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

DE SÉGUIER

Sur les équations de certains groupes

Journal de mathématiques pures et appliquées 5^e série, tome 8 (1902), p. 253-308.
<http://www.numdam.org/item?id=JMPA_1902_5_8__253_0>

Sur les équations de certains groupes;

PAR M. DE SÉGUIER.

L'objet de ce Travail est l'extension de la méthode indiquée par M. Jordan (*Traité des substitutions*, p. 32) pour la recherche des groupes plusieurs fois transitifs, avec des applications aux groupes connus d'ordre $\frac{1}{2}p(p^2-1)$, $p^n(p^n-1)$, $p^n(p^{2n}-1)$. J'ai été ainsi amené à reprendre et à compléter les recherches de Mathieu sur les groupes de degré $q=2p+1$, q et p étant premiers.

J'établirai d'abord certains théorèmes relatifs à la définition des groupes (finis ou non). Ils ont déjà été énoncés (¹); je ne crois pas qu'ils aient été démontrés rigoureusement.

Soit S un système d'équations $F_1=1$, $F_2=1$, ... entre les générateurs a_1, a_2, ... définissant un groupe G. Les F_i pourront contenir des a_i^{-1}. *Chacune de ses conséquences peut, par des transformations identiques* (*c'est-à-dire ne supposant aucune équation autre que* $a_i a_i^{-1}=1$ *entre des produits formellement distincts*), *être mise sous la forme typique* $\Pi_{V,F} V^{-1}FV=1$, F *parcourant un système de* $F_i^{\pm 1}$ *où le même peut revenir plusieurs fois,* V *parcourant, indépendamment de* F, *des produits quelconques de* a_i *et de* a_i^{-1}, *et* V^{-1} *étant écrit de manière que* $V^{-1}V=1$ *identiquement* (il en sera toujours de même pour les autres lettres affectées de l'exposant -1). En effet, S est sous forme typique. Supposons qu'on en ait déduit un

(¹) *Cf.* YOUNG, *A. J.*, t. XV, 1893; HÖLDER, *M. A.*, t. XLIII, 1893.

système de conséquences sous forme typique formant avec S un système S'. La transformation qui ramène une équation à la forme typique étant identique n'altère pas sa valeur logique, et l'on pourra, dans toute déduction, prendre sous forme typique chaque équation dont on se sert. Il suffit donc de montrer que toute conséquence de S' peut être mise sous forme typique. Or on ne peut déduire une conséquence d'un système d'équations que par la répétition de deux opérations : multiplier les deux membres d'une équation par un même facteur, substituer à un produit d'éléments un autre produit égal (identiquement ou non). Le résultat de la multiplication des deux membres de $\Pi V^{-1}FV = 1$ par A s'écrit identiquement $\Pi A^{-1}V^{-1}FVA = 1$ qui a la forme typique. Soient $ABC = 1$, $\Phi = 1$ deux équations de S', la seconde équivalant identiquement à $B = D$. Φ sera de l'une des formes $B^{-1}D$, DB^{-1}, BD^{-1}, $D^{-1}B$. Le résultat de la substitution de D à B s'écrira donc identiquement, ou $ABCC^{-1}B^{-1}DC = 1$, c'est-à-dire $ABC.C^{-1}\Phi^{\pm 1}C = 1$, ou $ADB^{-1}A^{-1}.ABC = 1$, c'est-à-dire $A\Phi^{\pm 1}A^{-1}.ABC = 1$, donc toujours sous forme typique.

Supposons que, dans les équations d'un système S définissant un groupe G, figurent deux séries de générateurs $a_1, a_2, \ldots, b_1, b_2, \ldots$ et désignons d'une manière générale par $X(a_i) = X(a)$, $X(b_i) = X(b)$ des produits des $a^{\pm 1}$ seuls ou des $b^{\pm 1}$ seuls, par $X_{a=1}$, $X_{b=1}$, ce que devient le produit de générateurs X ou le système d'équations X, quand on y remplace les a ou les b par 1. Il est clair que, si $\Phi = 1$ résulte de S, $\Phi_{b=1} = 1$ résultera de $S_{b=1}$ et plus généralement si, dans $\Phi = 1$, on fait quelques-uns des b égaux à 1 ou entre eux, le résultat obtenu résultera du système obtenu en faisant les mêmes changements dans S (il suffit pour le voir de faire les mêmes changements dans toutes les déductions conduisant à $\Phi = 1$). Si donc $\Phi = 1$ ne contient que les a, elle résultera de $S_{b=1}$; mais une conséquence de $S_{b=1}$ ne résulte pas en général de S.

Supposons que $S_{a=1}$ définisse un groupe B; en général, $S_{a=1}$ ne résultant pas de S, les conséquences de $S_{a=1}$ ne le seront pas de S, c'est-à-dire que la table de multiplication de B ne fera pas partie de celle de G et que G ne contiendra pas B. S_a étant le système des équations de S où ne figurent que les $a^{\pm 1}$, supposons encore que S_a définisse un groupe A. Ici, S_a résultant de S, les conséquences de S_a le seront de S;

mais G ne contiendra encore pas nécessairement A, parce que S peut identifier des $\alpha(a)$ laissés distincts par S_a. On observera que les conséquences de S dans A résultant toutes de $S_{b=1}$, G contiendra A si $S_{b=1}$ résulte de S_a. Je me bornerai au cas important où S a la forme

$$A_i(a)=1, \qquad B_j(b)=A'_j(a), \qquad b_k^{-1}a_ib_k=A_i^{b_k}(a)$$
$$(i, j, k, l=1, 2, \ldots).$$

Si $A'_j=1$, G contiendra B, car alors $S_{a=1}$ équivaut au système S_b des $B_j=1$. Si $A'_j=1$, $A_i^{b_k}=a_l$, G contient A. En posant $A_l^{b_k}(A_i^{b_m})=A_l^{b_k b_m}$, et généralement $A_l^{\beta(b)}(A_i^{\gamma(b)})=A_l^{\beta(b)\gamma(b)}$, d'où $A_l^{\beta(b)[\gamma(b)\delta(b)]}=A_l^{[\beta(b)\gamma(b)]\delta(b)}$, on aura

$$\beta(b)^{-1}a_i\beta(b)=A_i^{\beta(b)}, \qquad \beta(b)^{-1}\alpha(a)\beta(b)=\alpha(A_i^{\beta(b)}).$$

On pourra donc, en faisant passer les b à droite et les a à gauche, ou inversement, ramener tout élément de G à la forme $\alpha(a)\beta(b)$ ou $\beta(b)\alpha(a)$. Je dis qu'on aura chaque élément de G au moins une fois dans la forme $\alpha\beta$ (ou $\beta\alpha$) en faisant parcourir à α les éléments distincts de A et à β les *éléments distincts de* B (c'est-à-dire les produits que $S_{a=1}$ laisse distincts). En effet, tout $\beta(b)$ est égal dans B (c'est-à-dire en vertu de $S_{a=1}$) à un élément β_B de B, les diverses écritures qui représentent β_B dans B représentant en général plusieurs éléments de G. Dans la forme typique $\Pi V^{-1}B_j^{\pm 1}V=1$ de $\beta\beta_B^{-1}=1$, remplaçons B_j par $B_jA_j^{-1}$; l'égalité subsistera en vertu de $B_j=A'_j$. En faisant passer tous les b à gauche, on voit que $\Pi V^{-1}B_j^{\pm 1}V$, donc $\beta\beta_B^{-1}$ sera un $\alpha(a)$; donc $\beta=\alpha\beta_B$. α dépendra en général de l'écriture choisie pour β_B dans B. Mais le système des éléments distincts de $A\beta_B$ n'en dépendra pas et coïncidera avec le système des éléments distincts de $A\beta$. Ainsi β_B parcourant B avec une écriture quelconque, $\Sigma A\beta_B$ (et de même $\Sigma\beta_B A$) fournira au moins une fois chaque élément de G. Si $\beta_B\neq\beta'_B$ dans B, $A\beta_B$ et $A\beta'_B$ n'ont aucun élément commun, car de $\alpha\beta_B=\alpha'\beta'_B$ on déduirait, en remplaçant les a par 1, que $\beta_B=\beta'_B$ dans B. Donc, si un élément $\alpha\beta_B$ est répété, ce sera dans le système $A\beta_B$ où il se trouve, c'est-à-dire sous la forme $\alpha'\beta_B$, α et α' étant distincts *dans* A, c'est-à-dire en vertu de S_a, mais égaux *dans* G,

c'est-à-dire en vertu de S. Cela n'aura lieu que si S établit entre les a d'autres conséquences que S_a, c'est-à-dire si G ne contient pas A. En adjoignant à S_a toutes les conséquences que S établit entre les a, S et G ne changent pas; mais S_a deviendra un système S'_a définissant un groupe A' contenu dans G et dans A. Alors, α' parcourant A', on aura, *sans répétition d'éléments*, $G = A'B = BA'$.

Pour que S n'établisse pas entre les a d'autres relations que S_a, deux conditions sont évidemment nécessaires (¹).

1° Comme S donne $A_i(a_l) = A_i(b_k^{-1} a_l b_k) = 1$, il faut que, *dans* A, $A_i(A_l^{b_k}) = 1$ et que les $A_l^{b_k}$ (b_k restant fixe) ne vérifient dans A aucune relation $\Phi(A_l^{b_k}) = 1$ qui ne résulte des $A_i(A_l^{b_k}) = 1$; sans quoi S donnant $b_k^{-1}\Phi(a_l)b_k = \Phi(A_l^{b_k})$ donnerait $\Phi(a) = 1$, qui ne résulte pas de S_a. Cette condition sera dite *d'isomorphisme*. On observera que, $A_i(A_l^{b_k}) = 1$ résultant des $A_i(a) = 1$, $A_i(A_l^{b_k b_m})$ résultera de $A_i(A_l^{b_k}) = 1$, c'est-à-dire de $A_i(a) = 1$, et plus généralement que $A_i(A_l^{\beta(b)}) = 1$ résultera de S_a.

2° Il faut que, *dans* A, $A_j'^{\pm 1} a_l A_j'^{\pm 1} = A_l^{B_j^{\pm 1}}$; si G est fini, l'équation répondant aux signes inférieurs résulte de l'autre, comme on le voit en répétant la transformation par A'_j. Cette condition sera dite *de fermeture*. Si les A'_j se réduisent à 1, ces deux conditions suffisent pour que toute conséquence de S entre les a résulte du système S' des seules équations $A_i = 1$, $b_k^{-1} a_l b_k = A_l^{b_k}$. En effet, S' donne $b_k^{-1} A_j'^{-1} b_k a_l b_k^{-1} A'_j b_k = A_l^{b_k^{-1} B_j b_k}$. Donc ici, *en vertu de* S', $b_k^{-1} B_j b_k$ et, de même, tout $\beta^{-1} B_j \beta = \mathfrak{v}$ est permutable à a_l, donc à $b_i^{-1} a_l b_i$ (car $b_i^{-1} a_l b_i \mathfrak{v} = b_i^{-1} a_l b_i \mathfrak{v} b_i^{-1} b_i = b_i^{-1} b_i \mathfrak{v} b_i^{-1} a_l b_i = \mathfrak{v} b_i^{-1} a_l b_i$). Donc, dans une conséquence $\Phi = \Pi V_F F^{\pm 1} V_F = 1$ de S (F parcourant les premiers membres des équations de S ramenées à la forme typique), $V_F F^{\pm 1} V_F$ se ramène à la forme $\alpha^{-1} A_i (A_l^{\beta})^{\pm 1} \alpha$, si $F = A_i$, et à la forme $\alpha^{-1} \beta^{-1} B_j^{\pm 1} \beta \alpha$, si $F = B_j$. En faisant passer à gauche tous les $\beta^{-1} B_j^{\pm 1} \beta$, on voit que $\Phi = 1$ prend, *en vertu de* S', la forme $\mathfrak{v}\Phi' = 1$, $\mathfrak{v}$, Φ' étant les premiers membres de deux conséquences de $S_{a=1}$, S' respectivement. Or $\mathfrak{v}$, si l'on y intercale des $b_k^{-1} b_k$ à des places convenables, présente tous les b de Φ dans l'ordre où ils s'y rencontrent.

(¹) M. Hölder (*loc. cit.*) semble affirmer qu'elles sont suffisantes. C'est sur ce point que sa démonstration (en particulier le § 16) m'a laissé quelques doutes.

Ils se détruisent identiquement si $\Phi = 1$ ne lie que les a, et alors $\Phi = 1$, qui équivaut *en vertu de* S' à une conséquence $\Phi' = 1$ *de* S', résulte de S'. Si B est cyclique, S donne $b_1^{-1} A'_1 b_1 = A'_1$, donc $A'_1 (A'^{q}_1) = A'_1$ doit résulter de S_a. J'appellerai cette nouvelle condition *condition de permutabilité*. Si elle est vérifiée ainsi que les deux autres, toute conséquence $\Phi = 1$ (sous forme typique) de S entre les a résulte encore de S'. En effet, d'après les hypothèses, $F_1 = B_1 A_1^{-1}$ sera, *en vertu de* S', permutable aux a et à b_1. On pourra donc, dans Φ, faire passer à gauche d'abord tous les F_i qui y formeront un produit F_1^k, puis, A'_{1j} étant permutable à b_1, tous les B_j qui y formeront un produit $\mathfrak{B}$. Comme plus haut, on devra avoir $k = 0$. Donc F_1 disparaît en vertu de S' et $\Phi = 1$ résulte de S'.

Or, toutes les fois que S n'établit pas entre les a d'autres conséquences que S', les conditions d'isomorphisme et de fermeture suffisent pour que G contienne A. En effet, en appelant b'_k la substitution $(a_l, A'^{b_k}_l)$, a'_h la substitution $(a_l, a_l a_h)$, le groupe engendré par les a', b' (les b' ne sont pas nécessairement tous distincts) vérifie S' et contient le groupe $A' \equiv A$ (1) engendré par les a'_h. Quand les $A'_j = 1$, la condition de fermeture exprime évidemment que les isomorphismes $(a_l, A'^{b_k}_l)$ engendrent un groupe homomorphe à B.

1. Soient G un groupe de champ (j'entends par là l'ensemble des symboles) $1, 2, \ldots, n$; A le diviseur fixant 1, B un diviseur quelconque. *Si dans les deux éléments* $x_\alpha = (1\,\alpha \ldots)$, $x_\beta = (1\,\beta \ldots)$ *de* $G(\alpha, \beta \geq 1)$, α *et* β *appartiennent à un même système d'intransitivité de* B, *on a*

$$x_\alpha \equiv x_\beta \qquad (\mathrm{mod\,d}\, A, B).$$

Car $b = (\alpha\beta \ldots)$ étant dans B, $x_\alpha b x_\beta^{-1} = (1) \ldots$ est dans A, donc x_α dans $A x_\beta B$. *Réciproquement les éléments de* AxB *substituent évidemment à* 1 *les symboles d'un même système d'intransitivité de* B, système qui peut être choisi arbitrairement si G est transitif. Donc,

(1) Je représente par cette notation l'isomorphisme holoédrique. Je dirai d'ailleurs désormais, avec M. Klein, *homomorphe* pour *isomorphe*, et *isomorphe* pour *holoédriquement isomorphe*.

si G *est transitif,* (G; A, B) (¹) *est le nombre des systèmes d'intransitivité de* G *dans la représentation de* G *relative à* A (*chaque symbole non déplacé par* B *étant ainsi compté comme système d'intransitivité*).

Tout groupe $A = \Sigma a_\lambda$ de substitutions entre les symboles $1, \ldots, n$, $\tau(\geq 0)$ fois transitif divise d'autres groupes de substitutions, par exemple les symétriques dont le champ contient $1, \ldots, n$. Mais on peut se proposer de chercher s'il existe un groupe G_t, $t + \tau$ fois transitif entre les symboles $1, \ldots, n, \sigma_1, \ldots, \sigma_t$, où A soit le diviseur fixant $\sigma_1, \ldots, \sigma_t$. Soit d'abord $t = 1$, $G_1 = G$, $\sigma_1 = \sigma$. Si G existe, on aura la décomposition (modd A, A) $G = AXA$, $X = \Sigma_1^m x_i (x_1 = 1)$, chaque $x_i \neq 1$ substituant à σ un élément α_i d'un système d'intransitivité distinct de A, m étant le nombre de ces systèmes d'intransitivité (dans le champ effectif de G : l'un d'eux se réduit à σ) qui se réunissent avec σ en un seul système d'intransitivité de C, et $(AXA)^2 = AXA$ ou $XAX = AXA$. Il suffit évidemment qu'on puisse trouver des x_i vérifiant ces conditions, et, si G est primitif, donc A maximum dans G, on aura $G = (A, x_i)$.

La recherche de X par tâtonnement est abordable lorsque l'on sait *a priori* que G doit contenir des substitutions du second ordre $(\sigma\alpha_i), \ldots$, qu'on pourra prendre pour x_i. Bornons-nous à ce cas, et soit $F_i = \Sigma_1^{(F_i, 1)} f_{i\mu}$, de générateurs $f_{ik}^0 (k = 1, \ldots, N)$, le diviseur de $A = \Sigma_i^{(A, F_i)} F_i r_{i\nu} (r_{i1} = 1)$ qui fixe α_i; on aura

$$x_i F_i x_i = F_i.$$

Les conditions d'existence de G deviennent

$$(1) \quad x_i^2 = 1, \quad x_i f_{ik}^0 x_i = f_{i\mu'}, \quad x_i r_{i\nu} x_i = a_{\nu'} x_i a_{\nu''}, \quad x_i a_\lambda x_j = a_{\lambda'} x_k a_{\lambda''},$$

μ' dépendant de i, k; ν', ν'', i' de i, ν; λ', λ'', k de i, j, λ; $i = 2, \ldots, m$; $k = 1, \ldots, N$; $\nu = 1, \ldots, (A, F_i)$; $\lambda = 1, \ldots, (A, 1)$; et l'on peut mettre $a_{\lambda'} x_k a_{\lambda''}$ sous la forme $r_{k\beta}^{-1} x_k r_{k\gamma}^{-1} f_{k\delta}$. Si A est transitif, $i' = i$.

(¹) Je désignerai par (G, A) l'indice de A dans G, par (G; A, B) le nombre des éléments incongrus de G (modd A, B) (cf. Frobenius, *Crelle*, t. **101**).

Le groupe G′ *défini par le système* S, *formé de ces équations et de celles de* A, *est précisément* G (certaines équations de S peuvent d'ailleurs résulter des autres).

En effet, désignons un instant par G, A les groupes abstraits représentés jusqu'ici par les groupes de substitutions G, A. Les équations (1) donnent $G' = AXA$, donc $(G', 1) \leqq (G, 1)$. Mais, comme G les vérifie, on a aussi $(G', 1) \geqq (G, 1)$, donc $G' \equiv G$. Ainsi S exprime toutes les relations qui existent entre les substitutions génératrices de A et les x_i; autrement dit, toute relation que l'on peut obtenir en formant avec ces substitutions des produits égaux à 1 résulte de S, sans quoi ces substitutions engendreraient un groupe d'ordre $< (G, 1)$.

Si A est transitif, donc $\tau \geqq 1$, $m = 2$, G étant au moins deux fois transitif sera d'ordre pair et contiendra une s_2 (1) s; une conjuguée de s déplacera σ et pourra être prise pour x_2.

Soit $t > 1$ et A transitif. *Les conditions nécessaires et suffisantes pour l'existence d'un groupe* G_t, $t+1$ *fois transitif entre les symboles* $1, \ldots, n, \sigma_1, \ldots, \sigma_t$, *où* A *est le groupe fixant* $\sigma_1, \ldots, \sigma_t$, F *le groupe fixant* $1, \sigma_1, \ldots, \sigma_t$, *sont qu'il existe des substitutions d'ordre* 2, $s_h = (\sigma_{h-1}, \sigma_h)$, $\ldots$ ($\sigma_0 = 1$ *et les symboles non écrits faisant partie de* $2, \ldots, n$) *telles que*

$$(2)\quad \left\{\begin{array}{c} s_h^2 = 1, \qquad s_h f s_h = f_h, \qquad s_1 r s_1 = a' s_1 a'', \\ s_l a s_l = a_l, \qquad (s_i s_{i+1})^3 = f_{i1}, \qquad (s_j s_{j+k})^2 = f_{jk} \\ (h = 1, \ldots, t;\ i = 1, \ldots, t-1;\ j = 1, \ldots, t-2;\ k = 2, \ldots, \\ t-j;\ l = 2, \ldots, t;\ f \text{ parcourt les générateurs de F, } a \text{ ceux} \\ \text{de A qui sont hors de F; } r \text{ un système de restes} \not\equiv 1 \text{ de} \\ \text{A mod F; } a', a'', a_l \text{ sont dans A hors de F; } f_{i1}, f_{jk} \text{ dans F}), \end{array}\right.$$

(1) J'écrirai, d'une manière générale, g^n pour « groupe de degré n », s^n pour « substitution de degré n », en entendant par *degré* d'une substitution le nombre des symboles qu'elle déplace, g_n pour « groupe d'ordre n », s_n pour « substitution d'ordre n ». J'appellerai *pair* un groupe dont toutes les substitutions sont paires. J'appellerai *constituant* d'un groupe intransitif le groupe auquel il se réduit lorsqu'on ne considère que son action sur certains systèmes d'intransitivité.

et ces équations, jointes à celles de A, *définissent* G_t. Il suffit de montrer que le théorème subsiste lorsqu'on remplace t par $t+1$ [la première ligne de (2) se confond avec (1) pour $t=1$, $m=2$]. Or, si G_{t+1} existe, il y a, on l'a vu, une substitution de la forme

$$s_{t+1} = (1)(\sigma_1)\ldots(\sigma_{t-1})(\sigma_t\sigma_{t+1})\ldots,$$

telle que

$$s_{t+1}^2 = 1, \qquad s_{t+1}G_{t-1}s_{t+1} = G_{t-1}, \qquad s_{t+1}G_{t-1}s_tG_{t-1}s_{t+1} \leqq G_t s_{t+1} G_t$$

(les restes $\not\equiv 1$, $\bmod G_{t-1}$ de $G_t = G_{t-1} + G_{t-1}s_tG_{t-1}$ sont tous dans $G_{t-1}s_tG_{t-1}$) et ces équations développées définissent G_{t+1}. Puisque s_{t+1} fixe $1, \sigma_1, \ldots, \sigma_{t-1}$, il résulte de $s_{t+1}G_{t-1}s_{t+1} = G_{t-1}$ que $s_{t+1}Fs_{t+1} = F$, $s_{t+1}As_{t+1} = A$, et $(s_ts_{t+1})^3$, $(s_js_{t+1})^2 (j<t)$ sont évidemment dans F. Inversement, si (2) est vérifié quand on y remplace t par $t+1$, on aura, puisque $G_h = \{A, s_1, \ldots, s_h\}$,

$$s_{t+1}G_{t-1}s_{t+1} = G_{t-1};$$

et l'équation $(s_ts_{t+1})^3 = f_{t1}$ donne

$$s_{t-1}G_{t-1}s_tG_{t-1}s_{t+1} = G_{t-1}s_{t+1}s_ts_{t+1}G_{t-1} = G_{t-1}s_ts_{t+1}s_tG_{t-1} \leqq G_t s_{t+1} G_t.$$

Comme $G_1 = A + As_1A$, on aura ($s_2As_2 = A$) :

$$\begin{aligned} G_2 &= G_1 + G_1s_2G_1 \\ &= A + As_2 + As_1A + As_1s_2A + As_2s_1A + As_1s_2As_1A. \end{aligned}$$

Chaque complexe du second membre où A figure ρ fois contiendra, α désignant l'ordre de A, α^ρ éléments distincts ne figurant dans aucun autre complexe, car $\Sigma_\rho \alpha^\rho = \alpha(\alpha+1)(\alpha+2)$ est précisément l'ordre de G_2.

En observant que $s_1As_1 \leqq As_1A$, donc que $s_1As_1.A$ est $\leqq As_1A$ et $As_1A.s_1A \geqq s_1A$, en sorte que

$$As_1s_2As_1A = As_2s_1As_1A = As_2.As.As_1A$$

coïncide avec As_3s_1A, on a de même

$$\begin{aligned}G_3 = {} & A + As_2 + As_3 + As_2s_3 + As_3s_2 + As_2s_3s_2 + As_1A + As_1s_2A \\ & + As_2s_1A + As_1s_3A + As_1s_2s_3A + As_3s_2s_1A + As_1s_3s_2A \\ & + As_3s_2s_1A + As_1s_2s_3s_2A + As_2s_3s_1s_2A + As_2s_3s_2s_1A \\ & + As_1s_2As_1A + As_1s_3As_1A + As_1s_2s_3As_1A + As_1s_3s_2As_1A \\ & + As_1s_2s_3As_1s_2A + As_1s_2s_3s_2As_1A + As_2s_3s_1s_2As_1A \\ & + As_1s_2s_3As_1s_2As_1A,\end{aligned}$$

aucun élément n'étant répété dans le second membre.

En prenant $A = 1$, $\sigma_{h-1} = h$, $s_h = (h, h+1)$, on obtient immédiatement, pour les équations du symétrique de champ $1, 2, \ldots, t$,

$$(3)\quad \begin{cases} s_h^2 = (s_i s_{i+1})^3 = (s_j s_{j+k})^2 = 1, \\ (h = 1, \ldots, t-1;\ \ i = 1, \ldots, t-2;\ \ j = 1, \ldots, t-3;\ \ k = 2, \ldots, t-j-1). \end{cases}$$

Ces équations exprimant toutes les relations qui lient les $(h, h+1)$, il en résulte certainement, puisque

$$(12)(23)\ldots(t-1, t) = (1, 2, \ldots, t),$$

en posant $s_1 = a$, $s_1 \ldots s_{t-1} = b$, que

$$b^t = 1, \qquad s_h = b^{t-h} a b^{h-1},$$

donc aussi

$$(4)\quad \begin{cases} b^t = a^2 = (ab^{-1}ab)^3 = (ab^{-j}ab^j)^2 = 1; \\ j = 2, 3, \ldots, \frac{t}{2}, \text{ si } t \text{ est pair};\ \ j = 2, 3, \ldots, \frac{t-1}{2}, \text{ si } t \text{ est impair}. \end{cases}$$

Inversement de (4) on déduit (3) en observant que

$$b^{-h}.ab^{-h}ab^h.b^h = b^{-h}ab^h.b^{-h-k}ab^{h+k},$$

$$ab^j.ab^{-j}ab^j.b^{-j}a = ab^jab^{-j}$$

et en posant

$$b^{t-h}ab^{h-1} = s_h.$$

Donc (4) définit le symétrique de degré t (*Comparer* Moore, *P. L. M. S.*, t. XXVIII, 1896, p. 357).

Prenons pour A l'alterné de champ 1, 2, 3 engendré par

$$c = (123) = (12)(13).$$

En adjoignant les substitutions

$$s_i = (12)(i+2, i+3) \qquad (i = 1, \ldots, n-3;\ n \geq 4)$$

qui vérifient

$$(5)\quad \begin{cases} c^3 = (cs_i)^3 = (cs_l)^2 = s_i^2 = (s_j s_{j+1})^3 = (s_i s_{i+k})^2 = 1, \\ i = 1, \ldots, n-3; \qquad j = 1, \ldots, n-4; \\ k = 2, \ldots, n-i-3; \qquad l = 2, \ldots, n-3 \end{cases}$$

(on supprimera les équations où s aurait un indice > 1 si $n = 4$, ou > 2 si $n = 5$), on a un g'' $n-2$ fois transitif. C'est donc l'alterné $\mathfrak{A}_n$ de degré n, et $\mathfrak{A}_n$ est défini par (1). $\mathfrak{A}_n$ contient une substitution $b = s_{n-3} s_{n-4} \ldots s_2 s_1$ de la forme $(34 \ldots n)$ ou $(12)(34 \ldots n)$, selon que n est impair ou pair et $b^{-i} s_1 b^i = s_{i+1}$, $i = 1, \ldots, n-4$. Donc les équations suivantes (où a est mis pour s_1 et où n est supposé > 5)

$$(6)\quad \begin{cases} b^{n-2} = c^3 = a^2 = (ac)^3 = (ab^{-1}ab)^3 = (ab^{-x}ab^x)^2 = (cb^{-y}ab^y)^2 = 1, \\ x = 2, \ldots, \tfrac{1}{2}(n-2) \quad \text{si } n \text{ est pair}, \\ x = 2, \ldots, \tfrac{1}{2}(n-3) \quad \text{si } n \text{ est impair}, \\ y = 2, \ldots, n-3 \end{cases}$$

résultent de (5), qui exprime toutes les relations liant les

$$(12)(i+2, i+3) \qquad (i = 0, \ldots, n-3).$$

Inversement de (6) on déduit (5), en observant que

$$b^{-h}.ab^{-k}ab^k.b^h = b^{-h}ab^h.b^{-h-k}ab^{h-k}, \qquad ab^x.ab^{-x}ab^x.b^{-x}a = ab^x ab^{-x}$$

(*cf.* Moore, *loc. cit.*).

2. Prenons $A = |(z, iz)|$, z parcourant un corps de Galois $C(p^m)$ d'ordre p^m (p premier) dont i est racine primitive. A fixe le symbole o. Une détermination de G_1 sera le groupe $G = \Sigma(z, \alpha z + \beta)$, β parcourant C, et α C sauf o. C'est d'ailleurs la seule. En effet, dans un $g_{p^m(p^m-1)}G'$ deux fois transitif, de classe $p^m - 1$, il y a $p^{m-1}s_p^{p^m}$ formant avec l'unité un groupe normal H dont tous les éléments sont d'ordre p et conjugués dans G', donc permutables. Donc tout diviseur A' de G', qui fixe un symbole, divise le groupe J des isomorphismes de H. Or les éléments de H peuvent se mettre sous la forme $h = |x_i, x_i + a_i|$ $(i = 1, \ldots, m)$, x_i, a_i parcourant les entiers réels mod p, et celles de s sous la forme

$$j = |x_i, \Sigma_k \alpha_{ik} x_k| \pmod p \qquad (i, k = 1, \ldots, m).$$

Soit A' cyclique. Pour que j soit un générateur de A', donc d'ordre $p^m - 1$, il faut et il suffit que sa congruence caractéristique soit irréductible et appartienne à l'exposant $p^m - 1$ (Jordan, *Traité*, n° 159). Un changement de variables ramène alors j à la forme

$$|X_i, \rho_i X_i| \qquad (i = 0, \ldots, m-1, \ \rho_i = \rho^{p^i})$$

et h a la forme $|X_i, X_i + A_i|$. Les X_i étant conjugués, G' est isomorphe au groupe engendré par $|X_0, \rho X_0|$ et par les $|X_0, X_0 + A_0|$. Or $X_0 = \Sigma_0^{m-1} \rho^i y_i$, $A_0 = \Sigma_0^{m-1} \rho^i b_i$, les y étant des fonctions linéaires indépendantes des x et les b des a (puisque les X sont indépendants et de même les A). Donc $G' = A'H \equiv \Sigma(z, \alpha z + \beta) \equiv G$.

Cherchons les équations de G par la méthode précédente. On aura $G = |a, b|$, $a = (iz)$, $b = (01)\ldots$ étant du second ordre et de la forme $(\alpha z + \beta)$; donc $b = (1 - z)$, et G sera défini par les équations

$$a^{p^m-1} = b^2 = 1, \qquad ba^\xi b = a^\eta b a^\zeta,$$

où $\xi = 1, \ldots, p^m - 2$ et où η, ζ sont à déterminer en fonction de ξ.

Or on a

$$ba^\xi b = (i^\xi z + 1 - i^\xi) = (i^{-\xi}(i^\xi - 1), 0, 1 - i^\xi, \ldots),$$

donc

$$a^{\eta} = (i^{-\xi}(i^{\xi} - 1), 1, \ldots), \qquad a^{\zeta} = (1, 1 - i^{\zeta}, \ldots);$$

d'où les deux conditions

$$i^{\eta - \xi}(i^{\xi} - 1) \equiv 1 \pmod{p}, \qquad i^{\zeta} \equiv 1 - i^{\zeta},$$

la dernière déterminant ζ et montrant que, pour $\xi < m$, ζ est $\geq m$, la première donnant ensuite

$$\eta + \zeta - \xi \equiv \begin{cases} \frac{1}{2}(p^m - 1) & \text{si } p > 2 \\ 0 & \text{si } p = 2 \end{cases} \pmod{p^m - 1}.$$

Certaines des équations ainsi obtenues pour G pourront résulter des autres et être supprimées : de $ba^{\xi}b = a^{\eta}ba^{\zeta}$, $b^2 = 1$, par exemple, on déduit $ba^{-\xi}b = a^{-\zeta}ba^{-\eta}$, $ba^{\eta}b = a^{\xi}ba^{\zeta}$, $ba^{-\eta}b = a^{\zeta}ba^{-\xi}$, $ba^{\zeta}b = a^{-\eta}ba^{\xi}$, $ba^{-\zeta}b = a^{-\xi}ba^{\eta}$, et, si $p = 2$, on a

$$ba^{2\xi}b = a^{\eta}ba^{\eta+\zeta}ba^{\zeta} = a^{\eta}ba^{\xi}ba^{\zeta} = a^{2\eta}ba^{2\zeta},$$

d'où, par récurrence,

$$ba^{2^{\lambda}\xi}b = a^{2^{\lambda}\eta}ba^{2^{\lambda}\zeta}.$$

On obtient plus facilement un autre système d'équations comme il suit. Si l'on pose

$$(z + i^{\nu}) = c_{\nu} = a^{-\nu}c_0a^{\nu}, \qquad c_0 = c,$$

il est clair que tout élément de G est contenu une fois, et une fois seulement, dans la forme

$$a^x c_0^{\nu_0} \ldots c_{m-1}^{\nu_{m-1}} \qquad (x = 0, \ldots, p^m - 2;\ \nu_0, \ldots, \nu_{m-1} = 0, \ldots, p - 1).$$

Si $i^m = \Sigma_0^{m-1} \alpha_s i^s$, les α_s étant réels, a, c_0, $\ldots$, c_{m-1} vérifieront les équations

$$a^{p^m - 1} = c_{\rho}^{p} = 1, \qquad c_{\rho}c_{\sigma} = c_{\sigma}c_{\rho}, \qquad \rho, \sigma = 0, 1, \ldots, m - 1;$$

$$a^{-1}c_{\tau}a = c_{\tau+1}, \qquad \tau = 0, \ldots, m - 2; \qquad a^{-1}c_{m-1}a = c_0^{\alpha_0} \ldots c_{m-1}^{\alpha_{m-1}};$$

d'où $c_0, \ldots, c_{m-1}$ s'éliminent immédiatement. Or ces équations définissent un $g_{p^m(p^m-1)}$. Donc les *substitutions* $a, c_0, \ldots, c_{m-1}$ ne vérifient aucune équation qui ne résulte des précédentes.

Soient $p = 3$, $m = 2$. Les deux polynomes irréductibles appartenant à l'exposant 4 sont $z^2 \pm z - 1$. Soit $i^2 \equiv 1 - i$. Pour $\xi = 1$, $\zeta = 2$, $\eta = 3$, et des équations

$$a^8 = b^2 = 1, \qquad bab = a^3 ba^2,$$

on déduit des équations analogues pour $\xi = \pm 1, \pm 2, \pm 3$, en particulier $ba^2 b = aba^6$, dont le produit avec $bab = a^3 ba^2$ donne $ba^4 b = a^4 ba^4$. Il est donc inutile de faire $\xi = 4$ et le groupe est défini par trois équations. En prenant $i^2 \equiv 1 + i$, on aurait eu $bab = a^2 ba^3$, ce qui revient à changer a en a^{-1}. En écrivant $1, 2, \ldots, 9$ pour $1, i, i^2, \ldots, i^7, 0$, on a

$$a = 12345678, \qquad b = 19.23.47.68.$$

Pour $p = 2$, on a ce théorème (W. Burnside, *M. M.*, 1896, p. 187) que *les équations*

$$a^{\lambda} = b^2 = 1, \qquad bab = a^{1-m} ba^m$$

définissent un groupe d'ordre $2^{m'}\lambda (m' \leq m)$ *contenant un diviseur normal abélien d'ordre* $2^{m'}$ *dont tous les éléments* $\neq 1$ *sont d'ordre* 2. En effet, posons

$$a^{-i} ba^i = b_i \qquad (b_0 = b).$$

On aura $b_i b_{i+1} = b_{m+i}$ pour $i = 0$; cela résulte de la troisième équation, qui s'écrit

$$ba^{-1} b = a^{-m} ba^{m-1} \qquad \text{ou} \qquad ba^{-1} ba = a^{-m} ba^m,$$

et, si cela est vrai pour $i \leq j$, de $b_j b_{j+1} = b_{m+j}$ on déduit

$$a^{-1} b_j b_{j+1} a = a^{-1} b_{m+j} a \qquad \text{ou} \qquad b_{j+1} b_{j+2} = b_{m+j+1}.$$

En outre

$$\begin{aligned} b_i b_{i+k} &= b_i b_{i+1} . b_{i+1} b_{i+2} \ldots b_{i+k-1} b_{i+k} = b_{m+i} b_{m+i+1} \ldots b_{m+i+k-1} \\ &= a^{-m} b_i a^m . a^{-m-1} b_i a^{m+1} \ldots \quad = a^{-m} b_i b_{i+1} \ldots b_{i+k-1} a^m. \end{aligned}$$

Supposons alors prouvé que $\{b, b_1, \ldots, b_j\} = B_j$ est abélien et a tous ses éléments d'ordre 1 ou 2. Il en sera de même de B_{j+1}; car, pour $i \leq j$, $b_i b_{j+1} = a^{-m} b_i b_{i+1} \ldots b_j a^m$ et $b_i b_{j+1}$ est d'ordre 1 ou 2; donc, ou bien $b_{j+1} = b_i$, ou bien $b_i b_{j+1} = b_{j+1} b_i$. Enfin $b_m, \ldots, b_\lambda$ sont dans B_{m-1}, car $b_{(k+1)m+i} = b_{km+i} b_{km+i+1}$ (pour $i = m-1$, le second membre contient $b_{(k+1)m}$ qu'on réduit par la même formule où $i = 0$); $b, b_1, \ldots, b_{m-1}$ pouvant n'être pas indépendants, B_{m-1} est d'ordre $2^{m'}$, $m' \leq m$.

En revenant donc aux notations précédentes, si à $\xi = 1$ répond $\zeta = m$, donc $\eta = 1 - m$, les équations $a^{2^m-1} = b^2 = 1$, $bab = a^{1-m} b a^m$ définissent un groupe G′ d'ordre $\leq 2^m(2^m - 1)$. D'ailleurs, G′ est $\geq$ G, dont les équations comprennent celles de G′. Donc G′ = G.

Pour $p = 2$, $m = 3, 4, 6, 7$, il est facile de vérifier que i défini par $i^m \equiv 1 + i \pmod 2$ est racine primitive. Pour $m = 6$, par exemple, on aura

$$i^8 \equiv i^2 + i^3, \qquad i^{10} \equiv i^3 + i^5,$$
$$i^{60} \equiv (1+i)^{10} \equiv 1 + i^2 + i^8 + i^{10} \equiv 1 + i^3 + i^4 + i^5,$$
$$i^{61} \equiv 1 + i^4 + i^5, \qquad i^{62} \equiv 1 + i^5, \qquad i^{63} \equiv 1,$$

et i^7, i^9, i^{11} sont $\not\equiv 1$. Pour $m = 7$, on aura

$$i^8 \equiv i + i^2, \qquad i^9 \equiv i^2 + i^3,$$
$$i^{63} \equiv (1+i)^9 \equiv 1 + i + i^8 + i^9 \equiv 1 + i^3,$$
$$i^{126} \equiv (1 + i^3)^2 \equiv 1 + i^6, \qquad i^{127} \equiv 1,$$

et 127 est premier. Pour $m = 5$, i défini par $i^5 \equiv i + 1$ donne $i^{31} \not\equiv 1$ [aussi bien $z^5 + z + 1 \equiv (z^2 + z + 1)(z^3 + z^2 + 1)$ n'est pas irréductible]. Mais, en formant successivement les polynomes réductibles de degré 1, 2, 3, 4, 5, on trouve que les irréductibles sont

$$z + 1, \quad z^2 + z + 1, \quad z^5 + z^2 + 1, \quad z^3 + z + 1, \quad z^5 + z + 1,$$
$$z^4 + z^3 + 1, \quad z^4 + z^3 + z^2 + z + 1, \quad z^5 + z^4 + z^3 + z^2 + 1,$$
$$z^5 + z^4 + z^3 + z + 1, \quad z^5 + z^4 + z^2 + z + 1, \quad z^5 + z^3 + z^2 + z + 1,$$
$$z^5 + z^3 + 1, \quad z^5 + z^2 + 1.$$

Soit $i^5 \equiv i^2 + 1$; on aura $i^{18} \equiv i + 1$ et G d'ordre $2^5(2^5 - 1)$ sera défini par $a^{31} = b^2 = 1$, $bab = a^{14} b a^{18}$.

Pour définir le groupe $\mathfrak{L}(2,p)=\mathfrak{L}=\Sigma\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)$ d'ordre $p^m(p^{2m}-1)$ où les paramètres $\alpha, \beta, \gamma, \delta$ parcourent C avec la condition $\alpha\delta-\beta\gamma\not\equiv 0$, z parcourant C et la valeur ∞, il faut ajouter un générateur c représenté par une substitution de $\mathfrak{L}$ de la forme $(0\,\infty)\ldots$ ou $\left(\frac{\beta}{z}\right)$ et vérifiant $c^2=(cb)^3=1$, $cac=a^\tau$, τ étant à déterminer. Or

$$(cb)^3=\left(\frac{z(1-2\beta)+\beta(\beta-1)}{z(1-\beta)-\beta}\right).$$

Donc $\beta=1$, $cac=a^{-1}$ et les équations de $\mathfrak{L}$ s'obtiennent en adjoignant, à celles de G, $c^2=(cb)^3=(ca)^2=1$. On peut d'ailleurs réduire à deux le nombre des générateurs, car les deux équations $ba^\xi b=a^\eta ba^\zeta$, $ca^\eta c=a^{-\eta}$ donnent $ca^\eta cba^\xi b=ba^\zeta$; d'où, en posant $cb=d$, $b=a^{-\xi}d^2a^{-\eta}da^\zeta$, $c=db=da^{-\xi}d^2a^{-\eta}da^\zeta$, $d^3=1$.

Pour $p=2$, $m=3$, $p^m(p^{2m}-1)=504$, $\mathfrak{L}$ est simple et défini par

$$(7)\qquad a^7=b^2=c^2=(ca)^2=(cb)^3=1,\qquad bab=a^{-2}ba^3,$$

ou, en posant $cb=d$ et en remplaçant $(ca)^2=1$ ou $cac=a^{-1}$ par $ca^{-2}c=a^2$, $b^2=1$ par $(a^{-1}ba)^2=1$, $c^2=1$ par $a^{-1}ca=1$, $bab=a^{-2}ba^3$ par $ba^6b=a^4ba^2$ d'où $b=ad^2a^3da^2$,

$$(8)\qquad \begin{cases} a^7=1, \qquad d^3=1, \qquad (d^2a^3da^3)^2=1, \\ (da\,d^2a^3d)^2=1, \qquad (a^6\,da\,d^2a^4\,da^2)^2=1. \end{cases}$$

La troisième et la quatrième donnent

$$d^2a^3da^3=a^4d^2a^4d,\qquad da\,d^2a^3d=d^2a^4da^6d^2.$$

Donc

$$\begin{aligned} a^6\,da.d^2a^3\,da^3=a^6\,da^5d^2a^4d&=a^6\,da^5.d^2a^4\,da^6\,da^5.(a^6\,da^5)^{-1}\\ &=a^6\,da^5.da\,d^2a.(a^6\,da^5)^{-1} \end{aligned}$$

et le système équivaut à

$$(9)\qquad a^7=d^3=(d^2a^3\,da^3)^2=(d^2ad^2a^3)=(da\,d^2a)^2=1.$$

Si l'on pose $a=(iz)$, $b=(1-z)$, $c=(z^{-1})$, ou, en écrivant 1, 2, ..., 9 pour 1, i, i^2, ..., i^6, 0, ∞ respectivement, $a=1234567$, $b=18.24.37.56$, $c=89.27.36.45$, (5) exprime toutes les relations qui lient ces trois substitutions, et (8) toutes celles qui lient a et $d=cb=189.235.467$. Or, en posant

$$bcba=\alpha=\left(\frac{iz}{z-1}\right)=1927635, \qquad aba^6=\beta=(i^6-z)=13.26.45.78,$$

on vérifie les égalités

$$(10)\qquad \alpha^7=\beta^2=(\alpha\beta)^3=(\alpha^3\beta\alpha^5\beta\alpha^3\beta)^2=1,$$

$$(11)\qquad \alpha^3\beta\alpha^5=d, \qquad (\beta\alpha^2\beta d)^2=(\beta\alpha^2\beta\alpha^3\beta\alpha^5)^2=a,$$

en formant les substitutions $\alpha\beta$, $\alpha^3\beta\alpha^5\beta\alpha^3\beta$, ... Inversement (9) ou, ce qui revient au même, (8) résulte de (10). Considérons en effet (11) comme définissant a et d. On aura d'abord $d=\alpha^2.\alpha\beta.\alpha^5$, donc $d^3=1$, puis, en observant que (10) donne $\beta\alpha^6\beta=\alpha\beta\alpha$ (dont le carré et le cube sont $\beta\alpha^5\beta=\alpha\beta\alpha^2\beta\alpha$, $\beta\alpha^4\beta=\alpha\beta\alpha^2\beta\alpha^2\beta\alpha$), $\alpha^3\beta\alpha^5\beta\alpha^3\beta=\beta\alpha^4\beta\alpha^2\beta\alpha^4$,

$$\begin{aligned} a&=\beta\alpha^2.\beta\alpha^3\beta\alpha^5\beta\alpha^2.\beta\alpha^3\beta\alpha^5=\beta\alpha^6\beta.\alpha^2\beta\alpha^4.\beta\alpha^6\beta.\alpha^3\beta\alpha^5\\ &=\alpha.\beta\alpha^3\beta\alpha^5\beta.\alpha^4\beta\alpha^5=\alpha^5\beta\alpha^2\beta\alpha^4.\beta\alpha\beta.\alpha^5,\end{aligned}$$

$$(12)\qquad a=\alpha^4.\alpha\beta\alpha^2\beta\alpha.\alpha^2\beta\alpha^4,$$

$$\alpha^3a\alpha^4=\beta\alpha^4.\alpha\beta\alpha^2\beta\alpha=\beta\alpha^4\beta\alpha^5\beta,$$

$$\beta\alpha^4\beta\alpha^3.a.\alpha^4\beta\alpha^3\beta=\beta\alpha\beta\alpha\beta=\alpha,$$

$$a^x=\alpha^4\beta\alpha^3\beta.\alpha^x.\beta\alpha^4\beta\alpha^3;$$

donc $a^7=1$ et

$$\begin{aligned} a^4&=\alpha^4\beta\alpha^3.\beta\alpha^4\beta\alpha^4\beta\alpha^2.\alpha=\alpha^4.\beta\alpha\beta.\alpha^3\beta\alpha^3\beta\alpha\\ &=\alpha^2.\alpha\beta\alpha^2\beta\alpha.\alpha^2\beta\alpha=\alpha^2\beta\alpha^5\beta\alpha^2\beta\alpha\\ &=\alpha^2\beta\alpha^5.\beta\alpha^2\beta\alpha^3\beta\alpha^5.(\alpha^2\beta\alpha^5)^{-1};\end{aligned}$$

donc $(\beta\alpha^2\beta d)^7=1$, $(\beta\alpha^2\beta d)^8=\beta\alpha^2\beta d$, ou $a^4=\beta\alpha^2\beta d$.

Cela établi, on a

$$d^2a^3\,da^3=d^2a^{-4}\,da^{-4}=d\beta\alpha^5\beta\beta\alpha^5\beta=\alpha^3\beta\alpha^5\beta\alpha^3\beta,$$

qui est du second ordre d'après (10). Ce résultat donne immédiatement, d'après (12),

$$ad^2a^3\,da^3 = \alpha^5\beta\alpha^2.\beta\alpha\beta.\alpha^2\beta = \alpha^5.\beta\alpha\beta.\alpha^2\beta$$
$$= \alpha^1.\beta\alpha\beta = \alpha^3\beta\alpha^6 = d\alpha.$$

Donc

$$da\,d^2a^3d = a^3(a^1d.ad^2a^3\,da^3)a^1 = a^3(a^1d^2\alpha)a^1,$$

et, puisque $a^1 = \beta\alpha^2\beta d$,

$$da\,d^2a^3d = a^3\beta\alpha.\alpha\beta\alpha.a^1 = a^3\beta\alpha.\beta.\alpha^6\beta a^1,$$

qui est du second ordre. Enfin, d'après (12) encore,

$$a^6d.ad^2a^3\,da^3 = \alpha^3\beta\alpha^4\beta\alpha^5\beta\alpha^4\beta\alpha^5,$$
$$\alpha^5.a^6\,da\,d^2a^3\,da.\alpha^2 = \alpha\beta\alpha.\alpha^3\beta\alpha^5\beta\alpha^4\beta = \beta\alpha^6\beta.\alpha^3\beta\alpha^5\beta\alpha^3\beta.\beta\alpha\beta,$$

qui est du second ordre. *Donc* (10) *définit* $\mathfrak{L}$ (*cf.* Burnside, *M. A.*, t. LII; Fricke, *ibid.*, 1899).

3. Cherchons encore les équations d'un groupe $\mathfrak{G}$ deux fois transitif de degré $p+1$ (p premier >2) et d'ordre $\frac{1}{2}p(p^2-1)$. Le groupe G_2 fixant un symbole est d'ordre $\frac{1}{2}p(p-1)$, contient un seul diviseur d'ordre p et divise le groupe métacyclique; donc G_2 est semi-métacyclique. De plus G_2 ne contient aucun diviseur normal dans $\mathfrak{G}$. Donc $\mathfrak{G}$ contient $p+1$ diviseurs d'ordre p. *On va voir que, sauf si* $p=7$, $\mathfrak{G}$ *est nécessairement le groupe* $\mathfrak{v}_1(2,p)=\mathfrak{v}$, *formé des substitutions de* $\mathfrak{L}(2,p)$ *où* $\alpha\delta-\beta\gamma$ *est un carré. Si* $p=7$, $\mathfrak{G}$ *a une seconde forme possible.*

En posant $b=(z+1)$, $a=(i^2z)$, i étant racine primitive de p, G_2 est défini par

$$b^p = a^{\frac{p-1}{2}} = 1, \qquad a^{-1}ba = b^{i^2}$$

(d'où $a^{-x}b^ya^z = b^{y/i^{2x}}$, équation dont l'usage sera constamment sous-entendu dans la suite). Les symboles étant ∞, 0, 1, i, ..., i^{p-1}, on a

$$b=(0,1,2,\ldots,p-1), \qquad a=(i^0,i^2,i^4,\ldots,i^{p-3})(i,i^3,\ldots,i^{p-2});$$

si $p=3$, $a=1$. Cherchons une substitution du second ordre $c=(0\infty)\ldots$ telle que $\mathcal{G}=(G_2, c)$ soit deux fois transitif, G_2 étant le diviseur fixant ∞. Le groupe fixant 0, ∞ étant de classe $p-1$, c sera de degré $\geqq p-1$. Si le degré de c est $p-1$, $\{a\}$, d'ordre $\frac{1}{2}(p-1)$ et de degré $p-1$, doit contenir une substitution d'ordre 2 conjuguée de c; donc $p\equiv 1 \pmod 4$. Si donc $p=3$, $c=0\infty.12=(-z^{-1})$, $\mathcal{G}$ est défini par

$$b^3=c^2=(bc)^3=1$$

et contient normalement le groupe quadratique $\{c, b^{-1}cb\}$; donc $G=\mathfrak{v}$. Supposons désormais $p\geqq 5$. Il faut $cac=a^\alpha$ et $c^2ac^3=a$; donc $\alpha^2=1$.

Soit d'abord $\alpha=1$. — Si c transforme en lui-même chaque cycle de a, on aura, c étant de degré >2,

$$c=(0,\infty)(i^{2x}, i^{2x+2\rho})(i^{2x+1}, i^{2x+2\sigma+1}), \qquad x=0, 1, \ldots, \tfrac{1}{2}(p-3),$$

ρ et σ étant des entiers inconnus $<\frac{1}{2}(p-1)$. Le cycle $(i^{2x+2\rho}, i^{2x+4\rho})$ coïncidant avec $(i^{2x}, i^{2x+2\rho})$, on a $4\rho\equiv 0 \pmod{p-1}$, et, puisque $4\rho<2(p-1)$, $4\rho=p-1$. De même $4\sigma=p-1$ et $p\equiv 1 \pmod 4$, $c=(0,\infty)(z,-z)(z\not\equiv 0)=(0,\infty)a^{\frac{1}{4}(p-1)}$. Donc $\mathcal{G}$ contiendrait $(0,\infty)$ et sa classe serait $<p-1$. Ainsi c échange les deux cycles de a, et l'on aura $c=(0,\infty)(i^{2x}, i^{2x+\rho})$, $x=0, 1, \ldots, \frac{1}{2}(p-3)$, ρ *impair* $<\frac{1}{2}(p-1)$, ou $c=(0,\infty)\left(z, r^{\left(\frac{z}{p}\right)}z\right)(r=i^\rho, z\not\equiv 0)$, $\left(\frac{z}{p}\right)=z^{\frac{p-1}{2}}$ représentant $+1$ si z est carré, sinon -1 : c n'est évidemment pas dans $\mathfrak{v}(2,p)$. Il faut maintenant que $cb^\beta c$ soit, pour $\beta=1, \ldots, p-1$, de la forme $b^x a^y cb^{x'}a^{y'}$, ou, c étant permutable à $\{a\}$ et a à $\{b\}$, de la forme $b^x cb^{x'}a^y$, ou encore, en remplaçant $\{a\}$ par un de ses conjugués dans G_2, $cb^\beta c=b^x cb^{x'}b^{-t}a^y b^t$; et cela suffit. Faisons, en particulier $\beta=1$, $t=r$,

$$cbc=\left(\infty, r, \ldots, kr^{\left(\frac{k}{p}\right)}, (k+1)r^{\left(\frac{k+1}{p}\right)}, \ldots, -r^{\left(\frac{-1}{p}\right)}\right),$$

$b^{-t}a^y b^t$ fixera r et l'on devra avoir

$$x=r\left(\frac{-1}{p}\right), \qquad x'=r, \qquad cbc=b^{r\left(\frac{-1}{p}\right)}ca^y b^r.$$

Pour déterminer y, observons que $b^{r^{\left(\frac{-1}{p}\right)}}$ change $kr^{\left(\frac{k}{p}\right)}$ $(k \neq -1)$ en $kr^{\left(\frac{k}{p}\right)} + r^{\left(\frac{-1}{p}\right)} = u(\neq 0)$, que $c = \left(u, r^{\left(\frac{u}{p}\right)}u\right)$, et que, finalement, on a

$$(1) \quad ur^{\left(\frac{u}{p}\right)}i^{2y} + r = (k+1)r^{\left(\frac{k+1}{p}\right)} \quad \text{si } k > 0, \quad = 0 \quad \text{si } k = 0.$$

De là, pour $k = 0$,

$$\rho\left[\left(\frac{-1}{p}\right) - 2\right] + 2y \equiv \frac{p-1}{2} \pmod{p-1}.$$

Donc $\frac{p-1}{2}$ est impair comme ρ, $\left(\frac{-1}{p}\right) = -1$ (donc $p \geq 7$) et $2y = 3\rho + \frac{p-1}{2}$.

Cela posé, la suite S des termes $\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right)$ présente (JORDAN, *Traité*, p. 158) $\frac{p-1}{2}$ variations de signe exactement, c'est-à-dire $\frac{p-1}{2}$ termes suivis d'un terme de signe contraire et, en particulier, $\frac{1}{4}\left[p - \left(\frac{-1}{p}\right) - 4\right]$ $(\geq 1$ pour $p \geq 7)$ non carrés suivis d'un carré. Soit donc k non carré, $k+1$ carré. On aura $u = (k+1)r^{-1}$, (1) donnera

$$2k \equiv -1 \pmod{p}, \qquad k \equiv \frac{p-1}{2},$$

et comme il y a $\frac{p-1}{2}$ carrés, S présentera $3 = \frac{p-1}{2}$ variations de signe. Donc $p = 7$. On obtient ainsi un groupe $\mathcal{G}$ de degré 8 et d'ordre 168, $\not\equiv \mathfrak{v}(2, 7)$, défini, en prenant $i = 3$, $\rho = 1$, par

$$b^7 = a^3 = c^2 = 1, \qquad a^{-1}ba = b^2, \qquad cac = a, \qquad cbc = b^5cb^3$$

(les équations répondant à $\beta = 2, \ldots, 6$ résultent de celles-ci; *cf.* n° 1), et engendré par

$$0123456 = b, \qquad 124.365 = a, \qquad 0\infty.13.26.45 = c.$$

Il contient un diviseur normal D d'ordre 8 formé des $b^{-x}cb^x$ et de l'unité, et divise par conséquent le groupe linéaire total à trois variables dans C(2); en désignant respectivement ∞, 0, 1, 2, 3, 4, 5, 6 par les points 000, 100, 010, 001, 110, 011, 111, 101, on a

$$c = |x+1, y, z|, \qquad b = |z, x+z, y|, \qquad a = |x, z, y+z|.$$

Le diviseur normal $\{D, c\} = \{b, c\}$ est le groupe d'ordre $2^3(2^3-1)$ du n° 2. On a évidemment $\mathcal{G} = D\{a, b\}$, et D est le seul diviseur normal minimum possible dans un groupe primitif de degré 8. Le groupe fixant deux symboles $\{a\}$ a 28 conjugués et est, par suite, permutable aux seules substitutions du groupe Γ de générateur

$$ac = 164325 \,.\, 0\infty$$

composé des six substitutions permutant entre eux 0, ∞. Deux substitutions γ, γ' d'ordre $\neq 2$ de Γ ne peuvent être conjuguées dans $\mathcal{G}$, car si $s^{-1}\gamma s = \gamma'$, s doit permuter entre eux 0, ∞, donc être dans Γ. Donc chaque substitution d'ordre $\neq 2$ de Γ a 28 conjuguées. $\{b\}$ étant permutable aux seules substitutions de $\{a, b\}$, b n'a pas d'autre conjuguée dans $\{a, b\}$ par les opérations de $\mathcal{G}$ que par celles de $\{a, b\}$; donc pas d'autres que b, b^2, b^4. Ainsi dans $\mathcal{G}$ les opérations d'ordre 3, 6, 7 forment respectivement deux systèmes conjugués de 28, deux de 28, deux de 24. Les opérations d'ordre 2 forment un système de 7. $\{a\}$ et $\{b\}$ ne divisant normalement aucun diviseur normal, les facteurs de composition de $\mathcal{G}$ sont 3, 7, 2, 2, 2, 1 dans cet ordre unique.

Soit maintenant $\alpha = -1$. Si c transforme chaque cycle de a en lui-même, $c = (0, \infty)(i^{2x}, i^{2\rho-2x})(i^{2x+1}, i^{2\sigma-2x-1})$, $x = 0, 1, \ldots, \frac{1}{2}(p-3)$, $\rho, \sigma < \frac{1}{2}(p-1)$, ou $c = (z, \xi z^{-1})$, ξ étant égal à $i^{2\rho} = r$ ou à $i^{2\sigma} = s$ selon que z est carré ou non. Ici encore il faut et il suffit que $cb^\beta c = b^x cb^{x'} b^{-t} a^y b^t$. Or, si $p \equiv 1 \pmod 4$, c remplaçant -1 par $-r$, on aura

$$cbc = (\infty, r, \ldots, -r),$$

et, pour $t = r$,

$$b^{-t} a^y b^t = (r)(\ldots).$$

Donc, $x = x' = r$ et $cbc = b^r ca^\nu b^r$. Pour que le second membre fixe o, il faut $i^{2\nu} = -r$. Soit alors ν le premier non carré (mod p) dans la suite des entiers naturels;

$$cbc = \left(\infty, r, \frac{r}{2}, \cdots, \frac{r}{\nu-1}, \frac{s}{\nu}, \cdots, -r\right),$$

$$b^r ca^\nu b^r = \left(\frac{r}{\nu-1}, \frac{1-\nu}{r}s + r, \cdots\right).$$

Donc $s = r$, $c = (rs^{-1})$ et $\mathfrak{G} = \mathfrak{v}(2, p)$. Alors

$$cb^\beta c = \left(\infty, \frac{r}{\beta}, \frac{r}{2\beta}, \cdots, \frac{-r}{\beta}\right),$$

et pour $t = \frac{r}{\beta}$,

$$b^{-t} a^\nu b^t = \left(\frac{r}{\beta}\right)(\ldots), \qquad x = x' = \frac{r}{\beta}, \qquad cb^\beta c = b^{\frac{r}{\beta}} ca^\nu b^{\frac{r}{\beta}}.$$

Pour que le second membre fixe o, il faut $i^{2\nu} = \frac{-r}{\beta^2}$, et l'on vérifie directement que cela suffit, quel que soit le carré $-r = \varkappa^2$; en profitant de l'indétermination de $\varkappa$ on pourra choisir y pour une des valeurs des β. Ainsi $\mathfrak{v}$ est défini par $b^p = a^{\frac{p-1}{2}} = c^2 = (ca)^2 = 1$, $a^{-1} ba = b^\nu$, $cb^\beta c = b^{-\frac{\varkappa^2}{\beta}} ca^\nu b^{-\frac{\varkappa^2}{\beta}}$, $\beta i^\nu = \varkappa$, $\varkappa$ étant quelconque ($\neq$ o) et indépendant de β. Il suffira de faire parcourir à β un système de restes tels qu'aucune équation ne résulte des autres (*cf.* 1). En prenant $y = 1$ pour une valeur de β on pourra éliminer a par la dernière équation. Pour $\beta = \varkappa$, cette dernière équation se réduit à $(b^\varkappa c)^3 = 1$.

Pour $p = 5$, $i = 2$, $k = 1$, les équations

$$b^5 = a^2 = c^2 = (ca)^2 = (ab)^2 = (bc)^3, \qquad cb^2 c = b^2 cab^2$$

se réduisent à $b^5 = c^2 = (bc)^3 = 1$; il suffit de vérifier que, en posant $a = cb^3 cb^2 cb^3$, ces dernières équations entraînent

$$(cb^3 cb^2 cb^3)^2 = (b^3 cb^2 cb^3)^2 = (cb^3 cb^2 cb^3)^2 = 1.$$

Or on a

$$cb^3cb^2cb^3 = cb^2.bcb.bcb^3 = cb^2cb^4.cbc.b^3 = cb.bcb.b^2cb^2$$
$$= cbc.b^4cb^2cb^2 = b^4cb^3cb^2cb^2 = (b^4c)b^3cb^2.cbc(b^4c)^{-1}$$
$$= (b^4c)b^3.cbc.b^4(b^4c)^{-1} = (b^4c)b^2cb^3(b^4c)^{-1}$$

conjuguée de c, donc d'ordre 2,

$$b^3cb^3cb^3 = (b^3c)b^3.cbc.(b^3c)^{-1} = (b^3c)bcb^4(b^3c)^{-1}$$

conjuguée de c, enfin

$$cb^3cb^2cb^4 = cb^3cb^2.cb^4c.c = cb^3cb^3cbc$$
$$= (cbc)^{-1}.cb^4c.b^3cbc = (cbc)^{-1}bcb^4(cbc)$$

conjuguée de c. Ainsi $\mathfrak{v}(2, 5)$ d'ordre 60 est engendré par

$$b = (z+1) = (01234) \qquad c = (-z^{-1}) = (0\infty)(14)$$

et défini par

$$b^5 = c^2 = (bc)^3 = 1.$$

Si $p \equiv 3 \pmod 4$, $cbc = (\infty, r, \ldots, -s)$, et pour $t = r$ il faut $x = s$, $x' = r$, $cbc = b^s ca^y b^r$: le second membre devant fixer 0, il faut $i^{2y} \equiv -1$, ce qui est impossible, $-s$ n'étant pas carré.

Si c échange les cycles de a,

$$c = (0, \infty)(i^{2x}, i^{2\rho+1-2x})(i^{2x+1}, i^{2\sigma+1-2x-1}) = (z, \xi z^{-1});$$

$\xi = i^{2\rho+1} = r$ si z est carré, $\xi = i^{2\sigma+1} = s$ si z est non carré. Or si $p \equiv 1 \pmod 4$, $cbc = (\infty, r, \ldots, -r)$, et pour $t = r$ il faut

$$x = x' = r, \qquad cbc = b^r ca^y b^r;$$

le second membre devant fixer 0, il faut $si^{2y} = -r^2$, ce qui est impossible, s étant non carré. Si $p \equiv 3 \pmod 4$, $cbc = (\infty, r, \ldots, -s)$, et, pour $t = r$, $b^{-t}a^y b^t = (r) \ldots$, $x = s$, $x' = r$, $cbc = b^s ca^y b^r$. Le second membre devant fixer 0, il faut $i^{2y} = -r$. Soit alors ν le pre-

mier non carré (mod p) dans la suite des entiers naturels;

$$cbc = \left(\infty,\ r,\ \frac{r}{2},\ \ldots,\ \frac{r}{\nu-1},\ \frac{s}{\nu},\ \ldots,\ -s\right),$$

$$b^r ca^\nu b^s = \left(\frac{r}{\nu-1},\ \frac{1-\nu}{\nu}r+s,\ \ldots\right).$$

Donc $c=(rz^{-1})$, le groupe est $\mathfrak{v}(2, p)$ et l'on a les mêmes équations que tout à l'heure.

Pour $p=7$, $i=3$, $\varkappa=2$, les équations

$$(1)\quad b^7 = a^3 = c^2 = (ca)^2 = 1, \quad a^{-1}ba = b^2, \qquad cb^3c = bcab$$

(la dernière s'écrivant $a=cb^6cb^3cb^6$) suffisent, car de la dernière résulte

$$cbc = b^3cb^6a^2 = b^3ca^2b^3$$

dont le carré donne

$$\begin{aligned} cb^2c &= b^3.ca^2.b^6ca^2b^3 = b^3a.cb^6c.a^2b^3 \\ &= b^3.ab^4.ac.b^4a^2.b^3 = b^5cb^5 \end{aligned} \qquad \text{ou} \qquad (b^2c)^3 = 1,$$

et le carré de $cb^3c = bcab$ donne

$$cb^6c = bc.ab^2.cab = b.cbc.b \qquad \text{ou} \qquad (bc)^4 = 1.$$

Inversement (1) résulte de $b^7 = c^2 = (b^2c)^3 = (bc)^4 = 1$. En effet, en posant

$$a = cb^6cb^3cb^6,$$

$ca = b^6c.b^3cb^6$ est conjuguée de $b^3.cb^5c = b^5cb^2$, donc de c, qui est d'ordre 2.

$$\begin{aligned} a^{-1}ba &= bcb^3.bcbcbcb.b^5cb^3cb^6 \\ &= bcb^3.cb^5c.b^3cb^6 = b.cb^5cb^5c.b^6 = b^2. \end{aligned}$$

Enfin,

$$\begin{aligned} a^2 &= cb^6cb^3.cb^6cb^6c.b^3cb^6 = cb^6cb^6.b^5cb^5.b^6cb^6 \\ &= cb^6cb^6c.b^2.cb^6cb^6 = bcb^4cbc = a^{-1}. \end{aligned}$$

Ainsi $\mathfrak{v}(2,7)$ est engendré par

$$b=(z+1)=0123456, \qquad c=(3z^{-1})=0\infty.13.25.46$$

et défini par

$$b^7=c^2=(b^2c)^2=(bc)^4=1.$$

En posant $b=b'^4$, $b'=b^2$, on obtient les équations de M. Dyck (*M. A.*, t. XX, p. 41, 1882).

$\mathfrak{v}(3,2)\equiv\mathfrak{L}(3,2)$ *étant un* g^8_{168} *simple est isomorphe à* $\mathfrak{v}(2,7)$.

Pour $p=11$, $i=2$, $\varkappa=4$, les équations

$$b^{11}=a^5=c^2=(ca)^2=1. \qquad a^{-1}ba=b^4, \qquad cbc=b^6ca^2b^6$$

suffisent, car le carré de la dernière donne $cb^2c=b^3cab^3$, et sa quatrième puissance $(cb^4)^2=1$.

Pour $p=13$, $i=2$, $\varkappa=4$, les équations

$$b^{13}=a^6=c^2=(ca)^2=1, \qquad a^{-1}ba=b^4, \qquad cbc=b^{-3}ca^2b^{-3},$$
$$cb^2c=b^5cab^5$$

suffisent, car la dernière élevée au carré donne

$$cb^4c=b^5cab^{-3}cab^5=b^4cb^4;$$

elle donne encore directement $cb^6c=b^2cb^8a^5$ dont le produit avec $cbc=b^{-3}ca^2b^{-3}$ est

$$cb^6c=b^2cb^8a^5b^{-3}ca^2b^{-3}=b^2acb^{-1}ca^2b^{-3}=b^6ca^3b^6.$$

4. Soient $s=s_1\dots s_r$, $s_i=(a_{i1}\dots a_{ip})$ une substitution d'ordre premier p à r cycles, $\mathrm{H}=\{s\}$, $\mathrm{H}_i=\{s_i\}$. Cherchons le groupe Γ des substitutions permutables à H dans le symétrique de même champ. Γ contenant normalement H est imprimitif et contient normalement un groupe K ne permutant pas les systèmes d'imprimitivité. $\Gamma\,|\,\mathrm{K}$ est isomorphe au symétrique $\{(12),(12\dots r)\}$ de champ $1,2,\dots,r$.

Posons

$$\Pi_1^p(a_{1i}a_{2i}) = \alpha, \qquad \Pi_1^p(a_{1i}a_{2i}\dots a_{ri}) = \beta, \qquad |\alpha, \beta| = S.$$

α et β étant permutables à s, on aura $\Gamma = KS$. Soient k une substitution de K, k_i son effet sur $a_{i1}, \dots, a_{ip}$, ρ une racine primitive de p et $k^{-1}sk = s^{\rho^r}$. On aura $k_i^{-1}s_ik_i = s_i^{\rho^r}$ et k_i est dans le métacyclique $|s_i, t_i|$ où $t_i^{-1}s_it_i = s_i^{\rho}$. Donc k sera de la forme $\Pi_i s_i^{\sigma_i}t^x$, $t = t_1 \dots t_r$, et $K = |s_1, \dots, s_r, t|$ d'ordre $p^r(p-1)$. K contient normalement $|s_1, \dots, s_r| = K_0$ *et a la parité de* r. $k_i = s_i^{\sigma_i}t_i^x$ déplaçant $p-1$ symboles ou p, selon que $x \neq 0$ ou $x = 0$, K_0 contient toutes les s^{rp} de K. Il est clair que Γ *est résoluble si* $r \leqq 4$. En remplaçant au besoin t_i par une de ses conjuguées, on peut supposer que t_i fixe a_{i1}; alors chaque substitution de S sera évidemment permutable à chaque substitution de $|s, t|$.

Cherchons le plus grand commun diviseur D de K avec un groupe $G > \Pi$ de degré rp, mais de classe $c > (r-1)p$, ou du moins ne contenant pas de s_p de degré $< rp$. Dans une substitution $\Pi_1^r s_i^{\sigma_i}t^x$ de D, x ne peut s'annuler que si tous les σ_i sont $\neq 0$; et si D contient $u = \Pi_1^r s_i^{\sigma_i}$ et $u' = \Pi_1^r s_i^{\sigma'_i}$, donc $u^\alpha u'^{\alpha'}$, α et α' vérifiant $\alpha\sigma_1 \equiv -\alpha'\sigma'_1 \pmod p$, on devra avoir $\alpha\sigma_i \equiv -\alpha'\sigma'_i$, quel que soit i, donc $\sigma'_i \equiv \lambda\sigma_i$, $u' = u^\lambda$. Donc le plus grand commun diviseur de D, K_0 est $|u| = D^0$ normal dans D. Si $D > D_0$, soient vt^x, $v't^{x'}$, ... ses substitutions, v, v', ... étant dans K_0, et l'un au moins des x, x', ... étant $p-1$. D contiendra $(vt^x)^\beta(v't^{x'})^{\beta'}\dots = wt^{\beta x+\beta' x'+\dots}$, w étant dans K_0, et l'on peut choisir β, β', ... tels que $\beta x + \beta' x' + \dots$ soit le plus grand commun diviseur 0 de x, x', ... Mais si D contient wt^0 et $w't^{m0}$, il contient $(wt^0)^m = w_m t^{m0}$ et $w'w_m^{-1} = u^\delta$; donc $w' = u^\delta w_m$ et $w't^{m0} = u^\delta(wt^0)^m$. Donc $D = |u, wt^0|$ est isomorphe à un diviseur du métacyclique. En changeant au besoin de notation, on peut supposer que $D \equiv |s, t^0|$ et que t_i fixe a_{i1}, en sorte que chaque substitution de S (formée avec les nouveaux symboles) soit permutable à chaque substitution de D. Soient $0 > 0$, Δ le plus grand commun diviseur de G, Γ et $\gamma\chi$ une substitution de Δ, γ étant dans S et χ dans K. Pour que $(\gamma\chi)^{-1}s^y t^{0z}\gamma\chi$ soit dans D, quels que soient y et z, il faut et suffit que $\chi^{-1}t^{0z}\chi$ soit dans D, ou, puisque $\chi = \Pi_i s_i^{\alpha_i}t^x$, que $s_i^{-\sigma_i}t_i^0 s_i^{\sigma_i} = s_i^\sigma t_i^{0z}$,

σ *et* τ *étant indépendants de* i. Or, en observant que $t_i^{\sigma} s_i^{\tau} t_i^{-\sigma} = s_i^{\tau\rho^{-\sigma}}$, la condition précédente donne $s_i^{\tau(\rho^{-\sigma}-1)} t_i^{\sigma} = s_i^{\tau} t_i^{\sigma\tau}$, d'où $\sigma_i(\rho^{-\sigma}-1) = \sigma$, $\tau = 1$. Donc $\varkappa$ est dans $|s|$ et $\Delta = D\Sigma$, Σ divisant S; Δ est le produit direct de D, Σ, et si $r = 2$, $\Delta | |s|$ est abélien.

5. Je me bornerai à énoncer ici certains théorèmes dont j'aurai à faire usage.

Dans un groupe primitif G *de degré* kp *et d'ordre* akp (p *premier*, $ak \not\equiv 0 \bmod p$), *le plus petit multiple commun* M *des diviseurs d'ordre* p (*tous conjugués*) *est simple. Si* $k > 1$, (M, 1) *est composé.* Comme $G = MB$, B étant le groupe des substitutions permutables à un g_p, on a $G|M \equiv B|D$, D étant le plus grand commun diviseur de B, M. *Si donc* $k < 5$, $G|M$ *est résoluble. Si* $k = 1$, $G|M$ *est cyclique. Tout diviseur normal* $H > 1$ *de* G *étant transitif, donc d'ordre* $\equiv 0 \pmod p$, *donc* $\geq M$, $G|H$ *sera cyclique* (Miller, *P. L. M. S.*, t. XXXI, 1899, p. 148).

Un $g^{p+\alpha}$ *où* $\alpha \geq 3$ *ne peut être* $\alpha + 1$ *fois transitif sans contenir l'alterné.* On peut dire encore qu'*un* g^n *primitif d'ordre* $< \frac{1}{2} n!$ *ne peut contenir une* s_p^p *que si* $n = p$, $p+1$, $p+2$ Plus généralement, *un* g^n *primitif d'ordre* $< \frac{1}{2} n!$ *ne peut contenir une* s_p^{kp} ($k < 6$ *et* $< p$) *que si* $n \leq kp + k + 1$. *Un* $g^{2p+\alpha}$ ($\alpha \geq 3$) *ne contenant pas l'alterné ne peut être* $\alpha + 1$ *fois transitif.* (Jordan, *S. M.*, t. I, 1873, p. 40-45. *Cf.* Miller, *B. S. Am.*, t. IV, 1898, p. 141).

6. Soient G un groupe transitif de degré $n = rp$ (p premier), de classe $c > (r-1)p$, d'ordre $N = mp$ (m premier à p et $> n - p + 1$); $H = |s|$ un des g_p conjugués de G [$s = s_1 \dots s_r$, $s_i = (a_{i1} \dots a_{ip})$]; Δ le $g_{\delta p}$ des substitutions de G permutables à H; D le g_{dp} des substitutions de Δ qui ne permutent pas les systèmes d'intransitivité de H. On a vu que, si $d > 1$, Δ est le produit direct de D par un groupe Σ isomorphe à un diviseur du g^r symétrique. Les substitutions d'ordre multiple de p sont toutes dans les conjugués de Δ, et chacun de ces conjugués contient au moins $p-1$ de ces substitutions, celles de H. Il y a donc au moins $\frac{N}{\delta p}(p-1)$ substitutions d'ordre multiple de p (et, par suite,

de degré n). D'autre part, le nombre total des symboles déplacés par les substitutions de G est $N(n-1)$ et les x substitutions de degré $<n$ en déplacent

$$N(n-1)-n(N-x)=nx-N.$$

Or, c étant $>n-p$, $x-1$ de ces dernières sont de degré $\geq n-p+1$. Donc

$$nx-N\geq(n-p+1)(x-1) \qquad \text{et} \qquad x\geq\frac{N-n+p-1}{p-1}>\frac{N}{p}$$

(d'après l'hypothèse faite sur m). Or, c étant $>(r-1)p$, les x substitutions de degré $<n$ auront toutes un ordre premier à p et feront partie des μm (μ entier) substitutions dont l'ordre divise m. Donc $\mu\geq 2$ et il y a au plus $N-2\frac{N}{p}$ substitutions d'ordre multiple de p. Donc

$$N\frac{p-1}{\delta p}\leq N-\frac{2N}{p},$$

d'où

$$\delta\geq\frac{p-1}{p-2} \qquad \text{ou} \qquad \delta\geq 2.$$

Si $r=1$ les hypothèses se vérifient d'elles-mêmes pour G non cyclique et l'on a ce théorème de Mathieu (*J. M.*, 2e série, t. VI, 1861, p. 310) *qu'un g^p non cyclique contient des substitutions $\neq 1$ permutables à ses g_p.*

On peut remplacer les hypothèses faites sur m et c par celle *qu'il n'y a pas de s_p à moins de r cycles et que la transitivité t est ≤ 2.* Pour le faire voir, j'établirai d'abord une formule générale. Considérons les $\binom{n}{k}$ combinaisons k à k des n symboles déplacés par un $g^n G$ rangées dans un ordre arbitraire. Soit G_i^k le diviseur fixant les k symboles de la $i^{\text{ième}}$ combinaison. G_i^k peut coïncider avec G_j^k, donc aussi avec un $G_i^{k'}$, où $k'>k$; mais je regarderai ici chaque élément d'un G_i^k comme distinct de ceux des autres. Une substitution s fixant $k+\nu$ symboles déterminés et point d'autres figurera, si elle existe

dans G, dans $\binom{k+\nu}{k} = \binom{k+\nu}{\nu} G_i^k$. Donc, dans l'ensemble, $E_k = \Sigma_i G_i^k - \Sigma_i G_i^{k+1} + \ldots$, de nombre

$$e_k = \Sigma_i(G_i^k, 1) - \Sigma_i(G_i^{k+1}, 1) + \ldots = \Sigma_i(G_i^k, 1) - e_{k+1},$$

elle figurera $\binom{k+\nu}{k} - \binom{k+\nu}{\nu-1} + \binom{k+\nu}{\nu-1} - \ldots \pm 1 = \binom{k+\nu-1}{\nu}$ fois. Si s n'existe pas dans G, elle ne figurera pas non plus dans E_k et l'on aura, g_μ étant le nombre des éléments de G qui fixent μ symboles exactement,

$$e_k = \Sigma_0^{n-k}\binom{k+\nu-1}{\nu} g_{k+\nu} = \Sigma_k^n \binom{\mu-1}{\mu-k} g_\mu \geq \binom{n-1}{n-k} \qquad (\text{car } g_n = 1).$$

Pour $k = 1$, e_1 est le nombre exact des substitutions de degré $< n$. Si G est t fois transitif,

$$(G_i^k, 1) = (G, 1) : n(n-1)\ldots(n-k+1) \qquad (k \leq t)$$

et

$$e_1 = (G, 1) - \tfrac{1}{2!}(G, 1) + \ldots + \frac{(-1)^{t-1}}{t!}(G, 1) + (-1)^t e_{t+1}.$$

Cela posé, il y aura, dans le groupe particulier que nous considérons, $e_1 = \frac{1}{2}N + e_3$ $(e_3 > 1)$ substitutions de degré $< n$. Donc

$$N - \frac{N}{2} > N\,\frac{p-1}{\delta p} \qquad \text{ou} \qquad \delta > 2\,\frac{p-1}{p} \qquad \text{ou} \qquad \delta \geq 2.$$

Si t est ≥ 4, $e_1 = \frac{5}{8}N + e_5$ $(e_5 > 1)$ et $\delta > 3 - \frac{p+8}{3p}$; donc $\delta \geq 4$, si $p \geq 5$. Pour $t \geq 4$, $r = 3$, G pair, $(\Sigma, 1)$ doit être ≤ 3, donc $d \geq 2$. Pour $t \geq 2$, $r = 2$, G pair, $(\Sigma, 1)$ doit être $= 1$, donc $d \geq 2$ (et il en est de même pour $t = 1$ si $c > p$ avec $\frac{N}{p} > p + 1$).

7. Supposons maintenant $2p + 1 = q$ premier et soient G un g^q

transitif d'ordre $< \frac{1}{2}(q!)$ et $> q(q-1)$, G d'ordre N, le g^{2p} fixant un des symboles. G contiendra des s_p; car les substitutions ($\neq 1$) de $\mathcal{G}$ permutables à ses g_q sont de degré $q-1=2p$ et d'ordre 2, p ou $2p$; or, si elles étaient d'ordre 2, elles seraient impaires et, dans le plus petit commun multiple des substitutions paires de $\mathcal{G}$, les g_q ne seraient permutables qu'à leurs propres substitutions. G ne contiendra pas de s_p^p, car il faudrait $p \geq \frac{2}{3}q$, ce qui ne se peut. De plus N qui divise $(2p)!$ n'est pas divisible par p^2; car un g_{p^2} y serait abélien sans être cyclique; or, toute s_p est ici de la forme $s=s_1 s_2$ $[s_i=(a_{i_1}\dots a_{i_p})$; $i=1, 2]$, et dans les s_p permutables à s qui sont de la forme $s_1^{\alpha_1} s_2^{\alpha_2}$, il faut $\alpha_1=\alpha_2$, sans quoi $s^{-\alpha_1} s_1^{\alpha_1} s_2^{\alpha_2}$ serait une s_p^p. Soit d'abord $\mathcal{G}$ pair, donc $\delta=d$. Si G est intransitif, ses deux constituants transitifs de degré p, A et B, étant premiers à G, on a $G \equiv A \equiv B$, et comme A contient des substitutions d'ordre premier à p permutables à ses g_p, d est ≥ 2. Si G est transitif, $\mathcal{G}$ deux fois transitif contient $e_1=\frac{1}{2}qN+e_3 (e_3>1)$ substitutions de degré $\leq 2p$ et $qN\frac{p-1}{dp}$ s_p^{2p}. Donc

$$\frac{1}{2}qN - e_1 \geq qN\frac{p-1}{dp},$$

d'où

$$d > 2\frac{p-1}{p} \qquad \text{ou} \qquad d \geq 2.$$

Si $\mathcal{G}$ est impair, on arrive à la même conclusion en considérant le plus petit commun multiple de ses substitutions paires. *Ainsi $\mathcal{G}$ contient des substitutions de degré $2(p-1)=q-3$ permutables à $\{s\}$* (énoncé par Mathieu, *J. M.*, 2e série, t. XVIII, 1873, p. 26).

Soit $\mathfrak{M}$ le plus petit commun multiple des g_q de $\mathcal{G}$. Si $\mathcal{G}$ est pair, les substitutions d'ordre multiple de p permutables à un g_q seront toutes d'ordre p. Or, $(\mathcal{G}, \mathfrak{M})$ qui divise $p(\delta)$ ne peut être égal à p, car $(\mathcal{G}, 1)$ n'étant pas divisible par p^2, $(\mathfrak{M}, 1)$ serait premier à p et chaque g_q de $\mathfrak{M}$ ne serait permutable qu'à ses substitutions. Donc $(\mathcal{G}, \mathfrak{M})=1$. Donc *si $\mathcal{G}$ est pair, $\mathcal{G}=\mathfrak{M}$ est simple.*

Ainsi $D=\{s, g\}$, g étant une s^{q-3} permutable à $\{s\}$. Pour former g on n'a à choisir qu'entre un nombre limité de formes distinctes; car, si t_i est la s_{p-1}^{p-1} permutable à $\{s_i\}$ qui fixe a_{i_1} et si $t=t_1 t_2$, on a $D=\{s, s_2^\sigma t^\theta\}$, σ et θ étant indéterminés; $s_2^\sigma t_2^\theta$ est une conjuguée t_2^θ

de t_2 complètement déterminée par celui des a_{2k} qu'elle fixe, et si l'on pose $a_{2,\lambda+j} = a'_{2j}$ ($j = 1, \ldots, p$ et $\lambda + j$ étant pris mod p, ≥ 0, $\leq p-1$), t'_2 se déduit de t_1 en écrivant a'_{2j} pour a_{1j} : on aura toutes les $s_2^q t^0$ en faisant varier λ et 0.

Désignons les symboles de $\mathcal{G}$ par $0, 1, \ldots, q-1 \pmod q$: on pourra supposer que $\mathcal{G}$ contient $(z, z+1) = \alpha$ et que $s = (z, t^2 z)$ t étant racine primitive de q. Écrivons $s = (t^{2x}, t^{2(x+1)})(t^{1+2x}, t^{1+2(x+1)})$; en faisant correspondre t^{2x} dans le premier cycle et t^{1+2x} dans le second au symbole x de la substitution $(x, x+1) \pmod p$ et en observant que la $s_{\frac{p-1}{2}}$ conjuguée de $(x, \rho^0 x)$ (ρ racine primitive de p) et permutable à $|(x+1)|$ qui fixe ξ est la transformée $(x, \rho^0(x-\xi)+\xi)$ de $(x, \rho^0 x)$ par $(x+\xi)$, on voit que les diverses de g sont $(t^{2x}, t^{2x\rho^0})$ $(t^{1+2x}, t^{1+2[\rho^0(x-\xi)+\xi]})$ $(\xi = 0, \ldots, p-1;\ 0 = 1, p-2)$.

Écrivons β pour s, γ pour g^2, γ_i pour les différentes formes de γ, et considérons les groupes

$$(\alpha, \beta, \gamma_i) = G_i^q = G_i.$$

G_i étant pair sera toujours simple. Tout g_N^q $\mathcal{G}$ où $N > q(q-1)$ et $< \frac{1}{2}(q!)$ contient un G_i, soit G_1, et le plus petit commun multiple $\mathfrak{M}$ des g_q de $\mathcal{G}$ est $\geq G_1$. Si $\mathfrak{M} > G_1$, $\mathcal{G}$ contient des s_q^q hors de G_1 et $(\mathcal{G}, G_1)$ est $\geq q$. Or, on ne peut avoir $(\mathcal{G}, G_1) = q$, car N serait multiple de q^2 et ne diviserait pas $q!$. *Donc* $(\mathcal{G}, G_1) \geq q+1$.

8. Pour $q = 5$, G_i n'existe pas, car il devrait contenir une s^{q-3}. *Donc, tout g^5 transitif divise le métacyclique ou contient l'alterné.*

Soient $q = 7$, $\iota = 3$,

$$\alpha = 0123456, \qquad \beta = 124.365,$$
$$\gamma_1 = 24.56, \qquad \gamma_2 = 24.35, \qquad \gamma_3 = 24.36.$$

Ici G_2 est l'alterné, car $\alpha^{-1}\gamma_2\alpha\gamma_2 = 246$, et G_3 est conjugué de G_1, car, en posant $0 = 1326745$, on a $0^2 = \beta$, $0^{-1}\alpha 0 = \alpha^3$, $0^{-1}\gamma_3 0 = \gamma_1$. Écrivons γ pour γ_1, G pour G_1, et examinons $|\alpha, \beta, \gamma| = G$. On a $\alpha\gamma\alpha^{-1} = 13.45 = \delta$. Le $g^6 F$ qui fixe 0 est donc transitif puisque $|\beta, \delta|$ l'est, et G est deux fois transitif. Formons encore $\beta^{-1}\delta\beta\delta = 45.26 = \varepsilon$.

Le diviseur E qui fixe 0, 1 n'est pas de degré effectif 5, car contenant le groupe quadratique $\{\gamma, \varepsilon\} = Q$ il serait transitif et diviserait le métacyclique : or les g_8 du $g^8_{1.8}$ sont cycliques. D'ailleurs E ne renferme ni s^4 cyclique (G est pair) ni s^3. Donc $E = Q$, F d'ordre 4.6 est $\{\beta, \gamma, \delta\}$, et $(G, 1) = 4.6.7 = 168$. Comme α, β, γ vérifient les équations

$$\alpha^7 = \beta^3 = \gamma^2 = (\gamma\beta)^2 = 1, \qquad \beta^{-1}\alpha\beta = \alpha^2, \qquad \gamma\alpha^3\gamma = \alpha\gamma\beta\alpha,$$

G est le groupe $\mathfrak{v}(2,7) \equiv \mathfrak{v}(3,2)$ dont on a déjà obtenu la représentation en g^8.

Cherchons à former un g^8 trois fois transitif où G soit le diviseur fixant 7. Il contiendra une transformée de γ de la forme $\zeta = 07.1x$, x étant inconnu. Comme $\zeta\beta\zeta$ doit être dans F (**1**), x ne peut être 2 ni 4, car $\zeta\beta\zeta\beta$ serait une s^3; x ne peut être 5 ni 6, car on aurait respectivement $\varepsilon\zeta\varepsilon = 07.14$, $\varepsilon\zeta\varepsilon = 07.12$. Mais $\zeta = 07.13$ donne

$$\zeta\beta\zeta = \delta\beta, \qquad \zeta\gamma\zeta = \gamma, \qquad \zeta\delta\zeta = \delta, \qquad \text{donc} \qquad \zeta F\zeta = F$$

et

$$\zeta\alpha\zeta = \alpha\zeta\delta\beta^2\alpha^3, \qquad \text{donc} \qquad \zeta\alpha F\zeta = \alpha\zeta\delta\beta^2\alpha^3 F.$$

Or αF renferme un système de restes de $G(\mathrm{mod}\, d\, F, 1)$, puisque, F étant transitif, αF renferme des substitutions changeant o en 1, ..., 6, Donc on a bien $\zeta G\zeta \leqq G\zeta G$, et $\{\alpha, \beta, \gamma, \zeta\} = H$ est un g^8_{168} trois fois transitif, défini par les équations de G jointes à

$$\zeta^2 = (\zeta\gamma)^2 = (\zeta\delta)^2 = 1, \qquad \zeta\beta\zeta = \delta\beta, \qquad \zeta\alpha\zeta = \alpha\zeta\delta\beta^2\alpha^3 \quad (\delta = \alpha\gamma\alpha^{-1}).$$

On vérifie directement que les transformées respectives ξ_k ($k = 0, \ldots, 6$) de $\xi = \zeta\beta^{-1}\delta\beta\delta = 07.13.26.45$ par α^k forment avec 1 un g_8 abélien $(\xi, \xi_1, \xi_2) = A$ normal dans H. On remarquera que A n'est qu'une fois transitif dans H trois fois transitif. Tout diviseur normal I de H coïncide avec A, car on a $H = IG$, et G simple est premier à I. Donc I est d'ordre 8. Donc $I = A$, sans quoi IA serait normal $> A$ et $H \mid I \equiv G$ ne serait pas simple; $\{\alpha, \beta, \xi\}$ et $\{\alpha, \xi\}$ sont respectivement le g^8_{168} composé et le $g^8_{7.8}$ deux fois transitifs (**2, 3**). Si l'on convient que 7 représente ∞ du C(7), H contient $(z, -z^{-1}) = 0\infty.16.23.45 = \xi\beta^2\gamma$ et par suite aussi $\mathfrak{v}(2,7) = \{(z+1), (i^2 z), (-z^{-1})\}$.

Soit Γ un g^7 ne contenant pas l'alterné. $(\Gamma, 1)$ divise $\frac{7!}{2.3} = 4.5.6.7$. Si $(\Gamma, 1) > 7.6$, Γ est $\geq G$. Or on a vu que, si $\Gamma > G$, $(\Gamma, 1) > 4.6.7.8$. *Donc* G *est l'unique* g^7 *ne contenant pas l'alterné et ne divisant pas le métacyclique.* Par suite, s'il y a un g^8 K trois fois transitif dans le champ $0, \ldots, 7$ autre que H, le groupe M qui y fixe 7 sera le métacyclique qu'on peut supposer engendré par

$$\alpha = 0123456, \qquad \theta = 1326\,45 \ (\theta^2 = \beta),$$

et s'obtiendra en adjoignant un générateur ζ permutable à $\{\theta\}$, transformé de $\theta^3 = 16.34.25$, de la forme $\zeta = (07)(6)\ldots$, θ^3 étant l'unique s_2 de $\{\theta\}$, on aura

$$\zeta\theta^3\zeta = \theta^3;$$

donc ζ fixe 1. On ne peut avoir $\zeta = 07.34.25$, car $\zeta\theta^3$ serait de degré 4 et K est de classe 6. Donc ζ a l'une des deux formes $07.23.45 = \zeta'$, $07.35.42$. $\zeta'\theta\zeta' = 123654$ n'étant pas dans $\{\theta\}$, il faut que $\zeta = 07.35.42$. On a alors

$$\zeta\theta\zeta = \theta^5, \qquad \zeta\alpha\zeta = \alpha\zeta\theta^3\alpha;$$

or $\alpha\{\theta\}$ renferme un système de restes de M modd $\{\theta\}$, 1, puisque, $\{\theta\}$ étant transitif, $\alpha\{\theta\}$ contient des substitutions changeant 0 en $1, \ldots, 6$. *Ainsi* K *existe et est unique : c'est donc le* $g^8_{6.7.8}$, *trois fois transitif de Mathieu qui se trouve défini par* $\alpha^7 = \theta^6 = \zeta^2 = (\zeta\theta)^2 = 1$, $\theta^{-1}\alpha\theta = \alpha^3$, $\zeta\alpha\zeta = \alpha\zeta\theta^3\alpha$.

On a vu (**3**) qu'il y a deux g^8_{168}, et deux seulement, et que tout $g^8_{7.8}$ deux fois transitif a un g^8_8 normal abélien, contenant 7 s_2 conjuguées. Soient α une des s_7 d'un $g^8_{7.8}$ deux fois transitif, $\zeta = 07.1x.yz.tu$ la s_2 à adjoindre à α pour engendrer le groupe. Pour chacune des déterminations 2, 3, 4, 5, 6 de x, y étant un quelconque des symboles restants, z a trois déterminations possibles; d'où 15 formes à essayer. Mais $\theta^{-1}\zeta\theta$ convient ou non en même temps que ζ, et l'on connaît déjà la solution $\zeta = \xi = 07.13.26.45$. La condition $\zeta\{\alpha\}\zeta = \{\alpha\}\zeta\{\alpha\}$ exclut les formes restantes. Il n'y a donc qu'un $g^8_{7.8}$ deux fois transitif. Ce n'est d'ailleurs là qu'un cas particulier d'un théorème plus général (**2**). S'il y a encore un g^8 X deux fois transitif dans le champ

$0, \ldots, 7$, le diviseur M qui y fixe 7 sera un $g^1_{2.7}$ qu'on peut supposer être $\{\alpha, 0^3\}$ $(0^3 = 16.25.34)$ et s'obtiendra en adjoignant une s_2 $\zeta = (07)\ldots$, transformée de 0^3 permutable à 0^3, fixant par suite deux des symboles $1, \ldots, 6$ qui seront dans un même cycle de 0^3. En considérant au besoin le groupe transformé par 0, on peut supposer que ζ fixe 1 et 6. On ne peut avoir $\zeta = 07.34.25$, car $\zeta 0^3$ serait de degré 4 et X est de classe 6. Donc ζ a l'une des formes $07.32.45 = \zeta'$, $07.35.42$. Mais $\zeta'\alpha\zeta' = 7132546$ pour être dans $M\zeta'M$ devrait être de la forme $(60\ldots)\zeta'(01\ldots) = \alpha\zeta' 0^{3k}\alpha$, et l'égalité $\zeta'\alpha^6\zeta'\alpha\zeta'\alpha^6 = 0^{3k}$ est impossible. Il faudrait donc $\zeta = 07,35.42$. Mais $\zeta\alpha^2\zeta$ devrait être de la forme $\alpha^4\zeta 0^{3k}\alpha^4$ et $\zeta\alpha^3\zeta\alpha^2\zeta\alpha^3 = 0^5$. Donc X n'existe pas, et *les seuls* g^8 *de transitivité* $\geqq 2$ *sont un* $g^8_{7.8}$, *deux* g^8_{168}, *un* g^8_{336}, *un* g^8_{1344}.

9. Soit $q = 11$. On a, en écrivant a pour 10,

$$\alpha = 0123456789a, \qquad \iota = 2, \qquad \beta = 14593.28a76.$$

Si γ est d'ordre 2, γ a l'une des cinq formes

$$\gamma_1 = 43.59.86.a7, \qquad \gamma_2 = 43.59.a2.76, \qquad \gamma_3 = 45.59.78.62,$$
$$\gamma_4 = 43.59.6a.28, \qquad \gamma_5 = 43.59.27.8a.$$

Mais comme

$$[(\alpha^1\gamma_1)^6(\alpha^0\gamma_1)^6]^2 = 125, \quad (\alpha^3\gamma_3)^4 = 048, \quad [(\alpha\gamma_5)^6(\alpha^0\gamma_5)^6]^2 = 16a,$$

$G_1 = G_3 = G_5$ est l'alterné. Passons à γ_2, G_2 que j'appellerai respectivement γ, G. Les substitutions

$$\alpha^{-3}\gamma\alpha^3\alpha^{-6}\gamma\alpha^6 = 15.28.40.67 = \lambda, \qquad \alpha^2\gamma\alpha^{-2} = 081.237,45 = \mu$$

(qui montrent que G est deux fois transitif) engendrent un g^6 E où $\lambda\mu = 052.148.376 = \varkappa$ engendre un groupe normal, et où la troisième s_2 est $\varkappa^{-1}\lambda\varkappa = 42.01.85.36 = \nu$, les systèmes d'intransitivité étant 0, 1, 2, 4, 5, 8 et 3, 6, 7. Je dis que E est le groupe fixant a, 9.

En effet, en adjoignant $\zeta = \beta^{-1}\gamma\beta = 93.15.26.78$ et en posant $\zeta\varkappa = 05486.12397 = 0$, on a

$$0^5 = \zeta^2 = (\zeta 0)^3 = 1.$$

Donc $|\zeta, 0| = F$ est partiellement homomorphe au g^5_{60} *simple*. Donc il lui est isomorphe. D'ailleurs F contient $\lambda = 0^2\zeta 0^3\zeta 0^2$. Donc $F = |\zeta, \lambda, \mu|$ et F est l'*unique* g^{10}_{60} transitif.

Cherchons à adjoindre à F une substitution ρ telle que, dans $|F, \rho| = G'$, F soit le groupe fixant a. G' étant deux fois transitif, on peut supposer que $\rho = (9a)\ldots$ est conjugué de γ. On doit avoir $\rho E \rho = E$. Donc ρ permute entre eux les symboles de chaque système d'intransitivité de E et fixe un ou trois des symboles 3, 6, 7. Si ρ n'en fixait qu'un, ρ serait permutable à celle s des trois s_2 de E qui le fixe et fixerait deux symboles d'un des cycles de s en déplaçant quatre autres des symboles 0, 1, 2, 4, 5, 8 sans avoir dans le champ de ces symboles un cycle commun avec s (ρs serait alors une s^2); dans ces conditions ρ ne serait pas permutable à $|\varkappa|$.

Soit donc $\rho = 3.6.7.a9\ldots$; ρ devant être permutable à $\varkappa$, λ, μ, ν a trois formes possibles

$$\rho_1 = a9.04.12.58, \qquad \rho_2 = a9.01.28.45, \qquad \rho_3 = a9.08.15.24.$$

Mais comme $(\rho_2\zeta)^4 = a39$, $|F, \rho_2|$ est alterné et ρ_2 ne convient pas; si d'ailleurs on pose $52.48.36 = \tau$, on aura $\tau\rho_3\tau = \rho_1$ et $\tau\varkappa\tau = \varkappa^2$, $\tau\zeta\tau = \nu\zeta\varkappa^2$, donc $\tau F\tau = F$. Bornons-nous donc à faire $\rho = \rho_1$ et supprimons l'indice 1. On a

$$\rho 0\rho = 0\rho\mu 0, \qquad \rho 0^2\rho = 0^3\rho 0^3.$$

Or, $0E + 0^2E$ contenant des substitutions qui remplacent 9 par 0, ..., 8 renferme un système de restes de $F \pmod{E, 1}$. Donc, *il existe un* g^{11}_{60}, G' *deux fois transitif, et il est unique* comme le g^{10}_{60} transitif qui y fixe un symbole. Donc $G' = G\,[\alpha = \rho(\zeta 0^3)^3\zeta 0^2, \beta = 0^3\zeta 0^2\zeta\rho 0, \gamma = \beta\zeta\beta^{-1}]$, et G est défini par les équations de F jointes à

$$\rho^2 = (\rho\lambda)^2 = (\rho 0^2)^3 = 1, \qquad \rho\varkappa\rho = \varkappa, \qquad \rho 0\rho = 0\rho\mu 0,$$

ou, puisque $\mu 0 = \zeta 0^3\zeta 0^2\zeta$, par

$$0^5 = \zeta^2 = (\zeta 0)^3 = \rho^2 = (\rho 0^2)^3 = (\rho 0^2\zeta 0^3\zeta 0^2)^2 = 1,$$
$$\rho\zeta 0\rho = \zeta 0, \qquad \rho 0\rho = 0\rho\zeta 0^3\zeta 0^2\zeta.$$

G étant simple contient $12\,g_{11}$ et est représentable en g'^{12} deux fois transitif (le diviseur fixant un symbole contient des s_{11}). G est donc isomorphe à *l'unique* g^{12}_{660} deux fois transitif $\mathfrak{v}(2, 11)$ dont on a trouvé les équations sous une autre forme au n° 3.

Considérons maintenant $\{\alpha, \beta, \gamma_4\} = G_4$. Les substitutions

$$\alpha^2\gamma_4\alpha^{-2} = 06.12.37.48 = \mu'$$

et

$$\alpha^{-6}\gamma_4\alpha^6.\beta^{-3}\alpha^{-1}\gamma_4\alpha^4\beta^3 = 074.125.368 = \varkappa'$$

montrent que G_4 est deux fois transitif. En posant $\tau = 13427568$ on a $\tau^{-1}\varkappa'\tau = \varkappa$, $\tau^{-1}\mu'\tau = \mu$; donc $\{\varkappa', \mu'\}$, qui fixe $9, a$, est d'ordre 6 et G_4 d'ordre $\geqq 660$. D'ailleurs

$$\tau^{-1}\alpha\tau = \rho 0^3\mu\zeta\varkappa^2,$$
$$\tau^{-1}\beta\tau = 0^3\mu\rho\lambda 0^3\mu\zeta,$$
$$\tau^{-1}\gamma_4\tau = 0^2\mu\varkappa^2 0^3\mu\rho 0^3\mu\varkappa 0^3\mu.$$

Donc

$$\tau^{-1}G_4\tau = G.$$

Cherchons à adjoindre à G une substitution σ telle que, dans $\{G, \sigma\} = H$, G soit le groupe fixant b. H étant trois fois transitif, on peut supposer que $\sigma = (ab)\ldots$ est conjuguée de γ et l'on voit, comme pour ρ, que σ a l'une des trois formes

$$\sigma_1 = ab.04.12.58, \qquad \sigma_2 = ab.01.28.45, \qquad \sigma_3 = ab.08.15.24.$$

σ_1 est à rejeter, car $\sigma_1\rho = ab9$; σ_3 de même, car, en posant $\tau = 05.14.67$, on a $\tau\lambda\tau = \lambda$, $\tau\varkappa\tau = \varkappa^2$, $\tau\zeta\tau = \lambda\zeta$, donc $\tau F\tau = F$ et $\tau\sigma_3\tau = \sigma_1$. Soit donc $\sigma = \sigma_2$ et effaçons l'indice. On aura

$$\sigma^2 = (\sigma\rho)^3 = 1, \qquad \sigma\varkappa\sigma = \varkappa, \qquad \sigma\lambda\sigma = \lambda, \qquad \sigma\zeta\sigma = \lambda\zeta,$$

et ces équations jointes à celles de G définissent H. La substitution $\sigma' = (z, -z^{-1})$ (mod 11) qui s'écrit (en mettant b pour ∞, a pour 10) $0b.1a.25.37.48.69$ n'est pas dans H (contrairement à l'assertion

de MATHIEU, *J. M.*, 1873), car $0(\sigma\alpha^7\gamma\alpha^4\sigma'\alpha^7\gamma\alpha^4)^2 = 0426.1837$, qui fixe b, a, 9, n'est pas dans E.

Si γ est d'ordre 4, on a encore cinq formes $\gamma_6, \gamma_7, \gamma_8, \gamma_9, \gamma_{10}$, dont les carrés reproduisent respectivement $\gamma_1, \ldots, \gamma_5$. Comme $\{\alpha, \beta, \gamma_i\}$ est $\geq \{\alpha, \beta, \gamma_i^2\}$, il suffit de considérer

$$\gamma_7 = 4539.a726, \qquad \gamma_9 = 4539.62a8.$$

Considérons d'abord $G_7 = \mathcal{G}$ en écrivant γ pour γ_7. On a

$$\alpha\beta\alpha^{-1} = 03482.17965.a = \delta, \qquad \alpha^{-2}\gamma\alpha^2 = 6750.1948.a.2.3 = \varepsilon.$$

Donc le g^{10} fixant a est transitif et $\mathcal{G}$ l'est deux fois.

$$\gamma^{-2}\varepsilon\gamma^2 = 1538.0769.2.4.a = \gamma_1, \qquad \gamma_1\varepsilon\gamma_1^2 = 0879.1645.a.2.3 = 0.$$

Donc le g^2 fixant a, 3 et le g^8 fixant a, 2, 3 sont transitifs; et $\mathcal{G}$ est quatre fois transitif. $\{\varepsilon, 0\}$ est un g_8^8 régulier (le groupe des quaternions) que l'on peut transformer par $\gamma_1\delta^{-2}\varepsilon^2\delta^2 = \omega$ en un groupe $\mathfrak{w}$ de générateurs

$$\omega^{-1}\varepsilon\omega = 0567.1243 = \lambda, \qquad \omega^{-1}0\omega = 0263.1745 = \mu,$$

fixant a, 9, 8, défini par

$$\lambda^4 = \mu^4 = 1, \qquad \lambda^2 = \mu^2, \qquad \mu^{-1}\lambda\mu = \lambda^3.$$

S'il existe une s_2, $\zeta = (78)\ldots$ telle que, dans $\{\mathfrak{w}, \zeta\} = \mathcal{E}$, $\mathfrak{w}$ soit le diviseur fixant 8, on peut supposer ζ semblable à $\lambda^2 = 06.14.23.57$. Pour que $\zeta\lambda^2\zeta = (58)\ldots$ ait la forme $d'\zeta d'$, d, d' étant dans $\mathfrak{w}$, il faut que $d = 57\ldots$, $d' = 75\ldots$, donc, $\mathfrak{w}$ étant régulier, que $d = d' = \lambda^2$, donc que $\zeta\lambda^2\zeta = \lambda^2\zeta\lambda^2$, ou $(\zeta\lambda^2)^3 = (\lambda^2\zeta)^3 = 1$. Donc $\zeta\lambda^2 = (785)\ldots$ et $\zeta = (78)(5)\ldots$. ζ et λ^2 n'ont aucun cycle commun, car $\zeta\lambda^2$ étant une s_3 de degré < 9 serait une s_3^6, donc de degré inférieur à la classe. Donc, si x, y, z, t désignent 1, 2, 3, 4 dans un ordre quelconque et si $\zeta = 0x.6y\ldots$, x et y ne sont pas dans le même cycle de λ^2, car ζ et λ^2 auraient le cycle zt. On a donc à essayer

pour ζ les formes

$$\zeta_1 = 01.62.43.78, \qquad \zeta_2 = 01.63.42.78,$$
$$\zeta_3 = 02.61.43.78, \qquad \zeta_4 = 02.64.13.78,$$
$$\zeta_5 = 03.61.42.78, \qquad \zeta_6 = 03.64.12.78,$$
$$\zeta_7 = 04.62.13.78, \qquad \zeta_8 = 04.63.12.78.$$

On a $(\zeta_4\lambda^2)^3 = 1$, $\zeta_4\lambda\zeta_4 = \mu^3\zeta_4\lambda\mu$; donc on peut prendre ζ_4. $\zeta_2\lambda\zeta_2$ n'étant pas dans $\omega\zeta_2\omega$, ζ_2 est à rejeter. Or les substitutions 14.23, 14.06, 23.06 permutables à ω transforment respectivement ζ_4 en ζ_8, ζ_1, ζ_5 et ζ_2 en ζ_7, ζ_6, ζ_3. Il suffit donc de considérer ζ_4 dont je supprimerai l'indice (ce choix a pour but d'obtenir finalement un groupe contenant α, β, γ). $\{\omega, \zeta\} = \varepsilon$ est défini par les équations de ω jointes à $\zeta\lambda\zeta = \mu^3\zeta\lambda\mu$ [d'où résulte $(\zeta\lambda^2)^3 = 1$], qui s'écrit $(\zeta\lambda)^2 = \mu^3\zeta\mu$. S'il existe une s_2, $\rho = (89)\ldots$ telle que, dans $\{\varepsilon, \rho\} = \mathfrak{F}$, ε soit le diviseur fixant 9, on peut supposer, F étant trois fois transitif, ρ semblable à λ^2. $\zeta\rho$ devant être d'ordre 3, ρ fixe 7. $\zeta\rho$ devant être de degré 9 (la classe est 8), ρ n'a aucun cycle commun avec ζ. ρ devant être permutable à λ^2 fixe 5 et a un cycle commun avec λ^2, mais un seul sans quoi $\rho\lambda^2$ serait de degré inférieur à la classe. Donc ρ a l'une des trois formes

$$\rho_1 = 89.03.14.26, \qquad \rho_2 = 89.04.16.23, \qquad \rho_3 = 89.06.12.34.$$

Les substitutions 06.13.24, 01.23.46 permutables à ω et à ζ transformant ρ_1 respectivement en ρ_2 et en ρ_3, on peut se borner à considérer ρ_3 et supprimer l'indice; les relations $\rho\lambda\rho = \lambda^3$, $\rho\mu\rho = \lambda\mu^3$ [ou $(\rho\lambda)^2 = 1$, $(\rho\mu)^2 = \lambda$], $(\zeta\rho)^3 = 1$ assurent d'ailleurs l'existence de $\mathfrak{F}$ défini par ces équations jointes à celles de ε. S'il existe une s_2, $\sigma = (9a)\ldots$ telle que, dans $\{\mathfrak{F}, \sigma\} = \mathcal{G}'$, $\mathfrak{F}$ soit le diviseur fixant a, on peut supposer, $\mathcal{G}'$ étant quatre fois transitif, σ semblable à λ^2 et fixant 7, 8. $\lambda^2\sigma$ et $\zeta\sigma$ étant d'ordre 2 et $\rho\sigma$ d'ordre 3, σ fixe 5, a exactement un cycle commun avec λ^2 et ζ, mais aucun avec ρ, d'où, pour σ, les deux formes

$$\sigma_1 = 9a.02.14.36, \qquad \sigma_2 = 9a.01.23.46.$$

La substitution $06.13.24$ permutable à Ω, ζ, ρ transformant σ_1 en σ_2, on peut se borner à considérer σ_1 et supprimer l'indice; les relations $\sigma\lambda\sigma = \lambda\mu$, $\sigma\mu\sigma = \mu^3$, $(\sigma\zeta)^2 = (\sigma\rho)^3 = 1$ assurent d'ailleurs l'existence de $\mathcal{G}'$ défini par ces équations jointes à celles de $\mathcal{G}$. $\mathcal{G}'$ contenant $\alpha = \sigma\rho\zeta\lambda$ contient forcément β (**6**); il contient aussi $\gamma = \alpha^4\zeta\rho\mu\lambda^2\zeta\mu\lambda$. Donc $\mathcal{G}' \geqq \mathcal{G}$. D'ailleurs le diviseur de $\mathcal{G}'$ qui fixe a, 9, 8 est $\leqq$ au diviseur analogue de $\mathcal{G}$. Donc $\mathcal{G}' = \mathcal{G}$. On vérifie aisément que, pour tout autre système de déterminations de ζ, ρ, σ, $\mathcal{G}'$ est $\neq \mathcal{G}$.

γ_9 n'est certainement pas dans $\mathcal{G}$ comme le dit Mathieu, car

$$\rho\zeta\lambda\mu\gamma_9\rho\sigma\lambda\zeta = 03415\,76$$

devrait être dans Ω. Mais si l'on pose

$$(\gamma_9\alpha^3)^2 = \delta', \qquad \beta^{-1}\gamma_9\alpha^2\beta = \varepsilon' = 1084.2563,$$
$$\delta'^2(\gamma_9\alpha^6)^9 = \theta', \qquad \varepsilon'^{-1}\theta'\varepsilon' = \lambda' = 0425.1673,$$
$$(\theta'^2\delta'\lambda')^{-1}\delta'(\theta'^2\delta'\lambda')\varepsilon' = \mu' = 1072.3465,$$

on voit que $\{\alpha, \beta, \gamma_9\} = G_9$ est quatre fois transitif et que $\Omega' = \{\lambda', \mu'\}$ est $\leqq$ au diviseur de G_9 qui fixe a, 9, 8. En posant encore

$$\zeta' = 87.03.25.46, \qquad \rho' = 98.06.23.45, \qquad \sigma' = a9.02.35.46,$$
$$\{\Omega', \zeta', \rho', \sigma'\} = \mathcal{G}'', \qquad \omega = 104265,$$

$\mathcal{G}''$ contient $\gamma_9 = \mu'^3\zeta'\rho'\lambda'^3\zeta'\lambda'\sigma'\rho'$ et $\alpha = \sigma'\rho'\zeta'\mu'^3$, donc β, et l'on a

$$\mathcal{G}'' = G_9, \qquad \omega^{-1}\Omega\omega = \Omega',$$
$$\omega^{-1}\zeta\omega = \zeta', \qquad \omega^{-1}\rho\omega = \rho', \qquad \omega^{-1}\sigma\omega = \sigma',$$

c'est-à-dire que $\mathcal{G}''$ est semblable à $\mathcal{G}$.

S'il existe une s_2, $\tau = (ab)\ldots$ telle que, dans $\{\mathcal{G}, \tau\} = \mathfrak{H}$, $\mathcal{G}$ soit le diviseur fixant b, on peut supposer τ semblable à λ^2 et fixant 9, 8, 7. Comme $\tau\lambda^2$, $\tau\zeta$, $\tau\rho$ sont d'ordre 2 et $\tau\sigma$ d'ordre 3, τ a un cycle commun avec λ^2, ζ, ρ et aucun avec σ; d'où, pour τ, la forme unique

$$\tau = ab.06.13.24.$$

Les relations $\tau\lambda\tau = \lambda^2$, $\tau\mu\tau = \lambda\mu$, $(\tau\zeta)^2 = (\tau\rho)^2 = (\tau\sigma)^2 = 1$ assurent l'existence de $\mathfrak{H}$, qui est unique et défini par ces équations, jointes à celles de $\mathcal{G}$. Si l'on convient d'écrire b pour ∞, a pour 10, on aura

$$(z, -z^{-1}) (\mathrm{mod}\, 11) = 0b.1a.25.37.48.69 = \alpha^{-1}\tau\lambda\zeta\mu^3\rho\zeta\lambda\alpha;$$

donc $\mathfrak{H}$ contenant $(z+1)$, $(i^2 z)$, $(-z^{-1})$ contient $v(2, 11)$.

Soit Γ un g^{11} ne contenant pas l'alterné. $(\Gamma, 1)$ divisera

$$11! : 2.3.5.7 = 4.6.8.9.10.11$$

et aura la forme $11d(11k+1)$, d divisant 10 (*cf.* Cole, *Q. J.*, 1894, p. 45). Dans le g^{10} fixant un symbole, les s_3 ont deux cycles : donc les substitutions permutables à un g_3 dans ce g^{10} forment un groupe dont l'ordre 5δ divise 5.4 (4) et l'ordre du g^{10} a la forme $5\delta(5\varkappa+1)$. Si Γ ne divise pas le métacyclique, il contiendra G ($\mathcal{G}$ contient G) et δ sera ≥ 2, donc $= 2$ ou 4. Les seuls ordres multiples de 660 remplissant ces conditions sont 110.72, 110.96. Si Γ est pair, $d = 5$ et 110.72 est seul admissible : mais alors $\delta = 4$ et l'on retombe sur $\mathcal{G}$. Donc, G et $\mathcal{G}$ sont les seuls g^{11} pairs d'ordre > 11.10 et $< \frac{1}{2}11!$ L'ordre d'un g^{11} impair non symétrique devrait donc être, s'il dépasse 110, $2(\mathrm{G}, 1)$ ou $2(\mathcal{G}, 1)$: ces deux nombres étant $\neq 110.96$, G *et* $\mathcal{G}$ *sont les seuls* g^{11} *d'ordre* > 11.10 *et* $< \frac{1}{2}11!$.

On sait déjà que G et $\mathcal{G}$ étant pairs sont simples. Si $\mathfrak{H}$ avait un diviseur normal $\mathrm{A} < \mathfrak{H}$, on aurait $\mathfrak{H} = \mathcal{G}\mathrm{A}$; $\mathcal{G}$ simple devrait être premier à A; mais A, quatre fois transitif et normal, contenant, par suite, tous les g^{11} de $\mathfrak{H}$, contient ceux de $\mathcal{G}$ et ne peut être premier avec lui. *Donc* $\mathfrak{H}$ *est simple.* $\mathfrak{H}$ *est maximum dans le* g^{12} *alterné*, car si $\mathfrak{H}'$ était un $g^{12} > \mathfrak{H}$, le g^7 fixant cinq symboles dans $\mathfrak{H}'$ serait > 1 et la classe de $\mathfrak{H}'$, cinq fois transitif, serait $< 2.5 - 2$.

Dans $\mathfrak{H}$, une s_i ne peut être permutable à un g_{11} pour $i = 2, 3$, car on aurait un $g_{i.11}$ produit direct d'un g_i par un g_{11}, donc cycliques représenté en douze symboles, ce qui ne se peut. Cela exige qu'il y ait $2^2.3.5$ ou $2^6.3^3 = 1728$ g_{11}. Dans le premier cas, chacun est normal dans un $g_{2^2.11}$ qui devrait contenir 11 g_{2^2} dont deux auraient un plus grand commun diviseur d'ordre 2^2 normal dans un $g_{2^2.11}$ abélien con-

tenant un $g_{2.11}$ cyclique. *Il y a donc* 1728 g_{11}. De même une s_i ne peut être permutable à un g_3 pour $i = 3, 11$ et *cela exige qu'il y ait dans* $\mathfrak{H}$ $2376 g_3$. Donc, les g_3 étant de classe 10, chaque g^{10}_{720} qui fixe deux symboles en contient $2376 : \frac{12.11}{2} = 36$ dont le plus petit commun multiple *simple* est d'ordre $5.d.36$, d étant égal à 2 ou 4 (6). Si donc le g^{10}_{720} n'est pas simple, il contient un g^{10}_{360} simple. Or un g_{720} est toujours composé (*cf.* BURNSIDE, *P. L. M. S.*, t. XXVI, p. 334) et tout g_{360} simple est isomorphe au g^6 alterné. Mais le g^{10}_{720} n'est pas isomorphe au g^6 symétrique, car il ne contient pas de s_6; en effet, une s_6 paire, de degré ≥ 8 et ≤ 10, contient ou 1 cycle de 6 symboles et 1 de 2, ou 2 cycles de 3 et 2 de 2; dans les deux cas son carré est de degré < 8. Une s_i ne peut être permutable à un g_{27} pour $i = 5, 11$; cela exige que le nombre des g_{27} soit 5.11, $2^2.5.11$, $2^4.5.11 = 880$ ou $2^6.5.11$. Or un des g_{27}, P, est engendré par

$$\zeta\lambda^2 = 034.126.578 \qquad = \varphi,$$
$$\zeta(\lambda\zeta)^2 = 086.135.247 \qquad = \chi,$$
$$\tau\sigma\zeta(\mu\zeta)^2 = 076.138.245.ab9 = \psi$$

et défini par $\varphi^3 = \chi^3 = \psi^3 = 1$, $\varphi\chi = \chi\varphi$, $\psi^{-1}\varphi\psi = \varphi$, $\psi^{-1}\chi\psi = \chi\varphi^2$. Le groupe $\{\varphi\}$ des opérations normales de P ne peut être normal dans un $g_{3.2^k}$ pour $k > 4$ (4). Donc les deux premiers membres sont à rejeter. Comme $\tau P \tau = P$, le dernier est inadmissible, car P ne serait permutable qu'à ses opérations. *Il y a donc, dans* $\mathfrak{H}$, 880 g_{27}. Tout g_{60} de $\mathfrak{H}$ est conjugué de $\{\varepsilon, \rho, \tau\} = Q$. Le groupe $\{\lambda^2, \rho\}$ des opérations normales de Q ayant pour systèmes d'intransitivité 1, 2, 3, 4; 0,6; 5, 7; 8, 9; a, b ne peut être permutable à une s^{10}_5, ni à une s^{11}_1, ni à une s^9_3. *Il y a donc dans* $\mathfrak{H}$ $3^3.5.11 = 1485$ g_{60} (*cf.* BURNSIDE, *Theory of groups*, p. 220).

10. Soit $q = 23$. On a $t = 5$, et, en écrivant respectivement pour

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22,
v, x, y, b, p, g, q, e, s, c, d, r, f, n, k, i, m, h, o, l, t, a, u,

$$\alpha = vxybpgqescdrfnkimholtau,$$
$$\beta = xypsmconbqf.gdthrualiek.v.$$

γ est d'ordre 2, 5 ou 10, et, pour chacun de ces ordres, γ étant supposé fixer x est complètement déterminé par le symbole du second cycle de β qu'il fixe. Une fois l'ordre de γ choisi, j'écrirai $\gamma_g, \gamma_d, \ldots, \gamma_k$ pour les déterminations de γ qui fixent $g, d, \ldots, k$ respectivement. Ainsi, pour γ d'ordre 10, on a

$$\gamma_g = ypmbcfqnso.dtriukelha,$$
$$\gamma_d = ypmbcfqnso.thueagkirl,$$
$$\gamma_t = ypmbcfqnso.hrakldgeui,$$
$$\gamma_h = ypmbcfqnso.rulgitdkae,$$
$$\gamma_r = ypmbcfqnso.uaidehtglk,$$
$$\gamma_u = ypmbcfqnso.aletkrhdig,$$
$$\gamma_a = ypmbcfqnso.likhgurted,$$
$$\gamma_l = ypmbcfqnso.iegrdauhkt,$$
$$\gamma_i = ypmbcfqnso.ekdutlargh,$$
$$\gamma_e = ypmbcfqnso.kgtahiludr,$$
$$\gamma_k = ypmbcfqnso.gdhlreiatu.$$

Si γ est d'ordre 2, on vérifie directement que $(\alpha\gamma_g)^{52}$, $(\alpha\gamma_d)^{13}$, $(\alpha^3\gamma_t)^{9}$, $(\alpha\gamma_h)^{77}$, $(\alpha^2\gamma_r)^{33}$, $(\alpha^7\gamma_u)^{3}$, $(\alpha^3\gamma_a)^{12}$, $(\alpha^4\gamma_l)^{91}$, $(\alpha^3\gamma_i)^{12}$, $(\alpha\gamma_e)^{12}$, $(\alpha\gamma_k)^{17}$ sont des substitutions circulaires des degrés respectifs 3, 13, 13, 5, 5, 7, 11, 5, 5, 5, 5. Donc pour γ d'ordre 2, $\{\alpha, \beta, \gamma\}$ contient l'alterné. Il en est de même *a fortiori* si γ est d'ordre 10. Si γ est d'ordre 5, $(\alpha\gamma_d)^{16}$, $(\alpha\gamma_t)^{36}$, $(\alpha\gamma_h)^{19}$, $(\alpha\gamma_r)^{9}$, $(\alpha\gamma_u)^{5}$, $(\alpha^4\gamma_a)^{19}$, $(\alpha\gamma_l)^{17}$, $(\alpha^2\gamma_i)^{16}$, $(\alpha^3\gamma_e)^{6}$ sont des substitutions circulaires des degrés respectifs 3, 7, 3, 11, 11, 3, 5, 3, 13. Il reste donc seulement à essayer $\gamma = \gamma_g$, $\gamma = \gamma_k$.

Prenons d'abord $\gamma_k = ymeqs.pbfno.ghrit.dleau.x.v.k$. On a, en supprimant l'indice k,

$$\alpha^{-1}\gamma\alpha = bhdec.gpnkl.qofma.rtsuv.y.x.i;$$

donc le diviseur de $\{\alpha, \beta, \gamma\} = G$ qui fixe x est transitif;

$$\alpha^{-1}\beta\gamma\alpha = afrqt.bpcdg.eknyh.iomus.v.x.l = \delta$$

montre que le diviseur fixant x, ρ est transitif, et

$$\delta^{-2}\gamma\delta^2 = esgao.dcqhu.pktmf.blnri.\rho.x.y = \varepsilon,$$
$$\gamma\delta\gamma^{-1} = ebhci.pomut.lkfsg.rnyaq.\rho.z.d = \varkappa,$$
$$\delta^{-1}\varkappa = aph.blk.coc.dig.fqn.rst.\rho.x.y.u.m = m_0$$

que le diviseur fixant ρ, x, y est transitif. *Donc* G *est quatre fois transitif.* Les substitutions

$$\varkappa^{-1}\delta\varepsilon^{-2}(\varkappa^2\gamma^2)^2\varepsilon^2\delta^{-1}\varkappa = a_1 = ab.cf.dg.eh.im.kn.lo.pq,$$
$$\varepsilon^{-2}(\varkappa^2\gamma^2)^2\varepsilon^2 a_1 = a_2 = ac.bf.di.ek.gm.hn.lp.oq,$$
$$\delta^{-1}\varkappa(\varepsilon^2\varkappa^2\gamma^2)\varkappa^2 = a_3 = ad.bg.ci.el.fm.ho.kp.nq,$$
$$(\delta^{-1}\varkappa)^2\varepsilon^2\varkappa^2\gamma^2 = a_4 = ae.bh.ck.dl.fn.go.ip.mq,$$
$$a_1 a_4\delta^{-1}\varkappa = a_0 = rst.bcf.del.hpm.ino.kqg$$

engendrent un g_{48}^{10} B où le diviseur normal $A = \{a_1, a_2, a_3, a_4\}$ est représenté régulièrement, a, b, c, d, e, f, g, h, i, k, l, m, n, o, p, q étant mis respectivement pour 1, a_1, a_2, a_3, a_4, a_1a_2, a_1a_3, a_1a_4, a_2a_3, a_2a_4, a_3a_4, $a_1a_2a_3$, $a_1a_2a_4$, $a_1a_3a_4$, $a_2a_3a_4$, $a_1a_2a_3a_4$, en sorte que l'on peut écrire $(x_i, \xi_i = 0, 1)$

$$a_1^{\xi_1}a_2^{\xi_2}a_3^{\xi_3}a_4^{\xi_4} = (a_1^{x_1}a_2^{x_2}a_3^{x_3}a_4^{x_4},\ a_1^{x_1+\xi_1}a_2^{x_2+\xi_2}a_3^{x_3+\xi_3}a_4^{x_4+\xi_4}),$$
$$a_0 = (a_1^{x_1}a_2^{x_2}a_3^{x_3}a_4^{x_4},\ a_1^{x_1}a_2^{x_1+x_2}a_3^{x_4}a_4^{x_1+x_4})(rst),$$

ou, plus brièvement, si l'on désigne $a_1^{x_1}a_2^{x_2}a_3^{x_3}a_4^{x_4}$ par le point (x_1, x_2, x_3, x_4),

$$a_1^{\xi_1}a_2^{\xi_2}a_3^{\xi_3}a_4^{\xi_4} = (x_i, x_i + \xi_i),$$
$$a_0 = (x_1, x_2, x_3, x_4;\ x_2, x_1 + x_2, x_4, x_3 + x_4).$$

Les équations de B sont

$$a_0^3 = a_i^2 = 1, \qquad a_i a_k = a_k a_i (i, k = 1, 2, 3, 4),$$
$$a_0^{-1}a_1a_0 = a_2, \quad a_0^{-1}a_2a_0 = a_1a_2, \quad a_0^{-1}a_3a_0 = a_4, \quad a_0^{-1}a_4a_0 = a_3a_4,$$

d'où résulte que *toute opération de* A $a_0^{x_0}(x_0 = 1, 2)$ *est d'ordre* 3. On

observera aussi que $a_1^{r_1}a_2^{r_2}a_3^{r_3}a_4^{r_4}$ fait partie d'un seul groupe quadratique normal dans B, engendré par $a_1^{r_1}a_2^{r_2}a_3^{r_3}a_4^{r_4}$ et son transformé par a_0, $a_1^{r_1}a_2^{r_1+r_2}a_3^{r_3}a_4^{r_3+r_4}$. Deux groupes quadratiques Q_i, Q_k normaux dans B sont donc premiers entre eux et $Q_iQ_k = A$. Il y a dans A cinq diviseurs quadratiques normaux dans B,

$$Q_1 = \{a_1, a_2\}, \qquad Q_2 = \{a_3, a_4\},$$
$$Q_3 = \{a_1a_3, a_2a_4\}, \quad Q_4 = \{a_1a_4, a_2a_3a_4\}, \quad Q_5 = \{a_2a_3, a_1a_2a_4\}.$$

Les substitutions de A sont, avec l'unité,

$$a_1 = ab.\ cf.\ dg.\ eh.\ im.\ kn.\ lo.\ pq,$$
$$a_2 = ac.\ bf.\ di.\ ek.\ gm.\ hn.\ lp.\ oq,$$
$$a_3 = ad.\ bg.\ ci.\ el.\ fm.\ ho.\ kp.\ nq,$$
$$a_4 = ae.\ bh.\ ck.\ dl.\ fn.\ go.\ ip.\ mq,$$
$$a_1a_2 = af.\ be.\ dm.\ en.\ gi.\ hk.\ lq.\ op,$$
$$a_1a_3 = ag.\ bd.\ cm.\ eo.\ fi.\ hl.\ kq.\ pn,$$
$$a_1a_4 = ah.\ be.\ cn.\ do.\ fk.\ gl.\ iq.\ mp,$$
$$a_2a_3 = ai.\ bm.\ cd.\ ep.\ fg.\ hq.\ kl.\ no,$$
$$a_2a_4 = ak.\ bn.\ ce.\ dp.\ fh.\ gq.\ il.\ mo,$$
$$a_3a_4 = al.\ bo.\ cp.\ de.\ fq.\ gh.\ ik.\ mn,$$
$$a_1a_2a_3 = am.\ bi.\ cg.\ df.\ eq.\ hp.\ ko.\ ln,$$
$$a_1a_2a_4 = an.\ bk.\ ch.\ dq.\ ef.\ gp.\ io.\ lm,$$
$$a_1a_3a_4 = ao.\ bl.\ cq.\ dh.\ eg.\ fp.\ in.\ km,$$
$$a_2a_3a_4 = ap.\ bq.\ cl.\ dk.\ ei.\ fo.\ gn.\ hm,$$
$$a_1a_2a_3a_4 = aq.\ bp.\ co.\ dn.\ em.\ fl.\ gk.\ hi.$$

Les substitutions de Aa_0 sont

$$a_0 = rst.\ bcf.\ del.\ hpm.\ ino.\ kqg = a_0,$$
$$a_1a_0 = rst.\ acb.\ dko.\ epg.\ hli.\ mnq = f_0,$$
$$a_2a_0 = rst.\ afc.\ dnp.\ eqi.\ gho.\ klm = b_0,$$

$$a_3a_0 = rst.aed.\ bkm.cng.\ fhi.\ opq = l_0,$$
$$a_1a_0 = rst.ale.\ bpn.\ cqh.\ fok.\ gim = d_0,$$
$$a_1a_2a_0 = rst.abf.\ dhq.com.\ gnl.\ ikp = c_0,$$
$$a_1a_3a_0 = rst.akg.\ bei.\ chd.\ fnm.\ lpo = q_0,$$
$$a_1a_4a_0 = rst.aph.\ blk.\ coe.\ dig.\ fqn = m_0,$$
$$a_2a_3a_0 = rst.ani.\ bhg.cem.\ dfk.\ lqp = o_0,$$
$$a_2a_4a_0 = rst.aqk.\ boh.\ cln.\ dmi.\ efp = g_0,$$
$$a_3a_4a_0 = rst.adl.\ biq.\ cmo.\ fgp.\ hkn = e_0,$$
$$a_1a_2a_3a_0 = rst.ahm.bnd.\ cki.\ egf.\ loq = p_0,$$
$$a_1a_2a_4a_0 = rst.aon.\ bqe.\ cpk.\ dgm.\ flh = i_0,$$
$$a_1a_3a_4a_0 = rst.aio.\ bdp.\ cgl.\ ekh.\ fmq = n_0,$$
$$a_2a_3a_4a_0 = rst.amp.bgo.\ cdq.\ enk.\ fil = h_0,$$
$$a_1a_2a_3a_4a_0 = rst.agq.\ bml.\ cip.\ dof.\ ehn = k_0;$$

celles de A a_0^2 sont leurs inverses.

Je dis que B est le diviseur de G qui fixe u, v, x, y. Pour le voir, cherchons à construire un groupe quatre fois transitif où B soit le diviseur fixant u, v, x, y. Soit C un $g^{20}_{20.18}$ transitif où B soit le diviseur fixant u. Le nombre λ des g_5 de C sera 1, 6, 16 ou 96. Or λ est $\neq 1$ et $\neq 16$, sans quoi un g_5 à quatre systèmes d'intransitivité serait permutable à une s_3^{15} (4) et la classe est 16. λ est $\neq 6$ sans quoi un g_5 serait normal dans un $g_{5.32}$ qui devrait contenir une s_2^{10} (le groupe Σ du n° 4 étant ici isomorphe à un g_8 du g^4 symétrique). Donc $\lambda = 96$. Le nombre μ des g_3 de C est 1, 10, 40 ou 160. Or $\{a_0\}$ n'étant permutable dans B qu'à ses substitutions, les substitutions permutables à $\{a_0\}$ dans C seront de la forme $(ua)j$, $(ua)j'$, ..., j, j', ... étant dans le champ de B. jj' étant donc permutable à $\{a_0\}$ dans le champ de B, on a $j' = j^{-1}a_0$ ou $j^{-1}a_0^2$. Il n'y a donc hors de $\{a_0\}$ que trois substitutions permutables à $\{a_0\}$. Le groupe des substitutions permutables à $\{a_0\}$ étant d'ordre 6, $\mu = 160$. Le nombre ν des g_{60} est 1, 3, 5 ou 15. Or ν est $\neq 1$, car il y a au moins 75 s_2^{16} dans les 5 conjugués de A (A est unique de son ordre dans chacun des $4g^{19}$ fixant un des sym-

boles r, s, t, u). ν est $\neq 3$, car un g_{64} serait normal dans un $g_{5.64}$ qui devrait avoir un diviseur Δ normal dans C, tel que $C|\Delta$ soit représentable en g^5, ce qui ne se peut (Δ dont l'ordre diviserait $2^6.5$ devrait contenir les 96 g_5 de C). Enfin ν est $\neq 15$. En effet, 64 n'étant divisible par aucun des nombres 17, 18, 19, 20, tout g_{64} de C est intransitif et a un système d'intransitivité de 16 symboles (A est transitif). Le plus grand commun diviseur d'un g_{64} et de son constituant de degré 16 est un g^{16} contenu dans un g^{19}, donc conjugué de A. Soient P un g^{64} contenant (normalement) A et a_{0r}, a_{0s}, a_{0t} des conjuguées de a_0 dans les 3 g^{19} fixant r, s, t respectivement, lesquels contiennent normalement A. Si $\nu = 15$, P n'est permutable qu'à ses opérations et deux, w, w', des 9 substitutions 1, $a_0^{\pm 1}$, $a_{0r}^{\pm 1}$, $a_{0s}^{\pm 1}$, $a_{0t}^{\pm 1}$ ne pouvant transformer P en un même conjugué (car $w^{-1}w' \neq 1$ serait permutable à P), on a 9 conjugués de P ayant le système d'intransitivité $a, b, \ldots, q$. Mais les g^{19} fixant un symbole de C se partagent en 5 systèmes de 4 groupes ayant pour plus grand commun diviseur un g_{16}^{16} dont le champ forme un système d'intransitivité commun à 9 g_{64}. Il y aurait donc 45 g_{64} et non 15. Donc $\nu = 5$. Un g_{64} devra contenir un diviseur normal Δ de degré ≥ 8, car, $C|\Delta$ étant représentable en g^5, $(C|\Delta, 1)$ doit diviser 5! D'ailleurs $(\Delta, 1)$ est > 8, sans quoi $C|\Delta$ serait isomorphe au g_{120}^5 symétrique, C aurait un diviseur normal X d'indice 2 et la relation $C = BX$ exigerait dans B un g_{24} normal qui devrait contenir les 32 s_3 de B. Enfin $(\Delta, 1)$ est < 32, sans quoi $C|\Delta$ serait représentable en g_{30}^5 et il n'y a pas de g_{30}^5 (un g_{30}^5 devrait contenir des s_3^3). Donc $(\Delta, 1) = 16$. Comme un g_{64} contenant A est $\geq A\Delta$, A et Δ ont un plus grand commun diviseur $\mathfrak{D}$ d'ordre ≥ 4 qui, étant aussi le plus grand commun diviseur de B, Δ, est normal dans B. D'ailleurs $(\mathfrak{D}, 1)$ est < 8, sans quoi Δ ayant, avec les 5 conjugués de A, 5 plus grands communs diviseurs premiers entre eux deux à deux serait d'ordre > 35. Donc $\mathfrak{D}$ est un des Q_i. Les plus grands communs diviseurs $\mathfrak{D} = \mathfrak{D}_1, \mathfrak{D}_2, \mathfrak{D}_3, \mathfrak{D}_4, \mathfrak{D}_5$ de Δ avec les 5 conjugués de A dans C sont conjugués et premiers entre eux deux à deux; $\Delta = \Sigma \mathfrak{D}_i$ ayant tous ses éléments d'ordre 2 est abélien. Δ normal dans C déplace tous les symboles et permute exclusivement entre eux les symboles fixés par chacun des conjugués de A et a, par suite, 5 ou 10 systèmes d'intransitivité qui sont des systèmes d'imprimitivité de C. D'ailleurs B, qui est le diviseur

fixant a, n'est pas maximum dans C, puisque BΔ d'ordre $16.48:4$ est $>$ B et $<$ C. BΔ, d'indice 5 dans C, y est maximum et la représentation du groupe simple C|Δ relative à BΔ|Δ est semblable au g^5 alterné.

En transformant au besoin par l'inverse d'une substitution telle que

$$\mu_{\alpha\beta} = \begin{vmatrix} x_1 & \alpha_1 x_1 + \alpha_2 x_2 & + \beta_1 x_3 + \beta_2 x_4 \\ x_2 & \alpha_2 x_1 + (\alpha_1 + \alpha_2) x_2 + \beta_2 x_3 + (\beta_1 + \beta_2) x_4 \\ x_3 & \alpha_3 x_1 + \alpha_4 x_2 & + \beta_3 x_3 + \beta_4 x_4 \\ x_4 & \alpha_4 x_1 + (\alpha_3 + \alpha_4) x_2 + \beta_3 x_3 + (\beta_3 + \beta_4) x_4 \end{vmatrix}$$

qui est permutable à A et à a_0, donc à B et qui transforme respectivement a_1, a_2, a_3, a_4 en $a_1^{\alpha_1} a_2^{\alpha_2} a_3^{\alpha_3} a_4^{\alpha_4} = a'_1$, $a_1^{\alpha_1} a_2^{\alpha_1+\alpha_2} a_3^{\alpha_3} a_4^{\alpha_3+\alpha_4} = a'_2$, $a_1^{\beta_1} a_2^{\beta_2} a_3^{\beta_3} a_4^{\beta_4} = a'_3$, $a_1^{\beta_1} a_2^{\beta_1+\beta_2} a_3^{\beta_3} a_4^{\beta_3+\beta_4} = a'_4$, donc Q_1, Q_2 en $Q_2 = \{a'_1, a'_2\}$, $Q_3 = \{a'_3, a'_4\}$, on peut supposer que $\omega = Q_1$.

Les systèmes d'intransivité de Δ seront comme ceux de Q_1 de degré 4 et Δ en aura 5 : a, b, c, f; d, g, i, m; e, h, k, n; l, o, p, q; r, s, t, u. Dans Δ tout conjugué Q' de Q_1, autre que Q_1, contient trois substitutions des formes *rs.tu. ...*, *rt.su. ...*, *ru.st. ...*, qui s'obtiennent évidemment en transformant l'une d'elles par une s_3 de B qui permute exclusivement entre eux les symboles du système d'intransitivité fixé par Q'. Puisque $\Delta = Q_1 Q'$, *une seule substitution de* Δ *hors de* B *déterminera* Δ. Δ contient trois substitutions des formes *ru.st.ab.cf. ...*, *ru.st.ac.bf. ...*, *ru.st.af.be. ...*, car il contient certainement l'une d'elles et ses produits par a_1, a_2, $a_1 a_2$. Considérons une substitution $\xi = ru.st.ab.cf. ....$ Supposons que ξ fixe l, o, p, q. Son effet sur d, g, i, m sera *di.mg* ou *dm.ig*, sans quoi ξa_1 serait de degré < 16; son effet sur e, h, k, n sera respectivement *en.hk* ou *eh.kn*, sans quoi ξa_2 ou $\xi a_1 a_2$ respectivement serait de degré < 16; mais dans le second cas $l_0^{-1} \xi l_0 \xi$ est de degré < 16. *Donc si* ξ *fixe* l, o, p, q, ξ *a la forme*

$$\xi_1 = ru.st.ab.cf.di.mg.en.hk.$$

Le diviseur Q'_1 conjugué de Q_1 dont ξ_1 fait partie est $\Sigma_j l_0^{-j} \xi_1 l_0^j = \{\xi_1, \eta\}$, en posant $\eta = l_0^{-1} \xi l_0$, et Δ a la forme $\Delta_1 = Q_1 Q'_1$. Si ξ fixe e, h, k, n

ou d, g, i, m, on verrait de même, en se servant respectivement de e_0, d_0 au lieu de l_0, que ξ a respectivement les formes

$$\xi_2 = ru.st.ab.cf.dm.gi.lp.oq, \qquad \xi_3 = ru.st.ab.cf.ek.hn.lq.op,$$

et Δ les formes $\Delta_2 = Q_1 \Sigma_j e_0^{-j} \xi_2 e_0^j$, $\Delta_3 = Q_1 \Sigma_j d_0^{-j} \xi_3 d_0^j$. Comme les substitutions $rst = \lambda$ et λ^2 permutables à chaque substitution de B transforment respectivement ξ_2 en $a_2\eta$ et ξ_3 en $a_1 a_2 \xi\eta$, donc Δ_2, Δ_3 en Δ_1, il suffit de considérer Δ_1 et j'écrirai Δ, ξ pour Δ_1, ξ_1.

Les substitutions de Δ sont

$$ru.st.ab.cf.di.gm.en.hk = \xi, \qquad ru.ts.dm.gi.ck.hn.lo.pq = a_1\xi,$$
$$rt.su.af.bc.dg.im.ek.nh = \eta, \qquad rt.su.di.mg.eh.kn.lq.op = a_1 a_2 \eta,$$
$$rs.tu.ac.bf.dm.ig.eh.kn = \xi\eta, \qquad rs.tu.dg.im.en.hk.lp.oq = a_2 \xi\eta,$$
$$ru.st.af.bc.eh.kn.lp.op = a_2\xi, \qquad ru.ts.ac.bf.dg.im.lq.op = a_1 a_2 \xi,$$
$$rt.su.ac.bf.en.hk.lo.pq = a_1\eta, \qquad rt.su.ab.cf.dm.gi.lp.oq = a_2\eta,$$
$$rs.tu.ab.cf.ek.hn.lq.op = a_1 a_2 \xi\eta, \qquad rs.tu.af.bc.di.gm.lo.pq = a_1\xi\eta,$$

et celles de $Q_1 = \{a_1, a_2\}$. Les seuls diviseurs de Δ qui fixent 4 symboles fixent les 4 symboles d'un système d'intransitivité. *Donc les 5 conjugués de* A *dans* C *fixent chacun les* 4 *symboles d'un système d'intransitivité de* Δ. BΔ étant maximum dans C, il suffit pour engendrer C d'adjoindre à BΔ une substitution étrangère à BΔ. Cherchons pour cela à former le conjugué A_1 de A qui a avec Δ le plus grand commun diviseur $\{\xi, \eta\}$ et qui par suite fixe l, o, p, q. A_1 contient une substitution $\zeta = (rb)\ldots$. Pour que $\xi\zeta\xi = \zeta$, il faut que $\zeta = ua.rb.\ldots$. Pour que $\eta\zeta\eta = \zeta$, il faut que $\zeta = ua.rb.ct.fs. \ldots ; \zeta \{a_0\} \zeta$ fixant u et a est dans B et dans $\{a_0\}$; comme $\zeta a_0 \zeta = bcf. \ldots$, $\zeta a_0 \zeta = a_0^2$, ce qui exige, ζ fixant l, o, p, q, que

$$\zeta = ua.rb.ct.fs.de.hm.in.gk.$$

A_1 contient de même $\zeta' = rd.ui.tg.sm. \ldots$, et puisque $\zeta\zeta' = \zeta'\zeta$,

$$\zeta' = rd.ui.tg.sm.an.be.ck.fh \qquad \text{et} \qquad A_1 = \{\xi, \eta, \zeta, \zeta'\}.$$

Comme B a deux systèmes d'intransitivité $a, b, \ldots, q$; r, s, t, et que $\xi = ur.\ldots, \zeta = ua.\ldots$, il faut et il suffit (1) pour l'existence de C que $B + B\xi B + B\zeta B$ forme un groupe qui sera C. Or les relations faciles à vérifier : $\xi^2 = 1$, $\xi a_1 \xi = a_1$, $\xi a_2 \xi = a_2$, $\xi a_3 \xi = a_1 a_2 a_3$, $\xi a_4 \xi = a_2 a_4$, $\xi a_0 \xi = a_0^2 \xi a_0^2$, donnent $\xi A \xi = A$, $\xi A a_0 \xi = A a_0^2 \xi a_0^2$. Donc $\xi B \xi$ est dans $B\xi B$, et l'on voit déjà que $B + B\xi B$ est le groupe $|B, \xi| = B\Delta$, où B est le diviseur fixant u, $B\Delta$ étant défini par les équations précédentes jointes à celles B. On remarquera que $|A, \xi, \eta|$ est un g^{6^1} d'équations

$$a_i^2 = \xi^2 = \eta^2 = 1, \qquad a_i a_k = a_k a_i \quad (i = 1, 2, 3, 4), \qquad \xi\eta = \eta\xi,$$

$$(1)\quad \xi a_1 \xi = a_1, \quad \xi a_2 \xi = a_2, \quad \xi a_3 \xi = a_1 a_2 a_3, \quad \xi a_4 \xi = a_2 a_4,$$

$$(2)\quad \eta a_1 \eta = a_1, \quad \eta a_2 \eta = a_2, \quad \eta a_3 \eta = a_2 a_3, \quad \eta a_4 \eta = a_1 a_4.$$

$\mathfrak{B}$ est normal dans $B\Delta$, car on a ($l_0 = a_3 a_0 = a_0 a_4$) :

$$(3)\qquad a_0^{-1} \xi a_0 = a_1 \eta a_4, \qquad a_0^{-1} \eta a_0 = a_0 \xi a_0 a_1 a_3,$$

$$(4)\quad a_0^{-1} a_1 a_0 = a_2, \quad a_0^{-1} a_2 a_0 = a_1 a_2, \quad a_0^{-1} a_3 a_0 = a_4, \quad a_0^{-1} a_4 a_0 = a_3 a_4.$$

$B\Delta$ est évidemment aussi défini par les équations de $\mathfrak{B}$ jointes à (3), (4). Mais l'élimination de η fournit immédiatement le système déjà obtenu : la première équation (3) s'écrit $\eta = l_0^{-1} \xi l_0$; la seconde en résulte en vertu de (4), et de même (2) de (1).

On a en outre $\xi\zeta = a_1 \zeta a_1$ d'où $\xi = (a_1\zeta)^2$, $\xi A \zeta = A \xi\zeta = A \zeta a_1$, et puisque $\zeta a_0 \zeta = a_0^2$, $\xi A a_0 \zeta = A \zeta a_1 a_0^2$, $\xi A a_0^2 \zeta = A \zeta a_1 a_0$. Donc $\xi B \zeta$ est dans $B\zeta B$. Enfin

$$\zeta a_0 \zeta = a_0^2, \qquad \zeta a_1 \zeta = a_1 \xi, \qquad \zeta a_2 \zeta = i_0 \xi i_0^2, \qquad \zeta a_3 \zeta = d_0 \zeta d_0^2,$$

$$\zeta a_4 \zeta = e_0^2 \zeta e_0, \qquad \zeta a_3 a_4 \zeta = a_3 a_4 \zeta a_3 a_4.$$

Donc $\zeta a_1 a_2 \zeta$ est dans $B\xi B$ et $\zeta a_1 a_3 \zeta$, $\zeta a_1 a_4 \zeta$, $\zeta a_2 a_3 \zeta$, $\zeta a_2 a_4 \zeta$, $\zeta a_1 a_i a_k \zeta$ $(i, k = 2, 3, 4)$, $\zeta a_2 a_3 a_4 \zeta$, $\zeta a_1 a_2 a_3 a_4 \zeta$ dans $B\zeta B$. On voit donc que C existe et est complètement déterminé par Δ. Comme $\xi = (a_1\zeta)^2$, on a $C = |B, \xi, \zeta| = |B, \zeta|$. Les équations de C résultent de ce qui précède; mais elles peuvent se simplifier. On a

en effet $\zeta d_0 = rpnmc.sokib.tqhgf.uleda$. Donc ζ et d_0, vérifiant $\zeta^2 = d_0^2 = (\zeta d_0)^3 = 1$, engendrent un g_{60} simple I (3) premier au diviseur normal $\Delta = |a_1, a_2, \zeta, \eta|$. En mettant b_1, b_2, b_3, b_4, 0 pour a_1, a_2, ξ, η, d_0 respectivement, le g_{960}^{20} $C = \Delta I$ est défini par

$$b_i^2 = \zeta^2 = 0^3 = (\zeta 0)^5 = 1, \qquad b_i b_k = b_k b_i \quad (i, k = 1, 2, 3, 4),$$

$$\zeta b_1 \zeta = b_1 b_3, \quad \zeta b_2 \zeta = b_2 b_3 b_4, \quad \zeta b_3 \zeta = b_3, \quad \zeta b_4 \zeta = b_4,$$

$$0^{-1} b_1 0 = b_2, \quad 0^{-1} b_2 0 = b_1 b_2, \quad 0^{-1} b_3 0 = b_4, \quad 0^{-1} b_4 0 = b_2 b_4.$$

Cherchons à former un g^{21} E deux fois transitif, où C soit le diviseur fixant ∞. S'il existe, il sera engendré par C et une s_2 $\rho = uv...$ conjuguée de a_1 et déplaçant 14 des 19 lettres $a, \ldots, q, r, s, t$, donc fixant 2 des 16 lettres $a, \ldots, q$ au moins. On peut, en transformant ρ par une substitution de A, faire que l'une de ces 2 lettres soit a. Comme il faut que $\rho B \rho = B$, ρ permute entre elles les lettres r, s, t qui forment un système d'intransitivité de B et en fixe 1 ou 3. S'il en fixait 3, on aurait $\rho a_0 \rho = a$, puisque, ρ fixant a, $\rho_0 |a_0| \rho = |a_0|$; ρ fixant ensuite une des lettres $b, \ldots, q$ fixerait les 3 lettres du cycle de a_0 où elle figure et serait de degré $\leqq 15$. Donc ρ échange 2 des lettres r, s, t, et en transformant au besoin ρ par a_0 ou a_0^2 on peut supposer que $\rho = uv.rs....$ Comme $\rho a_0 \rho = a_0^2$, *2 quelconques des 3 symboles b', c', d' que ρ fixe parmi $b, c, \ldots, q$ ne peuvent se trouver dans un même cycle de a_0*; ρ étant permutable aux 3 s_2 de A, $\beta' = ab' \ldots$, $\gamma' = ac' \ldots$, $\delta' = ad' \ldots$, on a $\delta' = \beta'\gamma'$, sans quoi ρ, permutable à $\beta'\gamma' = ae' \ldots$, fixerait e' et serait de degré $\leqq 15$ (b', c', d' n'étant pas dans un même cycle de a_0, $|\beta', \gamma'|$ n'est pas un des Q_i); *donc chacune des 3 lettres b', c', d' est déterminée par les 2 autres.* Il reste $\frac{5.4}{1.2} \cdot \frac{9}{3} = 30$ manières de choisir b', c', d'. Or ρ transforme chacune des s_3, b_0', c_0', d_0' de B qui fixent respectivement b', c', d', en son carré : donc c' et d' ne sont pas dans un même cycle de b_0' et, si $b_0' = c'e'f'.d'g'h' \ldots$, $\rho = e'f'.g'h' \ldots$. De même d', b' ne sont pas dans le même cycle de c_0' et font connaître 2 *nouveaux* cycles de ρ (c' ne peut avoir 2 cycles formés des lettres b', e', f'; d', g', h', ni 2 cycles formés des lettres b', g', h'; d', e', f' : dans le premier cas, $b_0'c_0'$ ou $b_0'c_0'^2$ fixerait d', g', h'; dans le second, $b_0'c_0'$ serait d'ordre > 4); b', c' et d_0'

font connaître les 2 derniers cycles de ρ. *Ainsi, chacun des* 30 *choix de* 2 *des lettres, b', c', d' détermine* ρ. Mais $\rho\zeta\rho = (a\rho)\ldots$ devant être dans $C\rho C$ sera de la forme

$$(ua\ldots)\rho(ua\ldots) = \zeta\rho\beta''\zeta,$$

β'' étant dans B. Donc $(\rho\zeta)^3$ sera dans B, et comme $\rho\zeta = (a\rho u)\ldots$, $(\rho\zeta)^3$ fixera a, u et sera dans $|a_0|$. Si donc $(\rho\zeta)^3 \neq 1$, $\rho\zeta$ aura 2 cycles de 9 lettres. Or si ρ fixe b, $\rho = uv.rs.cf.a.b.t.\ldots$ et $\rho\zeta = (brftcs)\ldots$. Donc ρ déplace b, et de même c et f. b, c ou f entrant dans 18 des 30 combinaisons b', c', d', il reste 12 déterminations de ρ à essayer. 4 seulement satisfont à la condition que $(\rho\zeta)^3$ soit dans B. Ce sont

$$\rho_1 = uv.rs.bg.cq.el.fk.in.pm.a.d.h.o,$$
$$\rho_2 = uv.rs.bi.co.dl.fn.hp.kg.a.e.m.q,$$
$$\rho_3 = uv.rs.bm.cp.de.fh.gq.on.a.l.i.k,$$
$$\rho_4 = uv.rs.bd.cl.ef.hm.io.kq.a.g.n.p.$$

Les groupes $|C, \rho_i| = E_i$ sont semblables, car la substitution

$$\rho' = rts.bcf.hkn.img.opq$$

permutable à Q_1, Q_2, a_0, ζ, donc à C transforme ρ_1 en $a_0\rho_2 a_0^{-1}$, ρ_2 en $a_0\rho_3 a_0^{-1}$, et $\rho'' = rts.bcf.dig.enk.loq$ permutable à C, transforme ρ_1 en $a_0\rho_4 a_0^{-1}$. Il suffit donc de considérer ρ_1 et j'écrirai ρ, E pour ρ_1, E_1. On a

$$\rho a_1\rho = a_1 a_3, \qquad \rho a_2\rho = a_1 a_2 a_3 a_4, \qquad \rho a_3\rho = a_3,$$

d'où

$$\rho a_4\rho = a_3 a_4, \qquad \rho a_0\rho = a_0^2, \qquad \rho\zeta\rho = \zeta\rho\zeta, \qquad \rho\xi\rho = a_0^2\xi\rho a_0^2\xi a_0,$$

la dernière s'écrivant (puisque $\rho a_0^2 = a_0\rho$) $(\rho\xi a_0)^2 = 1$. Donc

$$\rho\zeta B\rho = \zeta\rho\zeta B, \qquad \rho\xi B\rho = a_0^2\xi\rho a_0^2\xi a_0.$$

Or $\zeta B + \xi B$ contenant des substitutions des formes $ua\ldots$, $ub\ldots$,

$uq\ldots$, $ur\ldots$, $us\ldots$, $ut\ldots$ contient un système de restes de C (mod d B, 1). Donc E répond à la question et est défini par les équations de C jointes à

$$p^2 = (p\zeta)^2 = (pa_2)^2 = (pa_0)^2 = (p\xi a_0)^2 = 1,$$

$$(pa_1)^2 = a_2, \qquad (pa_2)^2 = a_1 a_2 a_4.$$

E *est simple*, car s'il avait un diviseur normal *minimum* $X > 1$, on aurait $E = XC$. Or X n'est pas premier à C, car il serait d'ordre 21 et contiendrait *un seul* g_7, lequel serait normal dans C.

Donc le plus grand commun diviseur de X, C est Δ et $(X, 1) = 16.21$. Mais alors X contiendrait 8 g_7 qui seraient tous ceux de E, et dans E un g_7 serait permutable à une s_5, ce qui est impossible, 5 ne divisant pas $7.6\,(4)$ (*cf.* Miller, *S. M.*, t. XXVIII, 1900, p. 266).

Cherchons à adjoindre à E une s_2, $\sigma = a.u.xv\ldots$ telle que, dans $|E, \sigma| = F$, E soit le diviseur fixant x. On peut supposer que σ est de degré 16 et, comme pour ρ, qu'elle échange 2 des lettres r, s, t, fixe la troisième, et, par suite, aussi 3 des lettres $b, \ldots, q$. $\sigma\zeta\sigma = (ua)\ldots$ devant être dans B, donc $(\sigma\zeta)^2 = (u)(a)\ldots$ dans A, $(\sigma\zeta)^2$ sera dans $|a_0|$. Si donc $(\sigma\zeta)^2 \neq 1$, $\sigma\zeta = (vx)(ua)\ldots$ sera de degré 22. σ fixant a et une seule des lettres r, s, t, on aura $\sigma a_0 \sigma = a_0^2$. Donc σ ne fixe pas 3 lettres d'un cycle de a_0. σ permutable à C, donc à Δ, permute entre eux les systèmes d'intransitivité de Δ et, fixant a, fixe le système a, b, c, f, donc une des lettres b, c, f. En transformant au besoin par $a_0^{\pm 1}$ on peut supposer que $\sigma = b.cf.\ldots$; donc $\sigma a_1 \sigma = a_1$, $\sigma a_2 \sigma = a_1 a_2$, σ fixant les systèmes a, b, c, f; r, s, t, u, et étant d'ordre 2 fixera au moins un des 3 systèmes restants. Supposons que σ fixe le système l, o, p, q. Elle ne fixera pas les 4 lettres, car elle serait de degré < 16; elle ne les déplacera pas toutes, car elle contiendrait un des couples de cycles $lo.pq$, $lp.oq$, $lq.op$ et serait permutable à a_2. Donc σ, permutable à a_1, fixe l et o ou p et q. Si σ fixe l et o, elle est permutable à $|a_0|, |b_0|, |l_0|, |o_0|$, et $\tau = vx.cf.de.gh.in.km.pq.\ldots$, le dernier cycle étant rs, st ou tr. Mais $\sigma\zeta$ fixant d, e, i, n, il faut que $(\sigma\zeta)^2 = 1$, ce qui exige que le dernier cycle soit st. On a ainsi pour σ la détermination $\sigma_1 = vx.cf.de.gh.in.km.pq.st$. Si σ fixe p et q, on obtient de même la forme $\sigma_1' = vx.cf.dn.ei\ gk.hm.lo.st$. Si σ fixe le système e, h, k, n, elle fixera e et h ou k et n, et l'on obtient les

2 formes [ici $(\sigma\zeta)^2 = a_0$]

$$\sigma_2 = \nu x.cf.dl.go.iq.kn.mp.rt,$$
$$\sigma'_2 = \nu x.cf.dp.ch.gq.io.lm.rt.$$

Si σ fixe le système d, i, m, g, elle fixe i et m ou d et g, et l'on a les 2 formes [ici $(\sigma\zeta)^2 = a_0^2$]

$$\sigma_3 = \nu x.cf.dg.eq.hp.kl.no.rs,$$
$$\sigma'_3 = \nu x.cf.el.ho.im.kq.np.rs.$$

Mais, $(\sigma'_1\rho)^3$, $(\sigma'_2\rho)^3$, $(\sigma'_3\rho)^3$ n'étant pas dans B, σ'_1, σ'_2, σ'_3 sont à rejeter. D'ailleurs, les substitutions

$$(\nu x)\,\sigma'_1 = \sigma''_1, \qquad (\nu x)\,\sigma'_2 = \sigma''_2, \qquad (\nu x)\sigma'_3 = \sigma''_3$$

donnent

$$(1)\quad \left\{\begin{array}{lll} (\sigma''_1\rho)^2 = a_0^2, & (\sigma''_2\rho)^2 = a_0, & (\sigma''_3\rho)^2 = 1, \\ (\sigma''_1\zeta)^2 = 1, & (\sigma''_2\zeta)^2 = a_0, & (\sigma''_3\zeta)^2 = a_0^2, \\ \multicolumn{3}{c}{(\sigma''_i a_0 \sigma''_i = a_0^2), \qquad \sigma''_i \mathrm{A} \sigma''_i = \mathrm{A};} \end{array}\right.$$

$$(2)\quad \sigma''_i\sigma_i\sigma''_i = \sigma_i, \qquad \sigma''_i\sigma_k\sigma''_i = \sigma_2 \qquad (i \neq k,\ k \neq l,\ l \neq i).$$

Donc les 3 groupes $\{\mathrm{E}, \sigma_i\}$ sont semblables, et il suffit de considérer $\{\mathrm{E}, \sigma\} = \mathrm{F}$ en écrivant σ pour σ_1. Les relations

$$\sigma^2 = (\sigma\rho)^3 = (\sigma\zeta)^2 = (\sigma a_0)^2 = (\sigma a_1)^2 = 1,$$
$$\sigma a_2 \sigma = a_1 a_2, \qquad \sigma a_3 \sigma = a_1$$

démontrent l'existence de F. Jointes aux équations de E elles déterminent F.

F, *trois fois transitif, est simple,* car s'il y avait un diviseur normal $\mathrm{X} < \mathrm{F}$, on aurait $\mathrm{F} = \mathrm{XE}$, et puisque E est simple, X, premier à E, serait un g_{22}^{22} deux fois transitif, ce qui ne se peut.

Cherchons à adjoindre à F une s^2, $\tau = \nu.u.a.yx\ldots$ telle que, dans $\{\mathrm{F}, \tau\} = \mathrm{G}'$, F soit le diviseur fixant y. On peut supposer que τ est de degré 16, échange 2 des lettres r, s, t, fixe la troisième et par suite

aussi 3 des lettres $b, \ldots, q$. $(\tau\rho)^2$ et $(\tau\sigma)^3$ devant être dans B, τ ne peut avoir, d'après (1), qu'une des formes $\sigma_i''(xy)$, d'après (2) que l'une des formes

$$\tau_1 = \sigma_2''(xy) = xy.cf.dp.eh.gq.io.lm.rt,$$
$$\tau_2 = \sigma_3''(xy) = xy.cf.el.ho.im.kq.np.rs.$$

Comme $\sigma_1''\tau_1\sigma_1'' = \tau_2$, les 2 groupes $G_i = \{F, \tau_i\}$ sont semblables, on peut se borner à considérer τ_1 et j'écrirai τ pour τ_1. Les relations

$$\tau^2 = (\tau\sigma)^3 = (\tau a_0)^2 = (\tau a_1)^2 = 1, \qquad (\tau\rho)^2 = a_0,$$
$$(\tau\zeta)^2 = a_0, \qquad \tau a_2 \tau = a_1 a_2, \qquad \tau a_3 \tau = a_2 a_3 a_4$$

(d'où résulte $\tau a_4 \tau = a_1 a_4$) démontrent l'existence de G_1 : jointes aux équations de F elles définissent G_1. G_1 contient $\alpha = \tau\sigma\rho\zeta a_1$, donc β, et $\gamma = \zeta a_1 \zeta\rho\zeta e_0$. Donc $G_1 \geqq G$. Mais G où le diviseur fixant y, x, v est $\geqq B$ est lui-même $\geqq G_1$. Donc $G_1 = G$. On sait déjà que G est simple puisqu'il est pair : on peut, d'ailleurs, démontrer sa simplicité comme celle de F.

Cherchons encore à adjoindre à G une s_2, $\upsilon = yz.x.v.u.a. \ldots$, telle que, dans $\{G, \upsilon\} = H$, G soit le diviseur fixant z. υ aura forcément unes des formes $\sigma_i''(yz)$. La condition que $(\upsilon\tau)^3$ et $(\upsilon\sigma)^2$ soient dans B exclut $\sigma_2''(yz)$ et $\sigma_3''(yz)$. Donc

$$\upsilon = \sigma_1''(yz) = yz.cf.dn.ei.gk.hm.lo.st.$$

Les relations

$$\upsilon^2 = (\upsilon\tau)^3 = (\upsilon\sigma)^2 = (\upsilon\zeta)^2 = (\upsilon a_1)^2 = 1,$$
$$(\upsilon\rho)^2 = a_0^2, \qquad \upsilon a_2 \upsilon = a_1 a_2, \qquad \upsilon a_3 \upsilon = a_4$$

prouvent l'existence de H. H *est simple* : on le démontre comme pour F. Si l'on convient de représenter ∞ par z, la substitution

$$(Z, -Z^{-1}) \qquad (\mathrm{mod}\, 23)$$

sera

$$vz.xu.yr.bi.ph.gc.ql.en.st.dm.fa.ok = f_0 \eta\sigma\xi\sigma\rho\eta\tau\sigma\rho\xi\eta\sigma\tau\upsilon\tau\sigma,$$

et H contenant α, β, $(Z, -Z^{-1})$ contiendra $\mathfrak{V}(2, 23)$.

Prenons maintenant

$$\gamma_g = ymcqs.pbfno.druch.tikla.x.y.g.$$

et considérons $G_g = \{\alpha, \beta, \gamma_g.\}$ Comme

$$\alpha = vxybpgqescdrfnkimholtau,$$
$$\beta = xypsmconbqf.gdthrualiek.v,$$

la substitution $\delta_g = \alpha^{-1}\gamma_g\alpha = bhdec.gpnkl.rfvso.amitu.x.y.q$ montre que le diviseur de G_g fixant x est transitif et

$$\varepsilon_g = \gamma_g^{-2}\,\delta_g\gamma_g^2 = nruds.gfpat.covmb.iqlkh.x.y.c$$

que celui fixant x, y est transitif. En posant

$$\theta_g = \delta_g\varepsilon_g^2, \qquad \mu_g = \alpha\varepsilon_g\alpha^{-1}\gamma_g^2, \qquad \nu_g = \mu_g\delta_g\theta_g\mu_g\theta_g,$$

les substitutions

$$\varphi = \nu_g^{-2}\,\delta_g\nu_g^2 \qquad = kpfli.cgnra.usetb.qdhmo.v.x.y,$$
$$\psi = \nu_g^{-1}\,\theta_g^{-1}\delta_g\theta_g\nu_g = drpqg.bcome.snaki.lhtfu.v.x.y$$

montrent que le diviseur de G_g fixant x, y, v est transitif. Donc G_g est quatre fois transitif. G_g contenant

$$\varphi\theta_g = b_{g0}, \qquad \theta_g\varphi = s_{g0}, \qquad \psi\mu_g = f_{g0}, \qquad \varphi^3\psi^2 = r_{g0},$$
$$s_{g0}r_{g0} = ae.bh.ct.di.fr.gk.lq.os = a_{g1},$$
$$r_{g0}s_{g0} = al.bk.ci.dt.eq.fs.gh.or = a_{g2},$$
$$s_{g0}b_{g0} = ao.bt.ch.dk.es.fq.gi.lr = a_{g3},$$
$$b_{g0}s_{g0} = ah.be.co.df.gl.ir.kq.st = a_{g4},$$

le diviseur de G_g qui fixe x, y, v, u contient $B_g = \{a_{g1}, a_{g2}, a_{g3}, a_{g4}, b_{g0}\}$. Or la substitution

$$\chi = \begin{pmatrix} m & p & n & a & b & c & d & e & f & g & h & i & k & l & o & q & r & s & t \\ s & r & t & h & a & g & i & e & p & f & b & m & c & n & o & k & q & l & d \end{pmatrix}$$

transforme a_{g1}, a_{g2}, a_{g3}, a_{g4}, b_{g0}, $a_{g2}\theta_g\mu_g a_{g2}$ en a_1, a_2, a_3, a_4, a_0, $a_0^{-1}\zeta a_0$ respectivement. Donc $\chi^{-1}G_g\chi$ contient C; $\chi^{-1}G_g\chi$ contenant $a_0^{-1}\rho_1 a_0 = \chi^{-1}\theta_g^{-1}\delta_g^{-1}\theta_g a_2 a_3\xi$, $\rho''\chi^{-1}G_g\chi\rho''^{-1}$ contiendra ρ et E; $\rho''\chi^{-1}G_g\chi\rho''^{-1}$ contenant $\sigma_3 = (\chi\rho')^{-1}\beta^{-1}\alpha\chi\rho'(\zeta k_0\rho)^4$, $\sigma_2''\rho''\chi^{-1}G_g\chi\rho''^{-1}\sigma_2''$ contiendra σ et F; $\sigma_2''\rho''\chi^{-1}G_g\chi\rho''^{-1}\sigma_2''$ contenant

$$\tau_2 = \sigma\eta\xi a_1 a_2 a_3 a_4\zeta a_3 a_4\rho\eta\xi\sigma,$$

le transformé $\iota^{-1}G_g\iota$ de G_g par $\iota = \chi\rho''^{-1}\sigma_2''\sigma_1''$ contiendra τ et G. Comme d'ailleurs $\iota^{-1}\alpha\iota = \tau\sigma\rho b_0^2\zeta$, $\iota^{-1}\gamma_g\iota = \alpha a_2 a_1\zeta a_1 a_2 a_4\xi\rho\zeta a_2 a_4\alpha^{-1}$, G contient $\iota^{-1}\alpha\iota$; donc $\iota^{-1}\beta\iota$ et $\iota^{-1}\gamma_g\iota$. Donc $G = \iota^{-1}G_g\iota$.

Tout g^{23} transitif ne contenant pas l'alterné et ne divisant pas le métacyclique est semblable à G. En effet, un tel groupe X contient un groupe semblable à G et est quatre fois transitif, mais non cinq fois car $23 = 19 + 4$ (5). Donc le g^{19} Γ fixant quatre symboles est intransitif et ne contient ni s_{13}, ni s_{17}, ni s_{19}. Donc (X, 1) divisant $\frac{23!}{2.3.5.7.11.13.17.19}$, $(\Gamma, 1) = 48\omega$, ω divisant $4.9.10.12.14.15.16.18$; $\Gamma \geqq B$ a les mêmes systèmes d'intransitivité que B. Soient $\mathfrak{A}$ son constituant de degré 16, $\mathfrak{B}$ celui de degré 3, $\mathfrak{A}_0$, $\mathfrak{B}_0$ leurs plus grands communs diviseurs avec Γ. On a $\mathfrak{B}_0 = 1$; donc $\mathfrak{B} = \mathfrak{A}\,|\,\mathfrak{A}_0 = \Gamma\,|\,\mathfrak{A}_0$, et $(\mathfrak{A}, 1) = 48\omega$ divise $16! : 2.3.5.7$; donc ω divise

$$4.9.10.12.14.15.16 = 2^{10}.3^4.5^2.7.$$

De plus, X *est pair* sans quoi il contiendrait (5)

$$\beta_0 = xgydptshmrcuoanlbiqefk \quad (\beta_0^2 = \beta)$$

$\beta_0^{-1}\gamma\beta_0 = \gamma_g$, $\gamma\gamma_g^{-1} = geluhdkiart$, et X contenant une s_{11}' serait le symétrique. Donc $(X, 1) = 23.11(23j + 1)$ et le g^{22} fixant un symbole a un ordre de la forme $11.5(11j_1 + 1)$, d'où

$$23j + 1 = 5(11j_1 + 1) = 2.21.20.48\omega.$$

La condition $23j + 1 \equiv 0 \pmod 5$ donne

$$j = 5j' + 3, \qquad 11j_1 + 1 = 23j' = 14, \qquad j' = 11j'' - 2,$$
$$23(11j'' - 2) + 14 = 2^7.3^2.7\omega, \qquad j'' = 32j''',$$
$$253j''' - 252\omega = 1, \qquad \omega \equiv 1 \pmod{253}.$$

Or les seuls diviseurs de $2^{10}.3^4.5^2.7$ qui soient $\equiv 1 \pmod{253}$ sont 1 et $3^4.5^2$. ω étant premier à 7, Γ ne contient pas de s_7^{14} et, dans le g^{21} de X qui fixe deux symboles, le groupe des opérations permutables à un g_7 est d'ordre 3.7 ou 9.7 (4). Donc

$$(X, 1) = 2^3.2^2.3.7(7w+1) \quad \text{ou} \quad 2^3.2^2.3^2.7(7w+1).$$

Dans le premier cas $\omega \equiv 1 \pmod 7$; dans le second, $\omega \equiv 3 \pmod 7$. Or $3^4.5^2 \equiv 2 \pmod 7$. Donc $\omega = 1$ et $X \equiv G$.

11. Pour $q = 47$ et $q = 59$, M. Jordan a vérifié que tout g^q ne divisant pas le métacyclique contient l'alterné (*Comptes rendus*, t. LXXIX, 1894, p. 1151). Il suffit, pour refaire cette vérification, de trouver dans chaque $(\alpha, \beta, \gamma_i)$ une s_π^π, π étant premier $< \frac{2}{3}q$, ou même simplement, en se servant d'un théorème de M. Jordan énoncé au n° 5, une $s_\pi^{\varkappa\pi}$, π étant premier, $\varkappa < 6$ et $< \pi$, $\varkappa\pi + \varkappa + 1 < q$.