ess', euu', fmq', $fn'p$, fst', fur', gnp', $gm'q$, gru', gts', hms', $hn'r$, hqt', $hp'u$, inr', $im's$, itq', ipu', kmu', $kn't$, kqr', $kp's$, lnt', $lm'u$, $lq'r$, $ls'p$.

2. Étant données maintenant l'équation d'une surface du troisième degré et les équations d'une droite arbitraire, exprimons que la droite est contenue tout entière sur la surface. Nous obtiendrons des équations de condition qui permettront d'exprimer rationnellement

trois des paramètres de la droite en fonction du quatrième, qui sera déterminé par une équation du vingt-septième degré, dont chaque racine correspondra à l'une des vingt-sept droites. Nous conviendrons de désigner par a, b, c,... celles des racines de cette équation qui correspondent respectivement aux droites a, b, c,....

Le groupe G de l'équation considérée est exclusivement formé des substitutions qui n'altèrent pas la forme algébrique de la fonction suivante :

$$\varphi = abc + ade + \ldots + ls'p.$$

En effet, soient S une de ses substitutions, abc l'un des termes de φ. Les droites a, b, c forment un triangle, et cette propriété géométrique s'exprime par un système de relations analytiques

$$\varphi(a, b, c) = 0, \quad \psi(a, b, c) = 0, \ldots$$

entre les racines a, b, c. Les fonctions φ, ψ,..., ayant leur valeur nulle, et par suite rationnelle, ne sont pas altérées en valeur numérique par la substitution S. Si donc S remplace a, b, c par trois autres racines a', b', c', on aura

$$\varphi(a', b', c') = 0, \quad \psi(a', b', c') = 0, \ldots.$$

Donc les trois droites a', b', c' forment un triangle, et $a'b'c'$ sera l'un des termes de φ. Donc S transforme les termes de φ les uns dans les autres.

Réciproquement, si l'on admet que toutes les relations géométriques existant entre les vingt-sept droites peuvent se déduire de celles qui précèdent, ce qui est au moins fort probable, G contiendra toutes les substitutions qui n'altèrent pas φ.

Cette hypothèse étant admise, cherchons à déterminer le groupe G.

3. Soient μ le nombre des positions différentes où les substitutions de G permettent d'amener a; μ_1 celui des positions différentes où celles de ces substitutions qui laissent a immobile permettent d'amener b; μ_2 celui des positions différentes où celles des substitutions de G qui laissent a et b immobiles permettent de faire passer d; μ_3 celui des systèmes de positions que celles des substitutions de G

qui laissent a, b, d immobiles permettent d'assigner à m, p, r, t; μ_4 celui des substitutions de G qui laissent a, b, d, m, p, r, t immobiles. L'ordre de G sera évidemment égal à $\mu\mu_1\mu_2\mu_3\mu_4$.

Or μ est au plus égal à 27, nombre total des lettres : μ_1 ne peut dépasser 10; car toute substitution de G qui laisse a immobile permute exclusivement entre eux les cinq termes de φ qui contiennent a; elle remplace donc b, qui figure dans ces termes, par l'une des dix racines b, c, d, e, f, g, h, i, k, l qui y figurent également. De même μ_2 ne peut dépasser 8; car toute substitution de G qui laisse a et b immobiles n'altérera pas le terme abc, qui seul dans φ est divisible par ab : donc elle laissera c invariable, et permutera exclusivement entre elles les huit racines d, e, f, g, h, i, k, l. D'autre part, μ_3 ne peut dépasser 24; car toute substitution de G qui ne déplace pas a, b, c, d n'altérera pas les coefficients de leurs diverses puissances dans la fonction φ. Elle laissera donc invariables e, $fg + hi + kl$, $mn + pq + rs + tu$, $m'n' + p'q' + r's' + t'u'$, $mn' + pp' + rr' + tt'$, $nn' + qq' + ss' + uu'$. Donc elle permute exclusivement entre elles les quatre racines m, p, r, t, communes aux deux expressions $mn + pq + rs + tu$, et $mm' + pp' + rr' + tt'$; ce qui ne peut avoir lieu que de vingt-quatre manières. Enfin l'on voit de même que μ_4 se réduit à l'unité.

4. Donc l'ordre de G ne peut dépasser $27.10.8.24$. Mais il est égal à ce chiffre, car on vérifie de suite que G contient les substitutions

$$\begin{aligned}
A &= (amu)\,(cnt)\,(gq'r')\,(is'p')\,u'ld)\,(m'ek),\\
B &= (bhk)\,(cil)\,(pt'r')\,(ns'u')\,(p'tr)\,(n'su),\\
C &= (dhk)\,(eil)\,(pus)\,(m's'u')\,(qtr)\,(n'r't'),\\
D &= (fil)\,(ghk)\,(n'u's')\,(mtr)\,(m't'r')\,(nus),\\
E &= (fhk)\,(gil)\,(p'r't')\,(q's'u')\,(prt)\,(qsu),\\
F &= (hk)\,(il)\,(r't')\,(s'u')\,(rt)\,(su),
\end{aligned}$$

dont les cinq premières, combinées entre elles, permettent évidemment de faire succéder a à l'une quelconque des vingt-sept racines. Les substitutions B, C, D, E permettent ensuite, sans déplacer a, d'amener b à la place de l'une quelconque des dix racines b, c, d, e, f, g, h, i, k, l. Puis les substitutions C, D, E permettent, sans déplacer a, b

de faire succéder d à l'une quelconque des huit racines d, e, f, g, h, i, k, l. Les substitutions D, E, qui ne déplacent pas a, b, d, permettent de faire succéder m et p à deux quelconques des quatre racines m, p, r, t, ce qui donne pour ces racines douze systèmes de places distincts. Enfin la dernière substitution permet de permuter entre elles les deux racines restantes r et t, sans déplacer a, b, d, m, p.

Donc G ne contient pas moins de $27.10.8.12.2$ substitutions; en outre, le groupe partiel H dérivé des seules substitutions A, B, C, D, E en contient au moins $27.10.8.12$. Nous allons prouver : 1° qu'il en contient précisément ce nombre; 2° qu'il est permutable à toutes les substitutions de G.

5. Chacune des substitutions de G, transformant les uns dans les autres les divers termes de φ, équivaut à un certain déplacement opéré entre ces termes. Les divers déplacements ainsi équivalents aux diverses substitutions de G forment un groupe G_1, dont les substitutions correspondent une à une à celles de G. Celles des substitutions de G_1 qui résultent d'un nombre pair de transpositions entre les termes abc, ade,... forment un groupe partiel $\mathfrak{H}_1$ permutable aux substitutions de G_1. Les substitutions correspondantes du groupe G forment un groupe $\mathfrak{H}$, permutable aux substitutions de G. En effet, soient S, S' deux substitutions de $\mathfrak{H}$; S_1, S'_1 les substitutions correspondantes de $\mathfrak{H}_1$: $S_1 S'_1$ faisant partie de $\mathfrak{H}_1$, sa correspondante SS' fera partie de la suite $\mathfrak{H}$, laquelle formera ainsi un groupe. D'autre part, soient T une substitution quelconque de G, T_1 sa correspondante : $T_1^{-1} S_1 T_1$ faisant partie de $\mathfrak{H}_1$, sa correspondante $T^{-1}ST$ fera partie de $\mathfrak{H}$; donc T sera permutable à $\mathfrak{H}$.

Or on vérifie sans difficulté que chacune des substitutions A, B, C, D, E équivaut à un nombre pair de transpositions entre les termes abc, ade,.... Donc H, qui en dérive, est contenu dans $\mathfrak{H}$. Au contraire, la substitution F, équivalente à un nombre impair de transpositions, n'est pas contenue dans ce groupe. Donc $\mathfrak{H}$, dont l'ordre est un diviseur de celui de G, renferme au plus la moitié des substitutions de ce dernier groupe. Mais il contient H, qui en renferme la moitié : ces deux groupes sont donc identiques.

6. Les facteurs de composition de G sont évidemment 2 et les fac-

teurs de composition de H. Nous allons démontrer que ce dernier groupe est simple.

Considérons d'abord les racines a, b, c, d, m, m'. Elles forment deux termes, abc, dmm', de la fonction φ : de plus, a et d, b et m, c et m' se retrouvent ensemble dans trois autres termes, ade, bmn, $cm'n'$, de cette fonction. Chaque substitution de H, devant laisser φ invariable, fera succéder a, b, c, d, m, m' à un système de six racines α, β, γ, δ, μ, μ' jouissant de propriétés analogues. Réciproquement, soit α, β, γ, δ, μ, μ' un système quelconque de six racines jouissant de ces propriétés : H contiendra une substitution qui remplace ces racines par a, b, c, d, m, m'. En effet, si cela n'avait pas lieu, le nombre des systèmes tels que α, β, γ, δ, μ, μ' serait supérieur à celui des systèmes de places où les substitutions H permettent d'amener a, b, c, d, m, m'. Mais le premier de ces deux nombres ne peut dépasser $27.10.32$: car α peut être choisie de vingt-sept manières : cela fait, β, devant se rencontrer avec α dans un même terme de φ, ne peut être choisie que de dix manières; et γ sera déterminée par là : on pourra ensuite prendre pour $\delta\mu\mu'$ l'un quelconque des trente-deux termes de φ qui n'ont aucune lettre commune avec $\alpha\beta\gamma$; et δ, μ, μ' seront alors déterminées sans ambiguïté par la condition de se trouver respectivement avec α, β, γ dans un même terme de φ. D'un autre côté, les substitutions H permettent de donner à a vingt-sept places distinctes, puis à b dix places distinctes, puis à d huit places distinctes, puis à m quatre places distinctes : le nombre des systèmes de places qu'elles permettent de donner à a, b, c, d, m, m' est donc au moins égal à $27.10.8.4$, et *à fortiori* au nombre des systèmes α, β, γ, δ, μ, μ'.

7. Soit maintenant I un groupe contenu dans H, et permutable à ses substitutions : nous allons prouver qu'il se confond avec H.

1° I *contient une substitution différente de l'unité et qui ne déplace pas a*. En effet, soit S une substitution de I, qui remplace a par une autre racine α : α pourra être l'une des racines b, c, d, e, f, g, h, i, k, l, ou l'une des seize autres racines.

Dans le premier cas, on peut supposer $\alpha = b$. Car H contient une substitution Σ qui remplace α par b sans déplacer a; et I contiendra $\Sigma^{-1}S\Sigma$, qui remplace a par b. Soient donc $\alpha = b$. Si parmi les sub-

stitutions C, D, E, il en est une, T, non échangeable à S, I contiendra $S^{-1}.T^{-1}ST$, qui diffère de l'unité, et ne déplace pas a. Si, au contraire, S est échangeable à la fois à C, D, E, elle permutera exclusivement ensemble, d'une part les trois racines a, b, c que ces substitutions laissent immobiles, d'autre part les deux racines m, n, que D déplace et que C, E laissent immobiles. Si donc S ne laisse aucune racine immobile, elle permutera circulairement, d'une part les trois racines a, b, c, d'autre part les deux racines m et n : son carré ne se réduira pas à l'unité, et laissera m et n immobiles. Donc I contient dans tous les cas une substitution qui laisse quelque racine immobile. Soient S_1 cette substitution, β cette racine, Σ une des substitutions de H qui remplacent β par a : I contiendra $\Sigma^{-1}S_1\Sigma$, qui laisse a immobile.

Dans le second cas, on peut supposer $\alpha = m$. En effet, les substitutions dérivées de B, C, D, E permutent transitivement les seize racines m, n,... sans déplacer a. Soit Σ celle d'entre elles qui remplace α par m : I contiendra $\Sigma^{-1}S\Sigma$, qui remplace a par m. Soit donc $\alpha = m$. Si parmi les substitutions B, C, E, il est une, T, non échangeable à S, I contiendra la substitution $S^{-1}.T^{-1}ST$, qui ne déplace pas a. Dans le cas contraire, il faudra que S permute exclusivement ensemble, d'une part a et m, de l'autre les trois racines d, e, m' : cela posé, la démonstration s'achève comme au premier cas.

8. 2° I *contient une substitution, autre que l'unité, et qui laisse a, b immobiles.* Car soit S la substitution qui laisse a immobile, et dont on vient de démontrer l'existence : elle remplacera b par une des dix racines b, c, d, e, f, g, h, i, k, l qui se trouvent associées à a dans les termes de φ. Donc si S déplace b, elle le remplacera par c, ou par une des huit autres lettres.

Si S remplace b par c, il faudra, pour qu'elle n'altère pas φ, qu'elle n'altère pas le terme abc : donc elle remplacera c par b. Cela posé, si parmi les substitutions C, D, E, il en existe une, T, qui ne soit pas échangeable à S, I contiendra $S^{-1}.T^{-1}ST$, qui laisse a, b immobiles. Si au contraire S était échangeable à ces trois substitutions, elle permuterait exclusivement entre elles les racines m, n, que C, E laissent immobiles. Mais alors elle changerait le terme bmn en cmn, qui n'est pas un terme de φ : ce qui est absurde.

Si S remplace b par l'une, β, des huit racines $d, e, \ldots, l$, on voit comme tout à l'heure qu'on peut supposer $\beta = d$. Cela posé, si l'une T des substitutions D, E n'est pas échangeable à S, I contiendra $S^{-1}.T^{-1}ST$, qui laisse a et b immobiles. Dans le cas contraire, et sachant d'ailleurs que S permute exclusivement entre elles les dix racines $b, c, d, e, f, g, h, i, k, l$, associées à a dans les termes de φ, on vérifie sans peine qu'elle devra permuter exclusivement entre elles les deux racines f, g. Cela posé, I contiendra la transformée de S par EB^{-1}, laquelle laisse a immobile, et permute b et c exclusivement entre elles. On retombe ainsi sur un cas déjà discuté.

9. 3° I *contient une substitution autre que l'unité, et qui laisse a, b, d immobiles*. Car soit S la substitution qui laisse a et b immobiles et dont on vient de démontrer l'existence. N'altérant pas φ, elle n'altérera pas le terme abc : elle laissera donc c immobile. Si elle déplace d, elle le remplacera par e, ou par une des racines f, g, h, i, k, l.

Si S remplace d par e, il faudra, pour qu'elle n'altère pas φ, qu'elle n'altère pas le terme ade : donc elle remplacera réciproquement e par d. Cela posé, si parmi les substitutions D et E il en est une, T, qui ne soit pas échangeable à S, I contiendra $S^{-1}.T^{-1}ST$, qui laisse a, b, d immobiles. Dans le cas contraire, S permutera exclusivement entre elles les deux racines f, g. Si elle les laisse immobiles, I contiendra la transformée de S par EC^{-1}, laquelle laisse a, b, d immobiles. Si au contraire elle échange les deux racines f et g, il faudra, pour être échangeable à D et à E, qu'elle permute exclusivement entre elles les racines de chacun des systèmes ih, lk, $mnm'n'$, $pqp'q'$, $rsr's'$, $tut'u'$; et comme elle doit en outre transformer φ en elle-même on trouvera

$$S = (de)(fg)(hi)(kl)(mn)(pq)(rs)(tu)(m'n')(p'q')(r's')(t'u').$$

Cela posé, I contiendra la substitution $S^{-1}.B^{-1}SB = S'$, qui laisse a, d, f immobiles : et H contenant une substitution Σ qui remplace a, d, e, f, m, q' par a, b, c, d, m, m' (6), I contiendra $\Sigma^{-1}S'\Sigma$, qui laisse a, b, d immobiles.

Si S remplace d par l'une, β, des racines f, g, h, i, k, l, on peut supposer $\beta = h$. Cela posé, si S n'est pas échangeable à la substitution

$DE^{-1} = T$, I contiendra $S^{-1}.T^{-1}ST$, qui laisse a, b, d invariables. Si elle lui est échangeable, elle permutera exclusivement ensemble les racines d, e, h, i autres que a, b, c et que T laisse immobiles.

Or S remplace d par h : si elle remplace réciproquement h par d, on aura $S = DCU$, U étant une substitution de H qui laisse a, b, d, h immobiles. Mais les substitutions de H permettent d'amener a, b, d à $27.10.8$ systèmes de places distinctes : les substitutions D et E qui ne déplacent pas ces trois racines permettent d'amener ensuite h à six places distinctes. L'ordre de H est donc égal à $27.10.8.6.\nu$, ν étant le nombre des substitutions de ce groupe qui ne déplacent pas a, b, d, h. On déduit de là $\nu = 2$. Les deux seules substitutions que l'on puisse prendre pour U sont donc l'unité et la substitution T.

Soit en premier lieu $U = 1$, d'où $S = DC$. Cette substitution laisse immobiles a, b, c, p', q' : et H contenant une substitution Σ qui remplace c, p', q', a, d, e par a, b, c, d, m, m' (**6**), I contiendra $\Sigma^{-1}S\Sigma$, qui laisse a, b, d immobiles.

Soit en second lieu $U = T$. La substitution S laisse immobiles a, b, c, m, n : et H contenant une substitution Σ qui remplace b, m, n, a, d, e par a, b, c, d, m, m' (**6**), I contiendra $\Sigma^{-1}S\Sigma$, qui laisse a, b, d immobiles.

Supposons maintenant que S remplace h par e : I contiendra S^2, qui remplace d par e; et l'on retombe sur un cas déjà discuté.

Enfin, si h est remplacé par i, H contient une substitution Σ qui remplace a, h, i, b, m, n, par a, d, e, b, m, n (**6**) ; et I contenant $\Sigma^{-1}S\Sigma$, qui remplace d par e, sans déplacer a ni b, on retombe encore sur un cas déjà discuté.

10. 4° I *contient la substitution* E. En effet, soit S la substitution de I qui ne déplace pas a, b, d, et dont l'existence vient d'être démontrée. Si elle ne déplace pas m, elle se réduira à E ou à son carré, qui lui-même, étant élevé au carré, reproduira E. Si, au contraire, S déplace m, elle la remplace par l'une des trois racines p, r, t, et il est permis de supposer que c'est par t. On aura alors $S = VD$, V étant une substitution de H qui ne déplace pas a, b, d, m, et qui, par suite, se réduit à une puissance de E.

Supposons d'abord $V = 1$, d'où $S = D$. Cette substitution laisse im-

mobiles a, b, c, d, p, p'; et H contenant une substitution Σ qui remplace ces racines par a, b, c, d, m, m' (**6**), I contiendra $\Sigma^{-1}S\Sigma$, qui laisse a, b, d, m immobiles, et se réduit à E ou à E^2.

Si $V = E$, S laissera immobiles a, b, c, d, r, r'; et H contenant une substitution Σ qui remplace ces racines par a, b, c, d, m, m' (**6**), I contiendra $\Sigma^{-1}S\Sigma$, qui se réduit à E ou à E^2.

Si enfin $V = E^2$, I contiendra la substitution $S^{-1}.A^{-1}SA = S'$, qui laisse b, r, s, p, d, p' immobiles; et H contenant une substitution Σ qui remplace ces lettres par a, b, c, d, m, m' (**6**), I contiendra $\Sigma^{-1}S'\Sigma$, qui se réduit à E ou à E^2.

11. 5° I *se confond avec* H : car il contient les puissances de E, et leurs transformées par les substitutions de H. Mais A, B, C, D, E, dont H dérive, font toutes partie du système de ces transformées : car A, par exemple, laisse immobiles b, r, s, p, u', f; mais H contient une substitution Σ qui remplace ces lettres par a, b, c, d, m, m' : la transformée de A par Σ laissera donc a, b, d, m immobiles, et se réduira à une puissance de E. Réciproquement, la transformée de cette dernière substitution par Σ^{-1} reproduira A.

12. L'équation aux vingt-sept droites a plusieurs réduites remarquables, signalées par divers géomètres.

1° Prenons, par exemple, pour inconnue de la question le plan du triangle formé par trois droites qui se coupent : ces triangles étant au nombre de quarante-cinq, on aura une équation du quarante-cinquième degré, équivalente à la proposée.

2° On peut déterminer de $\frac{45.32}{2}$ manières différentes un système de deux triangles qui n'aient aucune droite commune; à chaque semblable système correspond un triangle associé (**1**). Réciproquement, chaque système de trois triangles associés (*trièdre* de Steiner) correspond aux trois combinaisons deux à deux des triangles qui les forment. Le nombre total de ces trièdres sera donc $\frac{45.32}{2.3}$. On peut d'ailleurs les grouper par paires (*doubles trièdres*) en réunissant ensemble ceux qui contiennent les mêmes droites. Enfin les doubles trièdres peuvent être associés trois à trois, en réunissant ensemble ceux qui n'ont au-

cune droite commune. Prenant pour inconnue ce système de trois doubles trièdres, on aura une équation de degré $\frac{45.32}{2.3\ 2.3} = 40$, et équivalente à la proposée.

3° On peut déterminer de $\frac{27.16}{2}$ manières différentes une paire de droites qui ne se coupent pas. On peut d'ailleurs grouper ces paires six à six (*doubles-six* de Schläfli), de telle sorte que les droites d'une paire rencontrent chacune une droite de chaque autre paire du double-six. Les doubles-six dépendent donc d'une équation du degré $\frac{27.16}{2.6} = 36$, qui sera encore équivalente à la proposée.

Aucune réduite d'un degré inférieur au vingt-septième n'ayant été rencontrée jusqu'ici, on était fondé à penser qu'il est impossible de ramener la résolution de l'équation aux vingt-sept droites à celle d'une équation d'un degré inférieur. Nous allons en effet prouver cette proposition.

13. En effet, si un semblable abaissement de degré pouvait avoir lieu, il aurait lieu *à fortiori* après l'adjonction de la racine carrée qui réduit le groupe de la proposée à H. Supposons donc cette adjonction opérée : soient E_{27} l'équation aux vingt-sept droites, E_d celle des équations équivalentes dont le degré d est minimum : cette dernière équation sera irréductible et primitive. En effet, ses racines sont des fonctions rationnelles de celles de E_{27} (*Commentaire sur Galois,* cité p. 140). Si donc E_d n'était pas irréductible, elle se décomposerait en facteurs irréductibles de degré inférieur à d; et la résolution d'un seul de ces facteurs, faisant connaître des fonctions des racines de E_{27} qui auparavant n'étaient pas rationnelles, abaisserait le groupe de cette équation. Mais ce groupe H est simple : donc l'équation E_{27} serait complétement résolue; donc d ne serait pas le minimum supposé. D'autre part, si E_d n'était pas primitive, ses racines se grouperaient en systèmes, dépendant d'une équation dont le degré divise d, et la résolution de cette dernière équation, abaissant le groupe de E_{27}, la résoudrait complétement; donc, ici encore, d ne serait pas minimum.

Cela posé, l'ordre du groupe G_d de E_d est égal à celui du groupe de E_{27}, lequel est $\Omega = 27.10.8.6.2\,(5)$; mais il est divisible par d, et

divise $1.2\ldots d$. Donc si $d < 27$, il sera l'un des nombres 24, 20, 18, 16, 15, 12, 10, 9.

14. *Il n'existe aucune réduite de degré* 24, 18 *ou* 12. Car soit, pour fixer les idées, $d = 24$. Adjoignons à l'équation E_{24} une de ses racines, x : l'équation E_{23} qui détermine les vingt-trois racines restantes a son groupe G_{23} formé des substitutions qui laissent x immobile, et son ordre est égal à $\frac{\Omega}{24}$, nombre divisible par les nombres premiers 2, 3, 4. Les équations irréductibles dont elle est le produit ont donc leur ordre divisible par ces trois nombres premiers, à l'exclusion de tous les autres (Mém. précéd., **7**). Donc chacune de ces équations est du degré 5 au moins; en outre, aucune d'elles n'a pour degré 7, 8 ou 9, car son ordre ne pourrait être divisible par 5 sans l'être par 7 (Mém. précéd., **8**); enfin aucune d'elles n'a son degré divisible par un nombre premier autre que 2, 3, 5, car ce nombre premier diviserait son ordre. D'après cela, les seules hypothèses admissibles pour les degrés de ces facteurs irréductibles sont les suivantes : 18 et 5; 12, 6 et 5; 6, 6, 6 et 5.

Mais ces hypothèses elles-mêmes doivent être rejetées. Considérons, par exemple, la première (les mêmes raisonnements s'appliqueraient aux deux autres). Supposons que E_{23} soit le produit de deux facteurs E_{18} et E_5, ayant respectivement pour racines $y_1,\ldots, y_{18}$ et $x_1,\ldots, x_5$. L'ordre du groupe partiel $\Gamma^{(\mu)}$ formé par celles des substitutions de G_{24} qui laissent immobiles x et x_μ sera $\frac{\Omega}{24.5}$ et celui du groupe partiel $\Delta^{(\nu)}$ formé par celles de ces substitutions qui laissent immobiles x et y_ν sera $\frac{\Omega}{24.18}$. Soit maintenant S une substitution de G_{24}, qui remplace x par x_μ, et soient z une autre racine quelconque de E_{24}, u la racine que S lui fait succéder. Le groupe partiel formé par les substitutions qui laissent x_μ et u immobiles est le transformé par S de celui dont les substitutions laissent x et z immobiles : il contiendra donc $\frac{\Omega}{24.5}$ ou $\frac{\Omega}{24.18}$ substitutions, suivant que z sera l'une des racines $x_1,\ldots, x_5$ ou l'une des racines $y_1,\ldots, y_{18}$.

Or l'équation E_5 ayant son ordre divisible par 3, son groupe est trois

fois transitif (Mém. précéd., **8**); donc le groupe formé par celles des substitutions de G_{23} qui laissent immobiles deux quelconques de ses racines, x_μ et $x_{\mu'}$, a pour ordre $\frac{\Omega}{24.5.4}$. Le groupe formé par celles des substitutions de G_{24} qui jouissent de cette propriété, contenant celui-là, a pour ordre un multiple de ce nombre; donc il ne peut avoir pour ordre $\frac{\Omega}{24.18}$; donc les cinq racines telles, que le groupe partiel formé par celles des substitutions de G_{24} qui laissent immobile l'une d'elles en même temps que x_μ ait pour ordre $\frac{\Omega}{24.5}$, sont x, $x_1,\ldots$, $x_{\mu-1}$, $x_{\mu+1},\ldots$. Mais S les fait succéder aux cinq racines $x_1,\ldots$, x_5, qui jouissent de la même propriété par rapport à x. Donc S permute exclusivement entre elles les six racines x, $x_1,\ldots$, x_μ; d'où l'on déduirait, comme au n° **6** du Mémoire précédent, que E_{24} n'est pas primitive, ce qui est contraire au numéro précédent.

15. *Il n'existe aucune réduite de degré* 20, 15 *ou* 10. Car s'il existait, par exemple, une réduite du vingtième degré, le groupe $\mathfrak{H}$ formé par celles des substitutions de H qui laissent sa racine invariable aurait pour ordre $\frac{\Omega}{20}$: et le groupe K formé par celles des substitutions de H qui laissent immobile la racine a ayant pour ordre $\frac{\Omega}{27}$, l'ordre du groupe $\mathfrak{K}$ formé par les substitutions communes à $\mathfrak{H}$ et à K serait $\frac{\Omega}{27.20}$, ou le vingtième de l'ordre de K (Mém. précéd., **3**).

Cela posé, les substitutions de K sont de la forme $A_\mu B_\mu$; A_1, $A_2,\ldots$ étant des substitutions partielles qui permutent ensemble les dix racines b, c, d, e, f, g, h, i, k, l, et B_1, $B_2,\ldots$ des substitutions opérées en même temps sur les seize autres racines : d'ailleurs on voit sans peine qu'aucune substitution de K (à l'exception de l'unité) ne laisse les dix premières racines immobiles à la fois. Soient en particulier $\mathfrak{A}_1\mathfrak{B}_1$, $\mathfrak{A}_2\mathfrak{B}_2,\ldots$ les substitutions de $\mathfrak{K}$: le groupe $\mathfrak{K}'$ formé par les substitutions partielles $\mathfrak{A}_1$, $\mathfrak{A}_2,\ldots$ opérées sur les dix premières lettres sera évidemment contenu dans le groupe K′ formé par les substitutions partielles A_1, $A_2,\ldots$, et contiendra un vingtième du nombre total de ses substitutions.

Or on voit immédiatement que K′, dérivé des substitutions

$$(bhk)(cil), \quad (dhk)(eil), \quad (fil)(ghk), \quad (fhk)(gil),$$

contient : 1° les substitutions qui résultent d'un nombre pair de transpositions entre les cinq systèmes binaires bc, de, fg, hi, kl : 2° les substitutions qui ne déplacent pas les systèmes, mais permutent ensemble les deux racines dans un nombre pair de systèmes. On reconnaît en outre facilement que tout groupe tel que $\mathfrak{K}'$, contenu dans K′ et contenant le vingtième de ses substitutions, contient le groupe L′ formé par ces dernières substitutions. D'ailleurs L′ est permutable aux substitutions de K′; et réciproquement tout groupe contenu dans K′ et permutable à ses substitutions est contenu dans L′.

Les substitutions de K et de K′ se correspondent évidemment une à une, de telle sorte qu'au produit de deux substitutions correspond le produit de sa correspondante. Le groupe $\mathfrak{K}$, formé des substitutions de K dont le premier facteur appartient à $\mathfrak{K}'$, contiendra le groupe L formé des substitutions de K dont le premier facteur appartient à L′ : donc $\mathfrak{H}$, qui contient $\mathfrak{K}$, contiendra L. En outre, L sera permutable aux substitutions de K, et réciproquement tout groupe contenu dans K et permutable à ses substitutions sera contenu dans L.

Soient maintenant S une substitution quelconque de H; a_1 la racine par laquelle elle remplace a : elle transformera K, L en deux autres groupes K_1, L_1, qui jouent par rapport à la racine a_1 le même rôle que K, L par rapport à la racine a. Raisonnant comme précédemment, on voit que $\mathfrak{H}$ contiendra L_1. Donc $\mathfrak{H}$ contiendra les transformées des substitutions de L par une substitution quelconque de H; mais ce dernier groupe étant simple, ces transformées, combinées entre elles, le reproduisent tout entier. Donc $\mathfrak{H}$, au lieu de contenir, comme il le faudrait, le vingtième des substitutions de H, se confondrait avec lui.

16. *Il n'existe aucune réduite du degré* 16. S'il en existait une, E_{16}, soient E_{15} l'équation qui donne quinze de ses racines après l'adjonction de la seizième, G_{15} son groupe, O_{15} son ordre : on voit, comme au n° **14**, que si E_{15} n'est pas irréductible, elle se décompose en deux facteurs du dixième et du cinquième degré, ou en trois facteurs du cinquième.

Mais E_{15} ne peut se décomposer en trois facteurs du cinquième degré : car l'ordre de E_{16} diviserait $(1.2...5)^3.16$ et ne pourrait être égal à Ω.

Supposons maintenant $E_{15} = E_{10}E_5$. L'équation du cinquième degré E_5, ayant son ordre O_5 divisible par 3, a son groupe G_5 trois fois transitif : d'ailleurs O_5, divisant $\frac{\Omega}{16}$, n'est pas divisible par 8; donc le groupe G_5 est alterné. Cela posé, soient G_{10} le groupe de E_{10}, O_{10} son ordre : on aura évidemment $\frac{\Omega}{16} = O_{15} = O_{10}P$, P étant l'ordre du groupe partiel Γ formé par celles des substitutions de G_{15} qui ne déplacent pas les racines de E_{10}. Ce dernier groupe est évidemment contenu dans G_5 et permutable à ses substitutions; et le groupe G_5 étant simple, Γ se confond avec lui ou ne contient d'autre substitution que l'unité. Mais si Γ se confondait avec G, P serait divisible par 5 et $O_{10}P$ par 25, tandis que $\frac{\Omega}{16}$ ne l'est pas. Il faut donc admettre la seconde hypothèse, d'où $P = 1$, $\frac{\Omega}{16} = O_{10}$.

Cela posé, adjoignons à l'équation E_{10} une de ses racines, δ : l'équation E_9 qui détermine les autres aura pour ordre $\frac{\Omega}{16.10} = 2.3^4$. Il faut évidemment pour cela qu'elle soit irréductible, mais que l'équation E_8 obtenue en s'adjoignant une nouvelle racine se décompose en facteurs irréductibles ayant chacun pour degré 1, 2, 3 ou 6. L'ordre de E_8 devant être égal à 2.3^2, l'un au moins de ces facteurs aura pour degré 3 ou 6, et il est aisé de voir que quelque hypothèse qu'on fasse sur les degrés de ces facteurs, l'équation E_9 sera non primitive (Mémoire précédent, n° 5). Cela posé, soient $\alpha, \beta, \gamma; \alpha', \beta', \gamma'; \alpha'', \beta'', \gamma''$ ses racines : on voit immédiatement que l'ordre de E_9 ne peut être égal à 2.3^4 que si son groupe G_9 est dérivé des substitutions

$$(\alpha\beta\gamma), \quad (\alpha'\beta'\gamma'), \quad (\alpha''\beta''\gamma''), \quad (\alpha\alpha')(\beta\beta')(\gamma\gamma'), \quad (\alpha\alpha'')(\beta\beta'')(\gamma\gamma'').$$

Il est facile maintenant de prouver l'impossibilité du groupe G_{10}. Ce groupe, étant deux fois transitif, contiendrait une substitution S qui remplace α, β, γ par δ, β, et par une autre racine ε (différente

ou non de α et de γ) : et G_{10} contiendrait la substitution $(\delta\beta\varepsilon)$, transformée de $(\alpha\beta\gamma)$ par S. Soient maintenant ζ une autre racine quelconque; T une substitution de G_{10} qui remplace ζ par δ; $\alpha_1, \beta_1, \gamma_1, \delta_1, \varepsilon_1$ les racines que T fait succéder à $\alpha, \beta, \gamma, \delta, \varepsilon$: les substitutions $(\delta_1\beta_1\varepsilon_1), (\alpha_1\beta_1\gamma_1)$, transformées de $(\delta\beta\varepsilon), (\alpha\beta\gamma)$ par T, ne déplaçant pas δ, appartiendraient à G_9; résultat absurde, car le groupe dérivé de ces deux substitutions, alterné par rapport à $\alpha_1, \beta_1, \gamma_1, \delta_1, \varepsilon_1$, ayant son ordre divisible par 4, ne peut être contenu dans G_9, dont l'ordre est 2.3^4.

17. Supposons maintenant l'équation E_{15} irréductible et primitive. Adjoignons-lui une de ses racines, x; l'équation E_{14} qui donne les racines restantes aurait pour ordre $O_{14} = \frac{\Omega}{16.15} = 4.27$, et se décomposerait en facteurs irréductibles dont l'ordre divise ce nombre, et admet les diviseurs premiers 2 et 3. On aurait donc deux facteurs du quatrième degré avec un du sixième, ou avec deux du troisième.

1° Ces deux hypothèses doivent être rejetées. En effet, considérons d'abord la première. Soient E'_4, E''_4, E_6 les trois facteurs de E_{14}. L'ordre de E_6 étant premier à 5, l'équation E_5 qui s'en déduit par l'adjonction d'une de ses racines sera décomposable en plusieurs facteurs irréductibles, et de quelque manière qu'on imagine que cette décomposition ait lieu, on arrivera à cette conclusion que E_6 n'est pas primitive (Mémoire précédent, n° 5). Les racines se grouperont donc deux par deux en trois systèmes, ou trois à trois en deux systèmes.

Le premier cas est inadmissible : car O_{14} serait divisible par 8 ou ne le serait pas par 27, et, par suite, ne saurait se confondre avec $\frac{\Omega}{16\ 15}$. En effet, O_{14} est égal au produit de O_6, ordre de E_6, par P, ordre du groupe Γ formé par celles des substitutions de G_{14} qui ne déplacent pas les racines de E_6. Chaque substitution de ce dernier groupe est le produit de deux substitutions partielles opérées respectivement sur les racines de E'_4 et de E''_4 : et son ordre est évidemment divisible par l'ordre P′ du groupe Γ' formé par les premières substitutions partielles. Mais Γ' est contenu dans le groupe G'_1 de l'équation E'_4 et évidemment permutable à ses substitutions. D'ailleurs G'_4 ayant son ordre divisible

par 4 et par 3, et non par 8, est alterné; et l'on voit immédiatement qu'il y a trois groupes contenus dans G'_4 et permutables à ses substitutions, lesquels ont respectivement pour ordre 12, 4 et 1. Donc $P' = 12$, 4 ou 1. Mais O_6 étant divisible par 6, $O_{14} = O_6 P$ sera divisible par 8 si $P' > 1$. On doit donc admettre que Γ' se réduit à la seule substitution 1. On voit de même que le groupe Γ'' formé par les secondes substitutions partielles se réduit à la seule substitution 1. Mais alors on aura $O_{14} = O_6$, et ce nombre divisant $1.2.3.(1.2)^3$ ne sera pas divisible par 27.

Supposons, au contraire, que les racines de E_6 se groupent trois à trois en deux systèmes. On aura $O_{14} = 2R$, R étant l'ordre du groupe I formé par celles des substitutions de G_{14} qui ne déplacent pas ces deux systèmes. Mais chaque substitution de I est le produit de trois substitutions partielles, opérées respectivement sur les racines de E'_4, de E''_4 et de E_6. Soit I' le groupe formé par les premières substitutions partielles; il est clair qu'il contiendra au moins six des douze substitutions du groupe alterné G'_4 : d'ailleurs I étant permutable aux substitutions de G_{14}, I' le sera *à fortiori* à celles de G'_4; donc I' contient les douze substitutions de G'_4. Cela posé, R étant évidemment divisible par l'ordre de I', O_{14} le sera par 8, ce qui est inadmissible.

2° Il reste à examiner le cas où E_{14} se décomposerait en deux facteurs du quatrième et deux du troisième degré. Mais l'impossibilité de cette hypothèse (l'équation E_{15} étant supposée primitive) se démontre par des considérations toutes semblables à celles du n° **14**.

18. Il nous reste à démontrer que E_{15} ne peut être à la fois irréductible et non primitive. Si cela avait lieu, ses racines se grouperaient cinq à cinq en trois systèmes, ou trois à trois en cinq systèmes. Examinons successivement ces deux cas.

1° Si les racines de E_{15} formaient trois systèmes, son groupe G_{15} aurait pour ordre mP, m étant le nombre de positions différentes que ses substitutions donnent aux systèmes, et P l'ordre du groupe I formé par celles des substitutions de G_{15} qui ne déplacent pas ces systèmes. Ces dernières substitutions sont de la forme $A_1^{(\mu)} A_2^{(\mu)} A_3^{(\mu)}$; A'_1, A''_1,... étant des substitutions partielles opérées sur les racines du premier système; A'_2, A''_2,..., et A'_3, A''_3,... d'autres substitutions partielles

opérées en même temps sur les racines du second et du troisième système.

Soient respectivement I_1, I_2, I_3 les groupes formés par les substitutions partielles A'_1, A''_1,...; A'_2, A''_2,...; A'_3, A''_3,...; $B'_2B'_3$, $B''_2B''_3$,... celles des substitutions de I qui ne déplacent que les racines des deux derniers systèmes; K le groupe formé par ces substitutions; K_2 le groupe formé par les substitutions partielles B'_2, B''_2,...; soit enfin L le groupe formé par celles des substitutions de I qui ne déplacent que les racines du troisième système. Il est clair que K est contenu dans I et permutable à ses substitutions : donc *à fortiori* K_2 est contenu dans I_2 et permutable à ses substitutions. De même L est contenu dans I_3, et permutable à ses substitutions.

Les groupes I_1, I_2, I_3 ont leur ordre divisible par 5. En effet, l'ordre de I est évidemment égal au produit des ordres p, q, r des groupes I_1, K_2, L. Mais E_{15} a pour ordre $O_{15} = \frac{\Omega}{16} = 2^2.3^4.5 = mpqr$. D'ailleurs m divise 1.2.3; donc un des nombres, p, q, r, et un seul, est divisible par 5. Supposons que q, par exemple, soit divisible par 5 : I_2, contenant K_2, aura *à fortiori* son ordre divisible par 5. D'ailleurs G_{15} contient une substitution S qui remplace les racines du second système par celles du premier : cette substitution transforme I_2 en I_1; donc p, ordre de I_1, est divisible par 5. De même pour l'ordre de I_3.

Le nombre p étant divisible par 5, comme on vient de le voir, q et r ne le seront pas. Ils se réduiront donc à l'unité; car si q, par exemple, était > 1, les racines du second système pourraient être partagées en classes, en réunissant ensemble celles que les substitutions de K_2 permutent entre elles : cela posé, les substitutions de I_2, étant permutables à K_2, permuteraient exclusivement entre elles les racines appartenant aux classes les moins nombreuses; donc I_2 ne serait pas transitif, et son ordre ne pourrait être divisible par 5.

Soit donc $q = r = 1 : O_{15}$, se réduisant à mp, divisera 1.2.3.1.2.3.4.5 et ne pourra être égal à $\frac{\Omega}{16}$, comme cela devrait être.

19. 2° Si les racines de E_{15} formaient cinq systèmes, $\frac{\Omega}{16} = O_{15}$ serait encore égal à mP, m étant le nombre de positions différentes que les

substitutions de G_{15} donnent aux systèmes, et P l'ordre du groupe I.

Supposons d'abord que m soit divisible par 3 : les déplacements des systèmes formeront un groupe de degré 5, transitif et dont l'ordre est divisible par 3 : ce groupe sera donc trois fois transitif; et son ordre n'étant pas divisible par 8, il sera alterné. On aura donc $m = 5.4.3$, d'où $P = 27$. Ce résultat est impossible. En effet, chaque substitution de I serait de la forme $A_1^{\alpha_1} A_2^{\alpha_2} A_3^{\alpha_3} A_4^{\alpha_4} A_5^{\alpha_5}$; $A_1, \ldots, A_5$ désignant des substitutions circulaires effectuées respectivement entre les racines du premier,..., du cinquième système, et $\alpha_1, \ldots, \alpha_5$ des entiers nuls ou positifs; et l'on aurait $P = nQ$, n étant le nombre de systèmes de valeurs non congrues suivant le module 3 que prennent, dans les substitutions de I, les entiers α_1, α_2, lequel divise 9, et Q le nombre des substitutions de I qui se réduisent à la forme $A_3^{\alpha_3} A_4^{\alpha_4} A_{15}^{\alpha_5}$. Donc $Q > 1$, et I, contient une substitution S de cette dernière forme, autre que l'unité. Supposons, pour plus de généralité que dans S les valeurs de α_3, α_4 diffèrent de o (mod. 3). Transformons cette substitution par celles de G_{15} qui laissent immobiles les troisième et quatrième systèmes, en remplaçant le cinquième par le premier et par le second. On obtiendra deux transformées telles que $A_3^{\beta_3} A_4^{\beta_4} A_1^{\beta_1}$, $A_3^{\gamma_3} A_4^{\gamma_4} A_2^{\gamma_2}$; $\beta_3, \beta_4, \gamma_3, \gamma_4$ étant des entiers différents de o (mod. 3). Cela posé, deux des trois rapports $\frac{\alpha_3}{\alpha_4}, \frac{\beta_3}{\beta_4}, \frac{\gamma_3}{\gamma_4}$ seront nécessairement congrus par rapport à 3. Soit, par exemple, $\frac{\beta_3}{\beta_4} \equiv \frac{\gamma_3}{\gamma_4}$. Les deux dernières substitutions ci-dessus, combinées entre elles, donneront la suivante : $A_1^{\beta_1} A_2^{-\gamma_2 \frac{\beta_3}{\gamma_3}}$, qui ne déplace plus que les racines de deux systèmes. Cette substitution, transformée par celles de G_{15}, donnera des substitutions déplaçant les racines de deux systèmes quelconques. Cela posé, soient respectivement $P_1, P_2, \ldots$, les ordres des groupes $I_1, I_2, \ldots$, formés par celles des substitutions de I qui laissent immobiles les racines du premier système, celles des deux premiers systèmes, etc., on aura

$$P = 3P_1 = 3^2 P_2 = 3^3 P_3 = 3^4 P_4 > 27.$$

Supposons enfin m non divisible par 3. On a

$$P = \varepsilon_1 P_1 = \varepsilon_1 \varepsilon_2 P_2 = \varepsilon_1 \varepsilon_2 \varepsilon_3 P_3,$$

$\varepsilon_1, \varepsilon_2, \varepsilon_3$ étant des diviseurs de 1.2.3. Mais $P = \frac{\Omega}{16m}$ est divisible par 3^4 : donc P_3 est divisible par 3, et I_3 contient une substitution S, autre que l'unité, et de la forme $A_4^{\alpha_4} A_5^{\alpha_5}$. Les entiers α_4, α_5 différeront de o (mod. 3); car si l'on avait $\alpha_5 \equiv o$, I contiendrait les transformées de S par les substitutions de G_{15}, transformées dont les puissances, combinées entre elles, reproduisent les 3^5 substitutions de la forme $A_1^{\alpha_1} \ldots A_5^{\alpha_5}$. Donc P, et, par suite, $\frac{\Omega}{16}$ serait divisible par 3^5, ce qui n'a pas lieu,

On peut évidemment, sans nuire à la généralité de la question, supposer $\alpha_4 \equiv 1$, $\alpha_5 \equiv 2$. On voit de même que I contient une substitution de la forme $A_5^{\beta_5} A_1^{\beta_1}$, β_5 et β_1 différant de o (mod. 3). Cette substitution (ou son carré si $\beta_2 \equiv 2$) sera de la forme $A_5 A_1^{\gamma_1}$, et l'on peut supposer $\gamma_1 \equiv 2$. On voit de même que I contient les substitutions $A_1 A_2^2$, $A_2 A_3^2$, $A_3 A_4^{\delta_4}$, δ_4 étant $\gtrless o$ (mod. 3). Mais ces substitutions, combinées entre elles, donnent la substitution $A_4^{1+\delta_4}$, que I doit contenir, ce qui ne serait pas possible, d'après ce qui précède, si δ_4 ne se réduisait pas à 2. Donc I contient les substitutions $A_1 A_2^2$, $A_2 A_3^2$,..., $A_5 A_1^2$, et en général toutes celles de la forme $A_1^{\alpha_1} \ldots A_5^{\alpha_5}$ pour lesquelles $\alpha_1 + \ldots + \alpha_5 \equiv o$, lesquelles dérivent de celles-là.

Le groupe G_{15} ne peut contenir aucune autre substitution d'ordre 3. Car cette substitution, ne déplaçant pas les systèmes, par hypothèse, serait de la forme $A_1^{\alpha_1} \ldots A_5^{\alpha_5}$, $\alpha_1 + \ldots + \alpha_5$ étant $\gtrless o$ (mod. 5); et en la combinant aux précédentes, on aurait un groupe d'ordre 3^5 contenu dans G_{15}, ce qui est impossible.

Soient maintenant a_1, b_1, c_1,..., a_5, b_5, c_5 les racines de E_{15}; x la dernière racine de E_{16}. Le groupe G_{16} de E_{16}, étant deux fois transitif, contient une substitution S qui remplace a_1 et b_1 par x et a_1 : et la transformée de $A_1 A_2^2 = (a_1 b_1 c_1)(a_2 c_2 b_2)$ par S sera de la forme $T = (x a_1 y)(zuv)$, y, z, u, v étant les racines que S fait succéder à c_1, a_2, c_2, b_2.

Supposons d'abord que y soit une des racines b_1, c_1, par exemple, b_1. Les substitutions $A_2^{\alpha_2} \ldots A_5^{\alpha_5}$ d'ordre 3 contenus dans I et qui laissent x, a_1, b_1 immobiles forment un groupe évidemment permutable à T, ou, ce qui revient au même, à la substitution partielle (zuv). Il faut pour cela que (zuv) soit une puissance de l'une des substitutions

$A_2, \ldots, A_5$, de A_2 par exemple. Cela posé, la substitution $A_1 A_2^2$, multipliée par T ou par T^2, donnera une substitution U qui laisse immobiles toutes les racines autres que a_1, b_1, c_1, x.

Supposons, au contraire, que y soit une autre racine, telle que a_2; (zuv) sera permutable à celles des substitutions de I qui sont de la forme $A_3^{\alpha_3} A_4^{\alpha_4} A_5^{\alpha_5}$, et, par suite, sera une puissance de l'une des substitutions A_3, A_4, A_5, ou permutera entre elles trois des racines b_1, c_1, b_2, c_2. Mais dans ce dernier cas, le produit de S par $A_1 A_2^2$ ou par son carré donne une substitution d'ordre 7, ce qui est inadmissible, Ω n'étant pas divisible par 7. Admettons donc que (zuv) soit une puissance de A_3 : S, combinée avec $A_2 A_3^2$, donne une substitution U qui laisse immobiles toutes les racines, sauf a_1, a_2, b_2, c_2, x.

Donc G_{16} contiendra dans tous les cas une substitution U qui déplace cinq racines au plus. Soit x' une des racines que U laisse immobiles : G_{16} contient une substitution V qui remplace x' par x; $V^{-1} UV = W$ ne déplace encore que cinq racines, et laissant x immobile, appartient à G_{15}. Mais toute substitution qui déplace les systèmes déplace au moins deux d'entre eux, soit six racines : donc W appartient à I et remplace les lettres de chaque système les unes par les autres. Mais si W déplace les trois lettres d'un même système, le premier, par exemple, son carré sera une puissance de A_1, qui ne peut être contenue dans I, ainsi qu'on l'a déjà vu. Si, au contraire, W laisse dans chaque système une racine au moins immobile, on pourra supposer

$$W = (a_1 b_1), \quad = (a_1 b_1)(a_2 b_2) \quad \text{ou} \quad = (a_1 b_1)(a_2 c_2).$$

Dans les trois cas, cette substitution, jointe à celles de la forme $A_1^{\alpha_1} \ldots A_5^{\alpha_5}$, que contient I, et à ses transformées par celles-ci, permettra de permuter ensemble d'une manière quelconque les trois racines a_1, b_1, c_1, puis, en laissant celles-là immobiles, de permuter ensemble a_2, b_2, c_2, puis de permuter entre elles a_3, b_3, c_3. Donc P serait égal à $(1.2.3)^3 P_3$, et divisible par 8, ce qui est inadmissible.