SUR LES GROUPES TRANSITIFS

DONT LE DEGRÉ EST LE CARRÉ D'UN NOMBRE PREMIER

PAR

L. SYLOW

À FREDERIKSHALD

Si l'ordre d'un groupe est divisible par une puissance d'un nombre premier, telle que p^m, mais non divisible par p^{m+1}, cet ordre est, comme on le sait, de la forme $p^m\pi(np+1)$; le groupe en contient un autre de l'ordre $p^m\pi$; celui-ci contient à son tour un troisième groupe, de l'ordre p^m, auquel toutes ses substitutions sont permutables; enfin le nombre des groupes de l'ordre p^m contenus dans le premier groupe est $np+1$. La détermination complète de ce dernier nombre, dans les divers cas qui peuvent se présenter, serait évidemment d'une grande importance pour la théorie des substitutions; malheureusement elle paraît être d'une extrême difficulté. Mais il sera possible de trouver des résultats plus ou moins intéressants sur la forme du nombre n par rapport aux modules $p, p^2, p^3, \ldots$; à cet effet on n'aura qu'à poursuivre le raisonnement qui m'a servi pour la démonstration du théorème cité (Mathematische Annalen, t. 5). Pour faire un premier pas dans cette direction, je me propose, dans le travail présent, de considérer le cas le plus simple, celui des groupes transitifs du degré p^2.

Je désignerai par G un groupe transitif du degré p^2, par O son ordre, que je supposerai divisible par $p^{\alpha+2}$, mais non divisible par $p^{\alpha+3}$; le nombre α pourra donc avoir les valeurs $0, 1, 2, \ldots, p-1$. Je désignerai de plus par I un groupe de l'ordre $p^{\alpha+2}$ contenu dans G, et par H le plus grand groupe contenu dans G dont les substitutions soient

permutables à I. L'ordre du groupe H sera dénoté par $p^{\alpha+2}.\pi$, où par conséquent π est premier à p; on aura donc

$$O = p^{\alpha+2}\pi(np + 1).$$

Je déterminerai dans un premier paragraphe la forme de I, dans un deuxième celle de H; dans les deux paragraphes suivants je m'occuperai du nombre n; enfin dans le dernier je ferai des résultats trouvés quelques applications, qui se présentent au premier coup d'oeil.

§ 1. *Détermination du groupe I.*

1. D'après le lemme de CAUCHY le groupe symétrique du degré p^2 contient un certain nombre de groupes de l'ordre p^{p+1}, tous isomorphes entre eux. Notre groupe I est contenu dans un de ces groupes de CAUCHY, et en disposant convenablement des indices, nous pouvons choisir ce dernier comme nous voudrons. En désignant les éléments par le symbole

$$u_{x,y},$$

les indices x et y étant pris suivant le module p, nous pouvons donc supposer que les substitutions de I soient contenues dans l'expression

$$\begin{vmatrix} x & x + a_0 + a_1 y + a_2 y^2 + \ldots + a_{p-1} y^{p-1} \\ y & y + b \end{vmatrix},$$

qui d'ailleurs peut être remplacée par cette autre

$$\begin{vmatrix} x & x + a_0 + a_1 y + a_2 (y)_2 + a_3 (y)_3 + \ldots + a_{p-1} (y)_{p-1} \\ y & y + b \end{vmatrix},$$

où, pour abréger, on a fait

$$(y)_i = \frac{y(y-1)(y-2)\ldots(y-i+1)}{1 \cdot 2 \cdot 3 \ldots i}.$$

En posant

$$U = \begin{vmatrix} x & x + a_0 + a_1 y + a_2 (y)_2 + \ldots + a_{p-1} (y)_{p-1} \\ y & y + 1 \end{vmatrix},$$

on trouve

$$U^m = \begin{vmatrix} x & x + ma_0 + a_1\{(y+m)_2 - (y)_2\} + \ldots + a_{p-2}\{(y+m)_{p-1} - (y)_{p-1}\} + a_{p-1}\sum_0^{m-1} {}_r(y+r)_{p-1} \\ y & y+m \end{vmatrix}$$

Si l'on fait $m = p$, on a, pour $i \leq p-1$,

$$(y+m)_i - y_i \equiv 0 \pmod p,$$

et

$$\sum_0^{m-1} {}_r(y+r)_{p-1} = 1,$$

donc

$$U^p = \begin{vmatrix} x & x + a_{p-1} \\ y & y \end{vmatrix}.$$

Ainsi l'ordre de la substitution U est égal à p ou à p^2 suivant que a_{p-1} est congru à zéro, ou non.

Parmi ces substitutions toutes celles qui ne changent pas l'indice y, sont échangeables entre elles. En faisant

$$S = \begin{vmatrix} x & x + f(y) \\ y & y \end{vmatrix}, \qquad T = \begin{vmatrix} x & x + \varphi(y) \\ y & y+1 \end{vmatrix},$$

on trouve

$$(1) \qquad T^{-1}ST = \begin{vmatrix} x & x + f(y-1) \\ y & y \end{vmatrix}, \qquad TST^{-1} = \begin{vmatrix} x & x + f(y+1) \\ y & y \end{vmatrix},$$

d'où

$$(2) \qquad S^{-1}T^{-1}ST = T^{-1}STS^{-1} = \begin{vmatrix} x & x - \{f(y) - f(y-1)\} \\ y & y \end{vmatrix},$$

$$(3) \qquad S^{-1}TST^{-1} = TST^{-1}S^{-1} = \begin{vmatrix} x & x + f(y+1) - f(y) \\ y & y \end{vmatrix},$$

$$(4) \qquad S^{-1}TS = \begin{vmatrix} x & x + f(y+1) - f(y) + \varphi(y) \\ y & y+1 \end{vmatrix},$$

2. Le groupe G étant transitif, I le sera également (voir le Mémoire cité plus haut, n° 4); donc I contient des substitutions de chacune des formes S et T du numéro précédent. Or, si β désigne le plus grand degré des fonctions $f(y)$, les formules (2) et (3) font voir que le groupe I contient aussi des substitutions dans lesquelles les fonctions $f(y)$ sont des degrés $\beta - 1, \beta - 2, \ldots, 1, 0$. On en peut conclure qu'on a $\beta = \alpha$, et qu'en faisant

$$\theta_i = | x, y \quad x + y^i, y |,$$

toutes les substitutions de I sont contenues dans l'expression

$$\theta_0^{a_0} \theta_1^{a_1} \ldots \theta_\alpha^{a_\alpha} . T^b;$$

d'ailleurs les substitutions θ_i peuvent être remplacées par les suivantes

$$\vartheta_i = | x, y \quad x + (y)_i, y |.$$

Si l'on désigne, pour un moment, par g_i le groupe dérivé des substitutions $\theta_0, \theta_1, \ldots, \theta_i$, et par I_i celui qui dérive des substitutions de g_i et de T, on voit (équat. (2) et (3)) que les substitutions de I_i sont échangeables entre elles à des substitutions de g_{i-1} près. Donc si l'on a $\alpha = 0$, toutes les substitutions de I_α sont échangeables entre elles; si $\alpha > 0$, les $\theta_0^{a_0}$ sont les seules substitutions de I_α qui soient échangeables à toutes les autres.

Transformons maintenant le groupe I par la substitution

$$U = | x, y \quad x + \phi(y), y |.$$

Les substitutions θ_i, ϑ_i conservent leurs formes, au contraire on a

$$U^{-1} T U = | x, y \quad x + \varphi(y) + \phi(y + 1) - \phi(y), y + 1 |.$$

Or, si en développant suivant les fonctions $(y)_i$, on a

$$\varphi(y) = a_0 + a_1 y + a_2 (y)_2 + \ldots + a_{p-2} (y)_{p-2} + a_{p-1} (y)_{p-1},$$

on peut faire

$$\phi(y + 1) - \phi(y) = - [a_0^* + a_1 y + a_2 (y)_2 + \ldots + a_{p-2} (y)_{p-2}],$$

ce qui donne

$$U^{-1}TU = |\, x, y \quad x + a_{p-1}(y)_{p-1}, y + 1 \,| = T'.$$

Si maintenant a_{p-1} est différent de zéro, transformons de nouveau par la substitution

$$V = |\, x, y \quad bx, y \,|,$$

qui évidemment est permutable au groupe g_a; on trouve

$$V^{-1}T'V = |\, x, y \quad x + a_{p-1}b(y)_{p-1}, y + 1 \,| = T'';$$

donc en faisant $a_{p-1}b \equiv 1 \pmod{p}$, on a

$$T'' = |\, x, y \quad x + (y)_{p-1}, y + 1 \,|.$$

Par un choix convenable des indices, la substitution T peut donc être réduite à l'une des deux formes suivantes

$$t = |\, x, y \quad x, y + 1 \,|, \qquad t = |\, x, y \quad x + (y)_{p-1}, y + 1 \,|.$$

On voit que, pour $\alpha < p - 1$, on a deux espèces de groupes de l'ordre $p^{\alpha+2}$, qui diffèrent seulement par la forme de la substitution t; dans la première espèce toutes les substitutions sont de l'ordre p; dans la seconde, celles qui ne font pas varier l'indice y sont de l'ordre p, les autres de l'ordre p^2. Quand $\alpha = p - 1$, les deux cas ne donnent qu'un seul groupe, puisque le groupe g_{p-1} contient la substitution

$$\vartheta_{p-1} = |\, x, y \quad x + (y)_{p-1}, y \,|,$$

Tous les groupes d'ordre p^2 contenus dans G étant isomorphes, cette classification peut aussi être appliquée aux groupes du degré p^2 en général; nous comprendrons dans la première espèce les cas où $\alpha = p - 1$.

Des équations (1) on déduit les suivantes:

$$(5) \qquad t^{-1}\vartheta_i t = \vartheta_0^{\pm 1}\vartheta_1^{\mp 1} \ldots \vartheta_{i-1}^{-1}\vartheta_i, \qquad t\vartheta_i t^{-1} = \vartheta_{i-1}\vartheta_i,$$

$$(6) \qquad t^{-1}\theta_i t = \theta_0^{\pm 1}\theta_1^{\mp i}\theta_2^{\pm (i)_2} \ldots \theta_{i-1}^{-i}\theta_i, \qquad t\theta_i t^{-1} = \theta_0\theta_1^{i}\theta_2^{(i)_2} \ldots \theta_{i-1}^{i}\theta_i.$$

En considérant les groupes de la seconde espèce, il est quelquefois

commode d'employer un seul indice, pris suivant le module p^2. A cet effet on peut faire

$$xp + y \equiv \xi \pmod{p^2},$$

en ayant soin de remplacer toujours y par le plus petit nombre positif qui lui est congru (mod p); on trouve ainsi

$$t = |\, \xi \quad \xi + 1 \,|,$$

$$t^p = \theta_0 = \vartheta_0 = |\, \xi \quad \xi + p \,|,$$

$$\vartheta_i = |\, \xi \quad \xi + p(\xi)_i \,|, \qquad \theta_i = |\, \xi \quad \xi + p\xi^i \,|.$$

Evidemment le groupe I est non-primitif, les éléments qui répondent à une même valeur de y formant un système; de plus si $\alpha > 0$, les éléments ne peuvent être répartis en systèmes que de cette manière, comme on le voit aisément.

Un groupe d'ordre $p^{\alpha+2}$ contenu dans G est complètement déterminé, quand on connaît les substitutions qui sont échangeables à toutes les autres, et qu'on connaît de plus de quelle manière les systèmes sont permutés entre eux. Supposons, en effet, que le groupe I', contenu dans G, contienne la substitution $\theta_0^a = |\, x, y \quad x + a, y \,|$ échangeable à toutes les autres, et que celles-ci déplacent les systèmes conformément à la substitution $|\, y \quad y + b \,|$. Evidemment les substitutions de I' sont comprises dans l'expression

$$T = |\, x, y \quad x + \varphi(y), y + b \,|.$$

Or G, contenant T et t, contient $T.t^{-b}$, substitution qui peut être écrite sous la forme suivante

$$Tt^{-b} = |\, x, y \quad x + F(y), y \,| = S.$$

Si maintenant S n'était pas contenu dans I, le groupe qui dérive de S et des substitutions de I serait d'un ordre $p^{\alpha+m}$, où $m > 2$; donc S, et par suite T, font partie de I, c'est-à-dire que I' coïncide avec I. En particulier, si G appartient à la seconde espèce, I' est complètement déterminé par une substitution quelconque de l'ordre p^2.

§ 2. *Détermination du groupe H.*

3. Considérons d'abord les groupes de la première espèce, en excluant préalablement les cas où $\alpha = 0$. Les θ_0^m étant les seules substitutions de I échangeables à toutes les autres, une substitution S de H doit transformer θ_0 en θ_0^a; par suite on doit avoir

$$S = | x , y \quad ax + \varphi(y) , \varphi_1(y) |,$$

φ et φ_1 dénotant des fonctions entières du degré $p - 1$ au plus. La transformée de t par S doit être une substitution de I, ce qui donne les conditions suivantes:

$$\left.\begin{aligned} &\varphi(y+1) - \varphi(y) \equiv b_0 + b_1\varphi_1(y) + b_2[\varphi_1(y)]^2 + \ldots + b_\alpha[\varphi_1(y)]^\alpha \\ &\varphi_1(y+1) - \varphi_1(y) \equiv c \end{aligned}\right\} \pmod p.$$

La seconde congruence donne

$$\varphi_1(y) \equiv cy + d;$$

en remettant cette valeur dans la première et développant suivant les fonctions $(y)_i$, on a un résultat de la forme suivante

$$\varphi(y+1) - \varphi(y) \equiv b'_0 + b'_1 y + b'_2 (y)_2 + \ldots + b'_\alpha (y)_\alpha,$$

d'où

$$\varphi(y) \equiv \varphi(0) + b'_0 y + b'_1 (y)_2 + b'_2 (y)_3 + \ldots + b'_\alpha (y)_{\alpha+1}.$$

Donc toute substitution de H est comprise dans l'expression

$$\left|\begin{matrix} x & ax + b_0 + b_1 y + b_2 y^2 + \ldots + b_{\alpha+1} y^{\alpha+1} \\ y & cy + d \end{matrix}\right|;$$

par conséquent elle est le produit d'une substitution de I par une autre de la forme suivante:

$$T = | x , y \quad ax + by^{\alpha+1} , cy |.$$

Evidemment les substitutions T forment un groupe, que nous désignerons par H'.

Quand $\alpha = p - 1$, on a $b = 0$; nous démontrerons maintenant que, sans nuire à la généralité, on peut supposer $b = 0$, même si $\alpha < p - 1$. En supposant $c^{\alpha+1} \equiv a \pmod p$ on trouve

$$T^m = \begin{vmatrix} x & c^{m(\alpha+1)}x + mbc^{(m-1)(\alpha+1)}y^{\alpha+1} \\ y & c^m y \end{vmatrix};$$

et en faisant m égal au plus petit exposant pour lequel $c^m \equiv 1 \pmod p$:

$$T^m = \left| x\,,\, y \quad x + m\frac{b}{a}y^{\alpha+1}\,,\, y \right|.$$

Or, si l'on n'avait pas $b \equiv 0$, la substitution T^m serait de l'ordre p, et par conséquent l'ordre de H serait divisible par $p^{\alpha+3}$; cela étant contre l'hypothèse, on conclut que si dans une substitution T de H' on a

$$a - c^{\alpha+1} \equiv 0,$$

on a en même temps

$$b \equiv 0.$$

Supposons maintenant que H' contienne les deux substitutions

$$T = \left| x\,,\, y \quad ax + by^{\alpha+1}\,,\, cy \right|, \qquad T_1 = \left| x\,,\, y \quad a_1x + b_1y^{\alpha+1}\,,\, c_1y \right|;$$

on trouve

$$T^{-1}T_1TT_1^{-1} = \begin{vmatrix} x & x + \dfrac{ab_1 - a_1b + bc_1^{\alpha+1} - b_1c^{\alpha+1}}{a_1c^{\alpha+1}}y^{\alpha+1} \\ y & y \end{vmatrix}.$$

Cette substitution, qui est étrangère à I, doit être identique, car autrement son ordre serait p, ce qui est impossible; donc on a

$$\frac{b_1}{a_1 - c_1^{\alpha+1}} \equiv \frac{b}{a - c^{\alpha+1}} \pmod p. \tag{7}$$

Cela posé, transformons le groupe H par la substitution

$$U = \left| x\,,\, y \quad x + ry^{\alpha+1}\,,\, y \right|,$$

qui est permutable à I; on trouve

$$U^{-1}TU = \left| x\,,\, y \quad ax + [b - r(a - c^{\alpha+1})]y^{\alpha+1}\,,\, cy \right|;$$

donc en faisant

$$r \equiv \frac{b}{a - c^{\alpha+1}},$$

on a

$$U^{-1}TU = |\, x, y \quad ax, cy \,|;$$

de plus la congruence (7) fait voir que les transformées de toutes les autres substitutions de H' prennent la même forme.

Il est donc démontré que, pour les groupes de la première espèce, α étant > 0, on peut supposer le groupe H' formé de substitutions de la forme

$$|\, x, y \quad ax, cy \,|;$$

l'ordre de H' est donc $\frac{(p-1)^2}{h}$, celui de H est $p^{\alpha+2}\frac{(p-1)^2}{h}$, le nombre h étant un diviseur de $(p-1)^2$.

4. Passons aux groupes de la seconde espèce. Quand $\alpha = 0$, le groupe I contient seulement les puissances de la substitution

$$t = |\, \xi \quad \xi + 1 \,| \pmod{p^2},$$

par suite toute substitution de H est le produit d'une substitution de I par une substitution de la forme $\xi, a\xi$, où a est premier à p, et appartient à un exposant qui est premier à p. Donc en désignant par ∂ une racine primitive du module p^2, les valeurs de a sont de la forme ∂^{xp}, par conséquent l'ordre de H est égal à

$$\frac{p^2(p-1)}{h},$$

h étant un diviseur de $p - 1$.

En général toute substitution U de H doit vérifier l'équation

$$tU = US,$$

S étant une substitution de I. En faisant

$$U = |\, \xi \quad \varphi(\xi) \,|,$$

on a ainsi la condition suivante:

$$\varphi(\xi + 1) - \varphi(\xi) \equiv m_0 + p\{m_1\varphi(\xi) + m_2(\varphi\xi)^2 + \ldots + m_\alpha(\varphi\xi)^\alpha\} \pmod{p^2}$$

On en tire

$$\varphi(\xi + 1) - \varphi(\xi) \equiv m_0 \pmod{p},$$

d'où

$$\varphi(\xi) \equiv m_0\xi + \varphi(0) \pmod{p}.$$

En remettant ce résultat dans la congruence primitive, elle prend la forme

$$\varphi(\xi + 1) - \varphi(\xi) \equiv n_0 + p\{n_1\xi + n_2\xi^2 + \ldots + n_\alpha\xi^\alpha\} \pmod{p^2}.$$

Comme nous avons supposé $\alpha < p - 1$, on en tire

$$\varphi(\xi) \equiv a\xi + b + p(a_2\xi^2 + a_3\xi^3 + \ldots + a_{\alpha+1}\xi^{\alpha+1}) \pmod{p^2}.$$

Donc toute substitution de H est le produit d'une substitution de I par une substitution de la forme suivante

$$T' = |\, \xi \quad a\xi + pb\xi^{\alpha+1} \,|.$$

Ces substitutions forment un groupe H'. En supposant

$$a^\alpha \equiv 1 \pmod{p},$$

on a

$$T'^m = |\, \xi \quad a^m\xi + pbma^{m-1}\xi^{\alpha+1} \,|;$$

si l'on fait m égal au plus petit exposant pour lequel $a^m = 1 + ph$, il vient

$$T^m = |\, \xi \quad \xi + p(h\xi + bma^{m-1}\xi^{\alpha+1}) \,|;$$

on en conclut que $b \equiv 0$, car autrement T^m serait de l'ordre p sans être contenu dans I. Ainsi la congruence

$$a^\alpha \equiv 1 \pmod{p}$$

entraîne celle-ci

$$b \equiv 0 \pmod{p}.$$

Or je dis que le groupe H ne peut contenir qu'une seule substitution pour chaque valeur de a. En effet, s'il contient

$$T = |\, \xi \quad a\xi + pb\xi^{\alpha+1} \,| \quad \text{et} \quad T_1 = |\, \xi \quad a\xi + pb_1\xi^{\alpha+1} \,|,$$

il contient aussi

$$T^{-1}T_1 = \left| \xi \quad \xi + p\frac{b_1 - b}{a^{\alpha+1}}\xi^{\alpha+1} \right|,$$

qui, étant de l'ordre p, doit être contenu dans I; donc on a $b_1 \equiv b \pmod p$, $T = T_1$.

Par conséquent les valeurs du nombre a sont les puissances d'une certaine valeur primitive; donc les substitutions de H' sont les puissances de l'une d'elles, T_0; soit

$$T_0 = | \xi \quad a_0\xi + pb_0\xi^{\alpha+1} |.$$

En transformant H par la substitution

$$U = | \xi \quad \xi + pr\xi^{\alpha+1} |,$$

I n'est pas changé, et l'on a

$$U^{-1}T_0U = | \xi \quad a_0\xi + p[b_0 - r(a_0 - a_0^{\alpha+1})]\xi^{\alpha+1} |.$$

Or, si b_0 n'est pas congru à zéro $(\mathrm{mod}\, p)$, $a_0 - a_0^{\alpha+1}$ ne l'est pas non plus; nous pouvons donc faire

$$r \equiv \frac{b_0}{a_0 - a_0^{\alpha+1}} \pmod p,$$

ce qui donne

$$U^{-1}T_0U = | \xi \quad a_0\xi |.$$

On peut donc supposer que les substitutions de H' soient de la forme $| \xi \quad a\xi |$; d'autre part toutes les substitutions de cette forme contenues dans G appartiennent à H'. Si $a > p$, faisons $a = a' + a''p$, où $a' < p$; on a

$$| \xi \quad a\xi | = | \xi \quad a'\xi | \cdot \left| \xi \quad \xi + p\frac{a''}{a'}\xi \right|,$$

et comme le dernier facteur appartient à I, on peut remplacer a par a'. Donc l'ordre de H' est $\frac{p-1}{h}$, celui de H est $\frac{p^{\alpha+2}(p-1)}{h}$, h étant un diviseur de $p - 1$.

Il est facile d'exprimer les substitutions de H par deux indices pris suivant le module p. En effet, ayant

$$T' = | \xi \quad a\xi | \pmod{p^2},$$

et faisant

$$\xi = px + y, \qquad y < p.$$

$$ay \equiv \eta \pmod{p}, \qquad \eta \geqq 0, \qquad \eta < p,$$

et désignant enfin par $E(m)$ le plus grand nombre entier contenu dans la fraction m, on a

$$a\xi = apx + ay = apx + pE\left(\frac{ay}{p}\right) + \eta;$$

donc

$$T = \begin{vmatrix} x & ax + E\left(\frac{ay}{p}\right) \\ y & \eta \end{vmatrix} = \begin{vmatrix} x & ax + E\left(\frac{ay}{p}\right) \\ y & ay \end{vmatrix} \pmod{p}.$$

5. Il nous reste à considérer le cas où le groupe I ne contient que les p^2 substitutions

$$| x, y \quad x + a, y + b |.$$

Le groupe H dérive évidemment des substitutions de I et de celles d'un certain groupe H' d'ordre π, dont les substitutions sont de la forme

$$| x, y \quad \alpha x + \beta y, \gamma x + \delta y |.$$

Inversement H renferme toutes les substitutions linéaires de G. Il faut donc trouver tous les groupes contenus dans le groupe linéaire homogène à deux indices dont les ordres sont premiers à p. La résolution de ce problème, beaucoup plus compliqué que celui que nous avons traité, peut être tirée de la détermination des groupes finis, contenus dans le groupe linéaire infini à deux variables, faite par M. JORDAN dans son *Mémoire sur les équations différentielles linéaires à intégrale algébrique* (Journal für Mathematik, Bd. **84**).[1] En effet, l'analyse de

[1] Ainsi M. GIERSTER s'en est servi dans son énumeration des groupes partiels contenus dans le groupe linéaire fractionnaire à un indice (Inauguraldissertation, Leipzig 1881).

M. JORDAN repose entièrement sur la circonstance qu'un groupe fini ne peut contenir aucune substitution de la forme

$$x, y \quad \alpha(x + \lambda y), \alpha y ,$$

λ étant différent de zéro, son ordre ne pouvant être fini; pareillement, dans notre problème, l'ordre d'une substitution de cette forme est toujours un multiple de p; elle ne peut donc appartenir à H'. En lisant la déduction de M. JORDAN, on voit aisément qu'on obtient toutes les formes du groupe H', en remplaçant les variables x et y par des indices pris suivant le module p, et changeant les équations de condition auxquelles doivent satisfaire les constantes, en des congruences (mod p). Dans l'énumération suivante les indices ξ, η sont ou réels, ou des nombres imaginaires et conjugués de la forme $a + b\varepsilon$, ε étant racine d'une congruence irréductible du second degré; ils sont réels ou imaginaires en même temps que les multiplicateurs de la première substitution, désignée par A et donnée sous forme canonique. Nous appellerons, avec M. JORDAN, substitutions de la première espèce celles qui, mises sous forme canonique, multiplient les indices par des nombres différents, substitutions de la seconde espèce celles qui multiplient les deux indices par un même nombre, nécessairement réel, et nous dénoterons ces dernières en écrivant simplement le multiplicateur, par exemple

$$a = |\, \xi, \eta \quad a\xi, a\eta \,|, \qquad -1 = |\, \xi, \eta \quad -\xi, -\eta \,|.$$

Premier type. Les substitutions sont de la forme

$$A = |\, \xi, \eta \quad a\xi, b\eta \,|.$$

Deuxième type. Le groupe dérive d'un groupe de premier type combiné avec une substitution de la forme

$$B = |\, \xi, \eta \quad c\eta, d\xi \,|.$$

Troisième type (type *tétraédrique*). Le groupe dérive des substitutions

$$A = |\, \xi, \eta \quad i\xi, -i\eta \,|, \quad \text{où} \quad i^2 + 1 \equiv 0 \pmod p,$$

$$B = |\, \xi, \eta \quad r\eta, s\xi \,|, \quad \text{où} \quad rs + 1 \equiv 0,$$

$$C = \begin{vmatrix} \xi & m\dfrac{1-i}{2}(\xi - r\eta) \\ \eta & m\dfrac{1+i}{2}(-s\xi + \eta) \end{vmatrix}, \quad m \text{ étant réel,}$$

et d'un certain nombre de substitutions de la seconde espèce. Parmi celles-ci se trouvent toujours $A^2 = B^2 = -1$, $C^3 = -m^3$. L'ordre du groupe est égal à 12ω, ω étant l'ordre du groupe formé des substitutions de la seconde espèce contenues dans H'. Le groupe alterné entre quatre lettres $\alpha, \beta, \gamma, \delta$ est isomorphe à H'. En désignant par le signe $\sim$ qu'une substitution de H' correspond à une substitution entre $\alpha, \beta, \gamma, \delta$, on a

$$a \sim 1\ ,\ aA \sim (\alpha\beta)(\gamma\delta)\ ,\ aB \sim (\alpha\delta)(\beta\gamma)\ ,\ aC \sim (\alpha\beta\gamma).$$

On doit évidemment omettre ce type quand $p = 3$.

Quatrième type (type *octaédrique*). Les groupes de ce type dérivent d'un groupe du troisième type et d'une substitution de la forme

$$D = |\,\xi, \eta \quad e\xi, ei\eta\,|,$$

où $e^2 \equiv fi$, f étant réel. Dans l'expression de la substitution C on peut toujours faire $m \equiv 1$. Le groupe symétrique entre 4 lettres est isomorphe à H'; on a

$$aD \sim (\alpha\gamma\beta\delta)\ ,\ aBD \sim (\gamma\delta).$$

L'ordre du groupe est 24ω; par conséquent il doit être omis quand $p = 3$.

Cinquième type (type *icosaédrique*). Le groupe dérive de substitutions de la seconde espèce et des trois substitutions suivantes:

$$A = |\,\xi, \eta \quad \theta\xi, \theta^{-1}\eta\,|, \quad \text{où} \quad \frac{\theta^5 - 1}{\theta - 1} \equiv 0,$$

$$B = |\,\xi, \eta \quad r\eta, s\xi\,|, \quad \text{où} \quad rs + 1 \equiv 0,$$

$$C = \begin{vmatrix} \xi & \lambda\xi + r\mu\eta \\ \eta & -s\mu\xi - \lambda\eta \end{vmatrix}, \quad \text{où} \quad \lambda \equiv \frac{1}{\theta^3 - \theta^2}\ ,\ \mu \equiv \frac{1}{\theta^4 - \theta},$$

et où par conséquent

$$\lambda^2 + \mu^2 + 1 \equiv 0.$$

Le groupe contient toujours la substitution $B^2 = C^2 = -1$; son ordre est égal à 60ω, ω ayant la même signification que plus haut; il n'existe que pour les nombres p de la forme $10h \pm 1$. Le groupe alterné entre cinq lettres $\alpha, \beta, \gamma, \delta, \varepsilon$ est isomorphe au groupe icosaédrique; on a

$$aA \sim (\alpha\beta\gamma\delta\varepsilon)\ ,\ aB \sim (\beta\varepsilon)(\gamma\delta)\ ,\ aC \sim (\beta\delta)(\gamma\varepsilon)\ ,\ aA^3C \sim (\alpha\beta\gamma).$$

Le groupe H' appartient donc toujours à l'une de ces cinq types, et il peut être réduit à l'une des formes canoniques ci-dessus par une transformation linéaire, qui est réelle ou imaginaire en même temps que les indices ξ et η. S'ils sont réels, on peut simplement changer ξ et η en x et y, puisque toute substitution linéaire et réelle est permutable au groupe I. Au contraire, si ξ et η sont imaginaires, et qu'on veuille conserver I sous sa forme réelle, il faut réduire A, B, C, D à des formes réelles, ce qui ne présente pas de difficulté. Mais comme, dans la suite, nous pourrons nous servir des formes canoniques même s'ils sont imaginaires, nous omettrons ces calculs.

§ 3. *Sur le nombre n.*

6. Le groupe G contient $np + 1$ groupes de l'ordre $p^{\alpha+2}$, que nous désignerons par

$$I_0, I_1, I_2, \ldots, I_{np}.$$

En les transformant tous par les substitutions de I_0, on obtient un groupe de substitutions entre les I_m, isomorphe à I_0. Si l'on réunit en systèmes ceux qui sont permutés entre eux d'une manière transitive, le nombre des groupes contenus dans chaque système est une puissance de p, I_0 seul formant un système du degré 1. On a donc une équation de la forme suivante:

$$np = n_1 p^{r_1} + n_2 p^{r_2} + n_3 p^{r_3} + \ldots$$

les nombres $r_1, r_2, r_3, \ldots$ étant tous égaux ou supérieurs à 1. Supposons que I_1 fasse partie d'un système du degré p^{r_1}; I_1 est évidemment permutable aux substitutions d'un groupe K de l'ordre $p^{\alpha+2-r_1}$ contenu dans I_0. Le groupe K sera aussi contenu dans I_1; en effet, si le nombre des substitutions communes à I_1 et à K est égal à $p^{\alpha+2-r_1-s}$, le groupe dérivé des substitutions de I_1 et de K aura pour ordre $p^{\alpha+2+s}$, d'où l'on conclut que $s = 0$, l'ordre de G n'étant pas divisible par $p^{\alpha+3}$. Inversement, si les substitutions communes à I_0 et à I_1 forment un groupe de l'ordre $p^{\alpha+2-r_1}$, I_1 fait évidemment partie d'un système du degré p^{r_1}. Spécialement, si $r_1 = 1$, I_1 appartient à un système du degré p; or K étant dans ce cas permutable aux substitutions de I_0, il sera contenu

dans tous les groupes du système, et sera permutable à leurs substitutions. Donc, si l'on désigne par $K_1, K_2, \ldots, K_m$ les groupes de l'ordre $p^{\alpha+1}$ contenus dans G, l'un quelconque d'entre eux, K_r, sera contenu dans les groupes d'un nombre n_r de systèmes, et l'on aura

$$np = n_1 p + n_2 p + \ldots + n_m p + n' p^2,$$

les nombres $n_1, n_2, \ldots, n_m$ pouvant être nuls, tous ou en partie. Pour discuter cette équation nous distinguerons dans la suite plusieurs cas, qui diffèrent par l'espèce du groupe et par la valeur de α.

7. Commençons par les groupes de la première espèce où $\alpha = 0$. Les groupes K_r sont en nombre $p + 1$, chacun d'eux contenant les puissances d'une seule substitution

$$S = |\, x, y \quad x + a, y + b \,|;$$

nous ferons l'indice r congru au rapport $\frac{b}{a}$. Supposons que $K_{\frac{b}{a}}$ soit contenu dans les groupes des n_1 premiers systèmes, savoir les groupes $I_1, I_2, \ldots, I_{n_1 p}$, et soit G_1 le groupe formé des substitutions de G qui sont échangeables à S. Les substitutions de chacun des groupes I étant échangeables entre elles, G_1 contient $I_0, I_1, \ldots, I_{n_1 p}$, mais il ne contient aucun des groupes $I_{n_1 p+1} \ldots I_{np}$. Par conséquent son ordre est $p^2 \pi_1 (n_1 p + 1)$, π_1 étant l'ordre du groupe H_1' qui contient les substitutions de H' échangeables à S. De plus, $K_{\frac{b}{a}}$ étant intransitif, G_1 est non-primitif, ses substitutions remplaçant les éléments de chaque cycle de S par les éléments d'un même cycle. Il existe donc un groupe G_1' du degré p, isomorphe à G_1, et l'on voit aisément que son ordre sera

$$p \pi_1 (n_1 p + 1),$$

ce qui réduit très considérablement les valeurs que peuvent avoir n_1 et π_1. Notamment on sait, en vertu de deux théorèmes de M. E. Mathieu (Journal de Liouville, année 1861, p. 310) qu'on ne peut avoir $\pi_1 = 1$, sans avoir $n_1 = 0$, et qu'on a également $n_1 = 0$, si $\pi_1 = 2$, $p = 4h + 3$.

Recherchons donc quelles sont les substitutions de H' qui peuvent être échangeables à une substitution de I_0. Soit

$$T = | x , y \quad \alpha x + \beta y , \gamma x + \delta y |$$

une substitution de H', et supposons que, réduite à sa forme canonique, elle devienne

$$\dot{T} = | \xi , \eta \quad s_1 \xi , s_2 \eta |;$$

on sait que s_1 et s_2 sont les racines de la congruence

$$s^2 - (\alpha + \delta) s + \alpha\delta - \beta\gamma \equiv 0 \pmod{p},$$

et qu'on peut faire

$$\xi = (s_1 - \delta) x + \beta y, \qquad \eta = (s_2 - \delta) x + \beta y.$$

Exprimant S par les nouveaux indices on a

$$S = | \xi , \eta \quad \xi + A , \eta + B |,$$

où

$$A = (s_1 - \delta) a + \beta b, \qquad B = (s_2 - \delta) a + \beta b,$$

et l'on trouve

$$T^{-1} S T = | \xi , \eta \quad \xi + s_1 A , \eta + s_2 B |.$$

Pour que T soit permutable au groupe $K_{\frac{b}{a}}$, il faut que $T^{-1}ST = S^m$, d'où

$$(s_1 - m) A \equiv 0, \qquad (s_2 - m) B \equiv 0 \pmod{p}.$$

Donc si T n'appartient pas à la seconde espèce, il faut avoir

$$s_1 \equiv m, \quad B \equiv 0, \quad \text{ou} \quad s_2 \equiv m, \quad A \equiv 0.$$

Le nombre m étant réel par définition, on a le résultat suivant: parmi les substitutions de la première espèce de H' celles seulement qui sont réductibles à des formes canoniques réelles, peuvent être permutables à un groupe d'ordre p contenu dans I_0; inversement, chacune de ces substitutions est permutable à deux groupes, savoir

$$K_{\frac{\delta - s_2}{\beta}} \quad \text{et} \quad K_{\frac{\delta - s_1}{\beta}},$$

et n'est pas permutable aux autres.

Si T doit être échangeable à S, il faut de plus que l'un de ses multiplicateurs soit congru à 1; en supposant $s_1 \equiv 1$, on a

$$1 - \alpha - \delta + s_2 \equiv 0;$$

alors T est échangeable aux substitutions du groupe

$$K_{\frac{1-\alpha}{\beta}},$$

et il est en outre permutable au groupe $K_{\frac{\delta-1}{\beta}}$.

Soit maintenant T une substitution de H' de la première espèce et échangeable à S; réduite à sa forme canonique elle sera

$$T = |\xi, \eta \quad \xi, s_2\eta|,$$

et l'on aura

$$S = |\xi, \eta \quad \xi + A, \eta|.$$

Les substitutions de H' permutables au groupe $K_{\frac{b}{a}}$ ont la forme suivante

$$T' = |\xi, \eta \quad m_1\xi + r\eta, m_2\eta|;$$

mais on trouve

$$T^{-1}T'T.T'^{-1} = \left|\xi, \eta \quad \xi + r\frac{1-s_2}{s_2 m_1}\eta, \eta\right|,$$

ce qui montre qu'on doit avoir $r \equiv 0 \pmod{p}$. Il s'ensuit que toutes ces substitutions sont échangeables entre elles. En particulier les substitutions de H' échangeables à S sont les puissances d'une seule d'entre elles; soit T' cette substitution. De plus toute substitution de H' permutable à $K_{\frac{b}{a}}$ est le produit d'une puissance de T par une puissance d'une seule substitution

$$T_1 = |\xi, \eta \quad a_1\xi, b_1\eta|.$$

Les substitutions de G qui sont permutables à $K_{\frac{b}{a}}$ forment un groupe G_2, qui contient T_1 et les substitutions de G_1, mais ne contient aucun des groupes I_{n_1p+1}, I_{n_1p+2}, ... Par conséquent son ordre est égal à $p^2\pi_1\pi_2(n_1p+1)$, où π_2 est l'exposant de la plus petite puissance de a_1

congrue à 1. Le groupe G_2 est non-primitif, tout comme G_1; donc il existe un groupe G_2' du degré p, isomorphe à G_2; l'ordre de ce groupe est évidemment

$$p\pi_1\pi_2'(n_1p + 1),$$

π_2' désignant l'exposant de la plus petite puissance de b_1 congrue à une puissance de s_2. Si $\pi_2' > 1$, cela donne une nouvelle réduction des valeurs de n_1.

8. Supposons que H' soit du premier type, et supposons que ses substitutions soient ramenées à la forme canonique

$$|\,\xi, \eta \quad a\xi, b\eta\,|.$$

Si maintenant ξ et η sont imaginaires, a et b ne peuvent être réels sans être congrus (mod p), donc, outre la substitution identique, aucune substitution de H' n'est échangeable à une substitution de I_0. Par suite les nombres $n_1, n_2, \ldots$ sont nuls, et l'ordre de G est de la forme

$$O = p^2\pi(n'p^2 + 1),$$

π étant un diviseur de $p^2 - 1$.

Si au contraire ξ et η sont réels, il est permis de les remplacer par x et y. Parmi les groupes d'ordre p, contenus dans I_0, il n'y a que deux, savoir K_0 et K_∞, dont les substitutions sont échangeables à des substitutions non identiques de H'. Soit δ_1 l'ordre du groupe contenu dans H' dont les substitutions sont de la forme

$$|\,x, y \quad x, m_1y\,|,$$

et δ_2 l'ordre de celui dont les substitutions sont de la forme

$$|\,x, y \quad m_2x, y\,|;$$

on aura

$$\pi = \delta_1 . \delta_2 . \delta_3.$$

D'après les numéros 6 et 7, on a

$$O = p^2\pi(n'p^2 + n_1p + n_2p + 1),$$

π étant un diviseur de $(p-1)^2$. Le nombre

$$p\delta_1\delta_3(n_1p+1)$$

doit être l'ordre d'un groupe du degré p, contenant un autre de l'ordre

$$p\delta_1(n_1p+1);$$

pareillement

$$p\delta_2\delta_3(n_2p+1)$$

est l'ordre d'un groupe du degré p, contenant un autre du degré

$$p\delta_2(n_2p+1).$$

On a $n_1=0$ si $\delta_1=1$, et $n_2=0$ si $\delta_2=1$; quand p est de la forme $4h+3$, on a même $n_1=0$ si $\delta_1=2$, et $n_2=0$ si $\delta_2=2$. Les substitutions de H' étant toutes permutables aux groupes K_0, K_∞, l'ordre des groupes que nous avons désignés par G_2 est $p^2\pi(n_ip+1)$. Il s'ensuit que $n'p+n_2$ est divisible par n_1p+1, et $n'p+n_1$ divisible par n_2p+1.

9. Considérons le cas où H' appartient au deuxième type. La moitié des substitutions de H' ont la forme

$$S=|\,\xi,\eta\quad a\xi,b\eta\,|,$$

et forment un groupe H'' de l'ordre $\frac{\pi}{2}$; les autres sont de la forme

$$T=|\,\xi,\eta\quad c\eta,d\xi\,|.$$

Supposons *en premier lieu* que ξ et η soient réels; ils peuvent alors être remplacés par x et y, sans changer la forme du groupe I_0. Nous écrirons donc

$$S=|\,x,y\quad ax,by\,|,\qquad T=|\,x,y\quad cy,dx\,|.$$

Puisque H'' contient la substitution $T^{-1}ST=|\,x,y\quad bx,ay\,|$, les valeurs de a et de b sont les mêmes; elles sont donc les puissances d'une seule d'entre elles. Nous conserverons la lettre a pour désigner cette valeur, en la supposant racine primitive de la congruence

$$z^\delta\equiv 1\pmod p.$$

Le groupe H'' en contient un autre donc les substitutions ne font pas varier l'indice x; ce groupe est formé des puissances d'une seule substitution

$$\varphi = | x , y \quad x , a^{\delta'} y |;$$

on peut supposer que δ' soit un diviseur de δ; en faisant

$$\delta = \delta_1 \delta',$$

l'ordre du groupe dont nous parlons est δ_1. De plus H'' contient une substitution de la forme suivante:

$$\varphi' = | x , y \quad ax , a^t y |;$$

évidemment toutes ses substitutions sont contenues dans l'expression $\varphi^m \varphi'^{m'}$, et l'ordre de H'' est égal à $\delta_1^2 \delta'$, d'où

$$\pi = 2\delta_1^2 \delta'.$$

D'autre côté H'' dérive aussi des substitutions

$$\varphi_1 = T^{-1}\varphi T = | x , y \quad a^{\delta'} x , y |, \qquad \varphi_1' = T^{-1}\varphi' T = | x , y \quad a^t x , ay |.$$

En exprimant que φ_1' peut être égalé à $\varphi^m \varphi'^{m'}$, on obtient la congruence

$$t^2 - 1 \equiv 0 \pmod{\delta'}.$$

Les seules substitutions de H'' échangeables à des substitutions non identiques de I_0 sont donc les puissances de φ et de φ_1, qui sont échangeables respectivement aux substitutions des groupes K_0 et K_∞. Or, en supposant que G contienne $n_1 p + 1$ groupes d'ordre p^2 dont les substitutions sont échangeables à celles de K_0, on en déduit, en les transformant par T, un nombre égal qui ont leurs substitutions échangeables à celles de K_∞. Toutes les substitutions de H'' sont permutables aux groupes K_0, K_∞; le nombre des substitutions qu'elles produisent entre les cycles de chaque groupe est évidemment égal à δ.

Voyons maintenant dans quels cas une substitution de la forme T est échangeable à des substitutions de I_0. En réduisant T à sa forme canonique, on trouve

$$T = | \xi , \eta \quad \sqrt{cd}\,\xi , -\sqrt{cd}\,\eta |;$$

il faut donc que $cd \equiv 1 \pmod{p}$, donc

$$T = |\, x, y \quad cy, c^{-1}x \,|.$$

On obtient toutes les substitutions de H' de cette forme, en multipliant l'une d'elles par les substitutions de H'' dont les déterminants sont congrus à 1. Ce sont les substitutions

$$|\, x, y \quad a^{h\delta_3}x, a^{-h\delta_3}y \,|,$$

où l'on a fait

$$t + 1 = \delta_2\tau, \qquad \delta' = \delta_2\delta_3,$$

et par suite

$$\delta = \delta_1\delta_2\delta_3, \qquad \pi = 2\delta_1^2\delta_2\delta_3,$$

δ_3 et τ étant premiers entre eux. Le nombre h peut avoir les valeurs $0, 1, 2, \ldots, (\delta_1\delta_2 - 1)$. Donc, si H' contient une substitution de la forme $|\, x, y \quad cy, c^{-1}x \,|$, il en contient un nombre de $\delta_1\delta_2$.

Telle que nous l'avons déterminée, la substitution T est échangeable aux substitutions du groupe K_{c-1}, c'est-à-dire aux puissances de

$$|\, x, y \quad x + c, y + 1 \,|;$$

outre la substitution identique, elle est la seule substitution de H' qui possède cette propriété. Or, si G contient un groupe G_1 de l'ordre $p^2 . 2(n_2p + 1)$, dont les substitutions sont échangeables à celles de K_{c-1}, on en peut conclure l'existence d'un autre ayant ses substitutions échangeables à celles de K_{rc-1}, pourvu que G contienne une substitution qui transforme K_{c-1} en K_{rc-1}. Sans une connaissance plus intime du groupe G, nous ne pouvons chercher cette substitution que dans H''. Les substitutions de celui-ci transforment K_{c-1} en $K_{a^\mu c-1}$, le nombre μ pouvant être égalé à un multiple quelconque du plus grand commun diviseur de $\delta_2\delta_3$ et $t - 1$. Or on a vu que $\delta_2\delta_3$ divise $t^2 - 1$, et que δ_2 est le plus grand commun diviseur de $\delta_2\delta_3$ et $t + 1$, donc δ_3 divise $t - 1$. En désignant le plus grand commun diviseur de $\delta_2\delta_3$ et $t - 1$ par

$$\varepsilon\delta_3,$$

ε divisera $t - 1$ et $t + 1$; on a donc $\varepsilon = 1$ ou $\varepsilon = 2$.

Quand $\varepsilon = 1$, K_{c-1} peut être transformé en tout autre groupe d'ordre p qui a ses substitutions échangeables à une substitution de la forme T; donc tous les groupes G_1 correspondants sont de l'ordre $p^2 . 2(n_2 p + 1)$. Quand au contraire $\varepsilon = 2$, K_{c-1} ne peut être transformé qu'en $K_{c-1} a^{2h\delta_3}$; donc la moitié des groupes G_1 sont de l'ordre $p^2 . 2(n_2 p + 1)$, les autres pouvant être d'un ordre différent, $p^2 . 2(n_3 p + 1)$.

Le groupe K_{c-1} est permutable aux substitutions du groupe d'ordre $2\delta_1\delta_3\varepsilon$ qui dérive de T et des substitutions de la seconde espèce de H''. Ces substitutions produisent, entre les cycles de K_{c-1} un groupe dont l'ordre est égal à $2\delta_1\delta_3\varepsilon$ ou seulement à $\delta_1\delta_3\varepsilon$, suivant que $\delta_1\delta_3\varepsilon$ est impair ou pair. En effet, la substitution $-1 . T$ ne déplace pas les cycles de K_{c-1}.

On possède maintenant les données nécessaires pour appliquer les résultats du numéro 7. On a, si $\varepsilon = 1$

$$O = p^2\pi(n'p^2 + 2n_1 p + \delta_1\delta_2 n_2 p + 1),$$

et, si $\varepsilon = 2$,

$$O = p^2\pi\left(n'p^2 + 2n_1 p + \frac{\delta_1\delta_2}{2} n_2 p + \frac{\delta_1\delta_2}{2} n_3 p + 1\right).$$

Les nombres n_i sont compatibles avec l'existence d'un groupe du degré p et de l'ordre $p\pi_1\pi_2'(n_i p + 1)$, contenant un second groupe de l'ordre $p\pi_1(n_i p + 1)$. Pour $i = 1$ on a

$$\pi_1 = \delta_1, \qquad \pi_2' = \delta_2\delta_3;$$

pour $i = 2$ ou 3

$$\pi_1 = 2, \qquad \pi_2' = \frac{\delta_1\delta_3\varepsilon}{2} \quad \text{ou} \quad \delta_1\delta_3\varepsilon$$

suivant que $\delta_1\delta_3\varepsilon$ est pair ou impair. En particulier on a $n_1 = 0$ si $\delta_1 = 1$, ou si $\delta_1 = 2$ avec $p = 4h + 3$; on a $n_2 = n_3 = 0$ si $p = 4h + 3$, et toutes les fois que G ne contient pas de substitution de la forme $|x, y \quad cy, c^{-1}x|$. Enfin G contient des groupes des ordres

$$p^2\frac{\pi}{2}(n_1 p + 1), \quad p^2 . 2\delta_1\delta_3\varepsilon(n_2 p + 1) \quad \text{et} \quad p^2 . 2\delta_1\delta_3\varepsilon(n_3 p + 1).$$

Considérons en *second lieu* le cas où ξ, η sont imaginaires. Les substitutions de H' de la forme S sont les puissances d'une seule d'entre elles, que nous désignerons par

$$S = |\, \xi, \eta \quad a\xi, a^p\eta \,|,$$

en supposant a racine primitive de la congruence

$$z^m \equiv 1 \pmod{p};$$

elles forment un groupe H'' de l'ordre $\frac{\pi}{2}$. Le nombre m est un diviseur de $p^2 - 1$; en supposant

$$p^2 - 1 = m \cdot m',$$

on peut faire

$$a = j^{m'},$$

j étant une racine primitive de la congruence

$$z^{p^2-1} \equiv 1 \pmod{p}.$$

En posant

$$m = \delta_1\delta_2, \qquad p + 1 = \delta_1\delta_3,$$

δ_2 et δ_3 étant premiers entre eux, on a

$$m' = \delta_3\delta_4, \qquad p - 1 = \delta_2\delta_4, \qquad \pi = 2\delta_1\delta_2.$$

Outre la substitution identique, aucune substitution de H'' n'est échangeable à une substitution de I_0; en effet les multiplicateurs a^r, a^{rp} sont imaginaires ou égaux. Parmi les autres substitutions de H' les

$$T = |\, \xi, \eta \quad c\eta, c^{-1}\xi \,|$$

seules sont échangeables aux substitutions d'un groupe K; comme $c\eta, c^{-1}\xi$ sont des nombres conjugués, on a $c^{p+1} \equiv 1$. On obtient toutes les substitutions de H' de cette forme en multipliant l'une d'elles par les substitutions de H'' à déterminant 1, c'est-à-dire par les

$$|\, \xi, \eta \quad a^{h\delta_2}\xi, a^{ph\delta_2}\eta \,|.$$

Par suite ou H' ne contient aucune substitution de la forme

$$|\, \xi, \eta \quad r\eta, r^{-1}\xi \,|,$$

ou il en contient δ_1, savoir les

$$\text{(a)} \qquad \left| \xi, \eta \quad a^{h\delta_2} c\eta, a^{-h\delta_2} c^{-1}\xi \right|.$$

En transformant T par S^{-t}, on trouve

$$S^t T S^{-t} = \left| \xi, \eta \quad a^{(p-1)t} c\eta, a^{-(p-1)t} c^{-1}\xi \right|;$$

or on peut rendre $a^{(p-1)t}$ ou $a^{\delta_2\delta_4 t}$ congru à

$$a^{h\varepsilon\delta_2},$$

où h est un entier quelconque, ε désignant le plus grand commun diviseur de δ_1 et δ_4; on a $\varepsilon = 2$ si δ_1 et δ_4 sont pairs, $\varepsilon = 1$ dans les autres cas. Donc si $\varepsilon = 1$, les δ_1 substitutions (a) peuvent être transformées les unes dans les autres par les substitutions de H'; au contraire, si $\varepsilon = 2$, on en peut déduire la moitié de la substitution T, l'autre moitié de $a^{\delta_2} T$. Dans le premier cas tous les groupes G_1 qui répondent aux diverses substitutions (a) ont le même ordre $p^2 . 2(n_1 p + 1)$, dans le second la moitié des groupes G_1 sont de l'ordre $p^2 . 2(n_1 p + 1)$, les autres pouvant avoir un ordre différent $p^2 . 2(n_2 p + 1)$.

Enfin le groupe formé des substitutions de H' qui sont permutables au groupe K_{c-1} dérive de T et des substitutions de la seconde espèce contenues dans H'' savoir les

$$\left| \xi, \eta \quad a^{\frac{h\delta_1}{\varepsilon}} \xi, a^{\frac{h\delta_1}{\varepsilon}} \eta \right|;$$

l'ordre de ce groupe est donc $2\delta_2\varepsilon$; il produit entre les cycles de K_{c-1} un groupe dont l'ordre est $2\delta_2\varepsilon$ ou $\delta_2\varepsilon$ suivant que $\delta_2\varepsilon$ est impair ou pair.

En vertu du numéro 7, on peut maintenant faire les conclusions suivantes:

Si $\varepsilon = 1$, on a

$$O = p^2\pi(n'p^2 + \delta_1 n_1 p + 1);$$

si $\varepsilon = 2$,

$$O = p^2\pi\left(n'p^2 + \frac{\delta_1}{2} n_1 p + \frac{\delta_1}{2} n_2 p + 1\right);$$

il existe des groupes du degré p des ordres

$$p . 2(n_1 p + 1), \; p . 2(n_2 p + 1)$$

contenus dans d'autres groupes, dont les ordres sont respectivement

$$p.2\delta_2\varepsilon(n_1p+1),\ p.2\delta_2\varepsilon(n_2p+1),\quad \text{si } \delta_2\varepsilon \text{ est impair,}$$

ou

$$p\delta_2\varepsilon(n_1p+1),\ p\delta_2\varepsilon(n_2p+1),\quad \text{si } \delta_2\varepsilon \text{ est pair.}$$

On a $n_1 = n_2 = 0$, quand p est de la forme $4h+3$, et quand le groupe G ne contient pas de substitution de la forme

$$|\xi, \eta \quad c\eta, c^{-1}\xi|.$$

Enfin le groupe G en contient d'autres des ordres

$$p^2.2\delta_2\varepsilon(n_1p+1),\ p^2.2\delta_2\varepsilon(n_2p+1).$$

10. Quand H' est tétraédrique, le nombre p est >3. Les substitutions de H' sont les

$$a,\ aA,\ aB,\ aAB,\ aC^r,\ aA^{-1}C^rA,\ aB^{-1}C^rB,\ aB^{-1}A^{-1}C^rAB,$$

les lettres ayant la même signification qu'au numéro 5. Les substitutions aA sont permutables aux groupes K_0, K_∞, pourvu que ξ et η soient réels. Cela exige que -1 soit résidu quadratique de p, c'est-à-dire que p soit de la forme $4h+1$. Or si H' contient la substitution i ou $|\xi, \eta \quad i\xi, i\eta|$, il contient iA et $-iA$, qui sont échangeables respectivement aux substitutions des groupes K_∞ et K_0. Comme on a

$$B^{-1}iAB = -iA,$$

les deux groupes G_1 qui correspondent à K_0 et à K_∞ sont les transformés l'un de l'autre; ils sont donc d'un même ordre $p^2.2(n_1p+1)$. En transformant $\pm iA$ par C et C^2, on en déduit $\pm iB$, $\pm iAB$; donc G contient six groupes de l'espèce que nous avons désignée par G_1, tous de l'ordre $p^2.2(n_1p+1)$. Les groupes G_1' du degré p qui y correspondent ont pour ordre $p.2(n_1p+1)$. Les groupes G_2 qui répondent aux six groupes G_1 sont évidemment de l'ordre $p^2.2\omega(n_1p+1)$; mais comme la substitution iA ne permute pas les cycles de K_0, l'ordre des groupes G_2' sera $p.\omega(n_1p+1)$.

Le déterminant de la substitution aC étant a^2m^2, sa congruence caractéristique est

$$s^2 - ams + a^2m^2 \equiv 0 \pmod{p},$$

d'où

$$s \equiv am\frac{1 \pm \sqrt{-3}}{2}.$$

Pour que la forme canonique de aC soit réelle, il faut donc que p soit de la forme $3h + 1$. On trouve ainsi

$$aC = \left| \xi', \eta' \quad am\frac{1+\sqrt{-3}}{2}\xi', am\frac{1-\sqrt{-3}}{2}\eta' \right|.$$

La condition relative au nombre p étant remplie, aC est permutable à deux des groupes K, que nous désignerons par K', K''. Les substitutions aC^r sont les seules permutables à ces groupes; en effet, dans le cas contraire, H' contiendrait un groupe d'un ordre au moins égal à 6ω, à substitutions échangeables entre elles (n° 7); par conséquent il existerait, entre quatre lettres, un groupe de l'ordre 6 ou 12, contenant exclusivement des substitutions échangeables entre elles, ce qui est absurde. Or, si l'on a

$$a \equiv \frac{1}{m}\frac{1-\sqrt{-3}}{2},$$

la substitution aC est échangeable aux substitutions de K'; si

$$a \equiv \frac{1}{m}\frac{1+\sqrt{-3}}{2}$$

elle est échangeable à celles de K''. Dans le premier cas H' contient la substitution $m\frac{1+\sqrt{-3}}{2}$, dans le second $m\frac{1-\sqrt{-3}}{2}$; s'il contient l'une et l'autre, il contient leur produit m^2, et, en vertu du n° 5, m^3, et par suite m, c'est-à-dire qu'on peut faire $m = 1$. Soient, pour abréger, C' et C'' les substitutions qui répondent aux deux valeurs de a:

$$C' = \left| \xi', \eta' \quad \xi', -\frac{1+\sqrt{-3}}{2}\eta' \right|, \qquad C'' = \left| \xi', \eta' \quad -\frac{1-\sqrt{-3}}{2}\xi', \eta' \right|;$$

C'' n'est pas la transformée de C' par une substitution de H'; c'est ce

qu'on voit sans calcul, en se souvenant de la correspondance qui a lieu entre les substitutions de H' et celles du groupe alterné entre quatre lettres. L'ordre du groupe G_1, formé par les substitutions de G échangeables à celles de K', peut évidemment être exprimé par $p^2.3(n_2p+1)$; celui de G_1' est donc $p.3(n_2p+1)$. Le groupe G_2 est de l'ordre $p^2.3\omega(n_2p+1)$. Or les substitutions communes à G_2 et H' sont les aC^r; s'il s'en trouve parmi elles qui ne permutent pas les cycles de K', ce ne peut être que les puissances de C''; cette circonstance ne se présente donc que dans le cas où l'on peut faire $m=1$. Par suite l'ordre du groupe G_2' sera $p\omega(n_2p+1)$ si $m=1$; mais il sera $p.3\omega(n_2p+1)$ dans le cas contraire. Quant aux groupes analogues qui répondent à K'', il suffit de remplacer n_2 par une autre lettre n_3. Des substitutions C', C'' on déduit, en les transformant par A, B, AB, six autres substitutions, échangeables respectivement aux substitutions de six autres des groupes K_r. Donc on a quatre groupes de l'espèce G_1 qui sont de l'ordre $p^2.3(n_2p+1)$, et quatre de l'ordre $p^2 3(n_3p+1)$.

De ce qui précède on tire les conclusions suivantes:

L'ordre de G est déterminé par la formule

$$O = p^2.12\omega(n'p^2+6n_1p+4n_2p+4n_3p+1).$$

On a $n_1=0$, quand p est de la forme $12h+7$ ou $12h+11$, et quand H' ne contient pas la substitution i,

$n_2=n_3=0$, quand p est de la forme $12h+5$ ou $12h+11$,

$n_2=0$, quand G ne contient pas la substitution $m\frac{1+\sqrt{-3}}{2}$,

$n_3=0$, quand G ne contient pas la substitution $m\frac{1-\sqrt{-3}}{2}$.

Les nombres n_r sont compatibles avec l'existence d'un groupe du degré p et de l'ordre $p.\pi_1.\pi_2'(n_rp+1)$, contenant un groupe de l'ordre $p.\pi_1(n_rp+1)$; pour $r=1$ on a $\pi_1=2$, $\pi_2'=\frac{\omega}{2}$; pour $r=2$ et $r=3$, on a $\pi_1=3$, et, si H' contient la substitution m, $\pi_2'=\frac{\omega}{3}$; dans le cas contraire on a $\pi_2'=\omega$. Enfin G contient des groupes des ordres

$$p^2.2\omega(n_1p+1),\ p^2.3\omega(n_2p+1),\ p^2.3\omega(n_3p+1).$$

11. Quand H' est octaédrique, on a aussi $p > 3$. Les substitutions de H' sont: les substitutions d'un groupe tétraédrique où l'on a $m = 1$, les 6ω transformées des aD, les 6ω transformées des aBD. On connaît déjà les groupes K_r qui sont permutables aux substitutions tétraédriques, et l'on connaît les substitutions tétraédriques qui sont échangeables aux substitutions de ces groupes; mais évidemment on ne peut employer immédiatement ce qui a été dit sur l'ordre des groupes G_1, G_1', G_2, G_2' qui s'y rapportent.

Les substitutions aD ou $|\xi, \eta \quad ae\xi, aei\eta|$ sont permutables aux groupes K_0 et K_∞, comme le sont les aA, pourvu que $p = 4h + 1$; en effet e est réel en même temps que ξ. Donc le groupe G_1 correspondant à K_0 est de l'ordre $p^2.2(n_1p + 1)$, si H' contient la substitution i, mais ne contient pas e. Si H' contient e il contient aussi i; en effet D^2A se réduit à e^2i; dans ce cas l'ordre de G_1 est $p^2.4(n_1p + 1)$. Le groupe G_2 est de l'ordre $p^2.4\omega(n_1p + 1)$; G_2' est de l'ordre $p\omega(n_1p + 1)$, quand H' contient e, mais de l'ordre $p.2\omega(n_1p + 1)$ dans le cas contraire; c'est ce qu'on voit en remarquant que la substitution $e^{-1}i^{-1}D$ ne permute pas les cycles de K_0.

On a vu, au numéro précédent, que les substitutions aC^r sont permutables aux deux groupes K', K''; évidemment elles sont les seules substitutions de H' permutables à ces groupes. Dans le cas qui nous occupe, les groupes K', K'', ainsi que les substitutions C'^r, C''^r, se transforment l'un dans l'autre au moyen de la substitution

$$F = ABD.$$

En effet, dans le groupe symétrique entre les lettres $\alpha, \beta, \gamma, \delta$, qui est isomorphe à H', la substitution $(\alpha\beta\gamma)$ correspond à C, $(\alpha\beta)$ à F, donc $F^{-1}CF$ et C^2 correspondent à $(\alpha\gamma\beta)$ d'où

$$F^{-1}CF = aC^2;$$

comme d'ailleurs C a son déterminant congru à 1, on doit avoir

$$F^{-1}CF = \pm 1 . C^2,$$

d'où

$$F^{-1}C^3F = \pm 1 . C^6;$$

or, comme on a $C^3 = -1$, on en conclut qu'il faut prendre le signe inférieur, donc

$$F^{-1}CF = -C^2.$$

En faisant, pour un moment, $\alpha = \frac{1-\sqrt{-3}}{2}$, on a

$$\alpha C = C', \qquad \frac{1}{\alpha} C = C'',$$

$$F^{-1}C'F = -\alpha C^2 = \frac{1}{\alpha^2} C^2 = C''^2,$$

$$F^{-1}C''F = -\frac{1}{\alpha} C^2 = \alpha^2 C^2 = C'^2.$$

Ainsi, dans le résultat final, les deux termes au coefficient 4 qui se présentent dans le cas où H est tétraédrique, se réunissent ici en un seul terme au coefficient 8. Les ordres des groupes G_1, G_1', G_2, G_2' sont évidemment les mêmes que dans le cas précédent en supposant $m = 1$.

On a

$$aBD = |\, \xi, \eta \quad ae\eta, \; ae i\xi \,|;$$

la congruence caractéristique de cette substitution étant

$$\sigma^2 + a^2 e^2 i \equiv 0 \pmod{p},$$

elle se réduit à la forme canonique

$$aBD = |\, \xi', \eta' \quad ae\sqrt{-i}\,\xi', \; -ae\sqrt{-i}\,\eta' \,|.$$

Pour que ξ', η' soient réels, il faut que $e\sqrt{-i}$ le soit. En supposant $p = 4h + 1$, e est réel; par conséquent il faut que $-i$ soit résidu quadratique de p, c'est-à-dire que p doit être de la forme $8h' + 1$. A cette condition aBD est permutable à deux des groupes K_r, que nous désignerons par K''', K''''; d'autre côté on voit que les a et aBD sont les seules substitutions de H' permutables à ces groupes. Si maintenant H' contient la substitution $e\sqrt{-i}$, on peut faire

$$a = \pm \frac{1}{e\sqrt{-i}};$$

on obtient ainsi les deux substitutions

$$|\xi', \eta' \quad \xi', -\eta'|, \qquad |\xi', \eta' \quad -\xi', \eta'|,$$

échangeables respectivement aux substitutions de K''' et de K''''. D'ailleurs ces substitutions sont les transformées l'une de l'autre, car en effet on a

$$A^{-1}BDA = -BD;$$

K'''' est donc la transformée de K''' par A. Il s'ensuit qu'en transformant le groupe G_1 correspondant à K''' par les substitutions de H', on obtient douze groupes G_1; tous de l'ordre $p^2.2(n_3p+1)$. Les groupes G_1', G_2, G_2' ont respectivement pour ordre $p.2(n_3p+1)$, $p^2.2\omega(n_3p+1)$, $p\omega(n_3p+1)$, comme on le voit aisément.

Quand $p = 4h+3$, le nombre n_3 est nécessairement nul; en effet la supposition contraire entraînerait l'existence d'un groupe du degré p et de l'ordre $p.2(n_3p+1)$.

On a donc le résultat suivant:

$$O = p^2.24\omega.(n'p^2 + 6n_1p + 8n_2p + 12n_3p + 1);$$

$n_1 = 0$, quand $p = 24h+7, 11, 19, 23$, et quand H' ne contient pas la substitution i;

$n_2 = 0$, quand $p = 24h+5, 11, 17, 23$, et quand H' ne contient pas la substitution $\frac{1+\sqrt{-3}}{2}$;

$n_3 = 0$, quand $p = 24h+5, 7, 11, 13, 19, 23$, et quand H' ne contient pas la substitution $e\sqrt{-i}$.

Les nombres n_r admettent l'existence d'un groupe du degré p et de l'ordre $p\pi_1\pi_2'(n_rp+1)$, contenant un autre de l'ordre $p\pi_1(n_rp+1)$, où les nombres π_1, π_2' sont déterminés de la manière suivante:

pour $r=1$, on a $\pi_1 = 4$, $\pi_2' = \frac{\omega}{4}$, ou $\pi_1 = 2$, $\pi_2' = \omega$, suivant que H' contient e ou non.

$r = 2, \quad \pi_1 = 3, \quad \pi_2' = \frac{\omega}{3};$

$r = 3, \quad \pi_1 = 2, \quad \pi_2' = \frac{\omega}{2}.$

Enfin le groupe G contient des groupes des ordres

$$p^2.4\omega(n_1p+1),\ p^2.3\omega(n_2p+1),\ p^2.2\omega(n_3p+1).$$

12. Quand H' est icosaédrique, le nombre p est de l'une des formes $10h+1$, $10h-1$. Par une analyse toute semblable à la précédente on trouve:

$$O=p^2.60\omega(n'p^2+12n_1p+20n_2p+30n_3p+1),$$

où

$n_1=0$, quand $p=60h+19, 29, 49, 59$, et quand H' ne contient pas la substitution θ;

$n_2=0$, quand $p=60h+11, 29, 41, 59$, et quand H' ne contient pas la substitution $\frac{1+\sqrt{-3}}{2}$;

$n_3=0$, quand $p=60h+11, 19, 31, 59$, et quand H' ne contient pas la substitution i.

Le nombre n_r admet l'existence d'un groupe du degré p et de l'ordre $p\omega(n_rp+1)$, contenant un autre de l'ordre $p\pi_1(n_rp+1)$, où pour $r=1,2,3$, le nombre π_1 est respectivement égal à $5, 3, 2$. Le groupe G contient des groupes des ordres $p^2.5\omega(n_1p+1)$, $p^2.3\omega(n_2p+1)$, $p^2.2\omega(n_3p+1)$.

On remarque que dans les cas où H' est de l'une des trois types polyédriques, les coefficients qui, dans l'expression de O, multiplient les termes en n_rp, sont les nombres des sommets, des faces et des arêtes des polyèdres correspondants.

13. Le cas où G est de la seconde espèce, α étant nul, est facile à traiter. En effet, I_0 ne contient que les puissances de la substitution

$$t=|\,x, y \quad x+(y)_{p-1}, y+1\,|;$$

par conséquent il ne contient qu'un seul groupe K de l'ordre p, qui est formé des substitutions

$$t^{ap}=|\,x, y \quad x+a, y\,|.$$

En supposant K contenu dans n_1 des groupes I_r, il existera un groupe G_1' du degré p et de l'ordre $p\pi_1(n_1p+1)$, où le nombre π_1 est l'ordre

du groupe renfermant les substitutions de H' échangeables à t^p. Or, les substitutions de H' étant toutes de la forme

$$\left| x, y \quad ax + E\left(\frac{ay}{p}\right), ay \right|,$$

on a évidemment $\pi_1 = 1$, d'où $n_1 = 0$. Donc l'ordre de G est exprimé par la formule

$$O = p^2\pi(n'p^2 + 1).$$

14. De ce qui est dit aux numéros précédents on peut conclure que, si $\alpha = 0$ et $\pi = 1$, on a $n = 0$. En effet, sous cette hypothèse le groupe G est de l'ordre $p^2(n'p^2 + 1)$, et contient $n'p^2 + 1$ groupes de l'ordre p^2. Deux quelconques de ces groupes n'ayant en commun que la substitution identique, le nombre des substitutions des ordres p et p^2 est égal à $(p^2 - 1)(n'p^2 + 1)$; ces substitutions déplacent tous les éléments. Les substitutions qui ne déplacent pas un élément donné quelconque $u_{x,y}$ sont en nombre $n'p^2 + 1$; par conséquent elles coïncident avec les $n'p^2 + 1$ substitutions dont l'ordre est premier à p, en d'autres termes, ces dernières ne déplacent aucun élément. Donc $n' = n = 0$.

On a ainsi le théorème suivant, analogue au premier des théorèmes de M. Mathieu, cités plus haut:

Tout groupe transitif G du degré p^2 contient un groupe transitif Γ d'ordre p^2; si G ne contient pas de groupe plus général dont les substitutions sont permutables à Γ, G coïncide avec Γ.

15. Soit maintenant $\alpha = 1$, et supposons que G soit de la première espèce. Un groupe K de l'ordre p^2 contenu dans I_0 et I_1 pourrait être transitif ou intransitif. Si K est intransitif il est formé des substitutions $\theta^m\theta_1^{m_1}$; une substitution T de I_1, étrangère à K, transformera θ_0 en θ_0^a, car évidemment θ_0 et ses puissances sont les seules substitutions de K qui déplacent tous les éléments. Par conséquent T aura la forme suivante:

$$T = | x, y \quad ax + \varphi_1(y), \varphi_2(y) |.$$

De plus T transformera θ_1 en $\theta^b\theta_1^c$, ce qui donne

$$T = \left| x, y \quad ax + \varphi_1(y), \frac{a}{c}y - \frac{b}{c} \right|.$$

Pour que cette substitution soit de l'ordre p, il faut que

$$a \equiv c \equiv 1 \pmod{p};$$

mais alors T serait contenu dans I_0, ce qui est absurde. Donc le groupe K ne peut être intransitif.

Si K est transitif, il dérive de deux substitutions échangeables entre elles, S et T, dont l'une fait varier l'indice y; on peut donc supposer

$$S = \theta_0^a \theta_1^b t, \qquad T = \theta_0^c \theta_1^d;$$

mais on trouve

$$S^{-1}TS = t^{-1}Tt = \theta_0^{c-d}\theta_1^d,$$

donc d est égal à zéro. Par conséquent il est permis de faire

$$S = \theta_1^b t, \qquad T = \theta_0.$$

Or I_1 dérive des trois substitutions θ_0', θ_1', t' analogues respectivement à θ_0, θ_1, t, et l'on voit que θ_0', qui est échangeable à θ_1' et à t', ne peut être étrangère à K; en effet, dans ce cas, les p^3 substitutions de I_1 seraient échangeables entre elles, ce qui est absurde. De plus, θ_0' ne peut être une puissance de θ_0, car alors I_1, étant entièrement déterminé par θ_0' et S, se confondrait avec I_0. Donc on peut supposer

$$\theta_0' = \theta_0^a \theta_1^b t, \qquad t' = \theta_0.$$

Ces substitutions déterminent complètement I_1; d'ailleurs, aux p valeurs qu'on peut donner au nombre a répondent p groupes de l'ordre p^3, tous contenant K et contenus dans G; en effet on a

$$\theta_1^{-c}\theta_0'\theta_1^c = \theta_0^{a+c}\theta_1^b t, \qquad \theta_1^{-c}t'\theta_1^c = t' = \theta_0.$$

Il en résulte que le groupe G contient un groupe G_1, dont les substitutions sont permutables à K, et dont l'ordre est égal à

$$p^3\pi'(p+1),$$

π' étant un diviseur de π. D'autre part, G ne contient d'autres groupes de la même espèce que G_1; c'est ce que nous démontrerons, en faisant

voir qu'on a nécessairement $b = 0$. Pour simplifier les calculs, introduisons, au lieu de x, le nombre

$$\xi = x - b(y)_2.$$

On trouve

$$\theta_0 = t' = |\,\xi, y \quad \xi + 1, y\,|, \qquad \theta_1 = |\,\xi, y \quad \xi + y, y\,|,$$

$$t = |\,\xi, y \quad \xi - by, y + 1\,|, \qquad \theta_0' = \theta_1' t = |\,\xi, y \quad \xi, y + 1\,|.$$

La substitution θ_1' doit être échangeable à θ_0', en ne faisant pas varier l'indice ξ; elle doit en outre satisfaire à la relation

$$t'^{-1}\theta_1' t' = \theta_0'^{-1}.\theta_1';$$

donc elle aura la forme suivante

$$\theta_1' = |\,\xi, y \quad \xi, y + \xi + a\,|.$$

Ainsi le groupe G_1, contenant les deux substitutions

$$|\,\xi, y \quad \xi + y, y\,|, \qquad |\,\xi, y \quad \xi, y + \xi\,|,$$

contiendra toute substitution linéaire et homogène par rapport aux indices ξ, y dont le déterminant est congru à 1 (mod p) (voir le *Traité des substitutions* de M. JORDAN, n° 121), entre autres celle-ci

$$\left|\xi, y \quad r\xi, \frac{1}{r}y\right| = \left|x, y \quad rx + b\frac{r^2 - 1}{2r}y - b\frac{r^3 - 1}{2r^2}y^2, \frac{1}{r}y\right|,$$

où r peut avoir toute valeur non congrue à zéro. Or cette substitution appartient évidemment au groupe H; donc comme nous avons supposé que les substitutions de ce groupe soient contenues dans l'expression

$$|\,x, y \quad \alpha x + \beta y + \gamma, \delta y + \varepsilon\,|,$$

il faut qu'on ait $b = 0$, comme nous l'avons annoncé. On a vu en même temps que le groupe H contient toutes les substitutions

$$\left|x, y \quad rx, \frac{1}{r}y\right|;$$

comme d'ailleurs toutes les substitutions de H sont permutables à K, on

a $\pi' = \pi$. L'ordre de G_1 est donc $O' = p^3\pi(p+1)$, celui de G est $O = p^3\pi(n'p^2 + p + 1)$, ou bien, puisque O est divisible par O',

$$O = p^3\pi(p+1)(n''p^2+1).$$

Le résultat final se résume donc comme il suit:

Si $\alpha = 1$, et que G soit de la première espèce, on a ou

$$O = p^3\pi(n'p^2+1),$$

π étant un diviseur de $(p-1)^2$, ou

$$O = p^3(p-1)\pi_1(p+1)(n'p^2+1) = \frac{p^2(p^2-1)(p^2-p)}{\delta}(n'p^2+1),$$

$\pi_1 = \frac{p-1}{\delta}$ étant le nombre des substitutions de la forme $|x, y \quad ax, y|$ contenues dans G. Quand la première formule a lieu, G ne contient d'autres substitutions linéaires que celles de H. En effet, si la substitution linéaire S est étrangère à H et, par suite, non permutable à I_0, le groupe I_1, transformé de I_0 par S, contiendra le groupe (ϑ_0, t), ce qui est contre l'hypothèse, si S appartient à G.

16. Passons au cas où G est de la seconde espèce, α étant égal à 1. D'abord on voit, comme au numéro précédent, qu'un groupe K de l'ordre p^2, contenu dans I_0 et I_1, ne peut être intransitif. Si K était transitif, il serait formé des puissances d'une seule substitution

$$t' = \theta^a\theta_1^b t,$$

mais alors I_0 et I_1, étant complètement déterminés par la substitution t', se confondraient, ce qui est contre l'hypothèse. Ainsi deux des groupes I_r ne peuvent contenir un même groupe d'ordre p^2. Donc

$$O = p^3\pi(n'p^2+1),$$

π étant un diviseur de $p-1$.

17. Dans les cas où $\alpha > 1$, deux quelconques des groupes I_r, par exemple I_0 et I_1, ne peuvent contenir un même groupe transitif dont l'ordre surpasse p^2. En effet ce dernier groupe contiendrait nécessaire-

ment ϑ_0, ϑ_1 et une substitution de la forme $\vartheta_2^{m_2}\vartheta_3^{m_3}\dots\vartheta_\alpha^{m_\alpha}t$; or ces substitutions déterminent complètement le groupe de l'ordre $p^{\alpha+2}$ qui les contient, de sorte que I_0 et I_1 se confondraient. Donc si I_0 et I_1 contiennent un même groupe K de l'ordre $p^{\alpha+1}$, celui-ci est intransitif, et par suite il dérive des substitutions $\vartheta_0, \vartheta_1, \dots, \vartheta_\alpha$. Cherchons les substitutions qui sont permutables à K.

Nous désignons par $c_0, c_1, \dots, c_{p-1}$ les cycles de ϑ_0, de sorte que c_y soit une substitution qui permute circulairement les éléments dont le second indice est congru à y, et qu'on ait

$$\vartheta_0 = \prod_0^{p-1} {}_y c_y .$$

Si maintenant U désigne une substitution permutable à K, U transformera chaque substitution c_y en une puissance d'une autre, par exemple c_y en $c_{\psi(y)}^{f(y)}$; donc on a

$$U = |\, x, y \quad xf(y) + f_1(y), \psi(y) \,|.$$

Or, comme K est permutable à t, et contient la substitution

$$\vartheta_\alpha = c_\alpha \cdot c_{\alpha+1}^{(\alpha+1)_\alpha} \cdot c_{\alpha+2}^{(\alpha+2)_\alpha} \dots c_{p-1}^{(p-1)_\alpha},$$

il contient en général la suivante

$$c_z \cdot c_{z+1}^{(\alpha+1)_\alpha} \cdot c_{z+2}^{(\alpha+2)_\alpha} \dots c_{p-\alpha+z-1}^{(p-1)_\alpha} = S_z .$$

Evidemment K dérive des substitutions $S_0, S_1, \dots, S_{p-1}$; donc pour que U soit permutable à K, il est nécessaire et il suffit que U transforme chacune des substitutions S_z en une substitution T de K, laquelle, comme S_z, est composée de $p - \alpha$ cycles. Les substitutions de K ayant la forme

$$|\, x, y \quad x + F(y), y \,|,$$

où $F(y)$ est une fonction entière de y du degré α, on trouve les substitutions T en déterminant la fonction $F(y)$ de manière qu'elle s'annule pour α valeurs incongrues par rapport au module p. Soit $y_0, y_1, \dots, y_{\alpha-1}$ ces valeurs; on aura

$$F(y) = M(y - y_0)(y - y_1) \dots (y - y_{\alpha-1}),$$

M étant une constante, et

$$T = | x, y \quad x + F(y), y | = \Pi c_y^{F(y)}.$$

Comme d'ailleurs K contient toutes ces substitutions, on peut énoncer le critérium de la manière suivante: il faut et il suffit que U transforme les substitutions T les unes dans les autres. Or on a

$$U^{-1}TU = \Pi c_{\psi(y)}^{f(y).F(y)},$$

donc il faut que

$$f(y).F(y) \equiv F'[\psi(y)]$$

$$\equiv M'[\psi(y) - \psi(y_0)][\psi(y) - \psi(y_1)] \ldots [\psi(y) - \psi(y_{\alpha-1})] \pmod p,$$

ou bien, en posant $\frac{M'}{M} \equiv N$,

$$(7) \qquad f(y) \equiv N \frac{[\psi(y) - \psi(y_0)][\psi(y) - \psi(y_1)] \ldots [\psi(y) - \psi(y_{\alpha-1})]}{(y - y_0)(y - y_1) \ldots (y - y_{\alpha-1})} \pmod p.$$

Quand $\alpha = p - 1$, cette congruence ne dit rien, puisque on ne peut donner à y d'autre valeur que y_{p-1}, sans annuler le numérateur et le dénominateur. Et, en effet, toute substitution de la forme

$$| x, y \quad xf(y) + f_1(y), \psi(y) |$$

est dans ce cas permutable à K, qui contient toutes les substitutions c_y.

Quand $\alpha = p - 2$, on peut faire $y = y_{p-1}$, et $y = y_{p-2}$; on trouve ainsi, en vertu du théorème de WILSON,

$$\frac{f(y_{p-1})}{y_{p-1} - y_{p-2}} \equiv \frac{N}{\psi(y_{p-1}) - \psi(y_{p-2})}, \qquad \frac{f(y_{p-2})}{y_{p-2} - y_{p-1}} \equiv \frac{N}{\psi(y_{p-2}) - \psi(y_{p-1})},$$

d'où

$$f(y_{p-1}) \equiv f(y_{p-2});$$

comme d'ailleurs y_{p-1} et y_{p-2} sont arbitraires, on conclut que $f(y)$ est constant. Donc si $\alpha = p - 2$, on a

$$U = | x, y \quad ax + f_1(y), \psi(y) |.$$

En effet, K dérive des substitutions $c_y . c_{y+1}^{-1}$, ou bien des $c_y . c_{y_1}^{-1}$, lesquelles par U sont transformées en $c_{\psi(y)}^{a} . c_{\psi(y_1)}^{-a}$.

Supposons maintenant $\alpha < p-2$, $\alpha > 0$, et par conséquent $p > 3$. En faisant dans la congruence (7) successivement $y = y_{p-1}$, $y = y_{p-2}$, et divisant les résultats, on a

$$\frac{f(y_{p-1})}{f(y_{p-2})} \tag{8}$$

$$\equiv \frac{[\psi(y_{p-1})-\psi(y_0)][\psi(y_{p-1})-\psi(y_1)]\cdots[\psi(y_{p-1})-\psi(y_{\alpha-1})]}{[\psi(y_{p-2})-\psi(y_0)][\psi(y_{p-2})-\psi(y_1)]\cdots[\psi(y_{p-2})-\psi(y_{\alpha-1})]} \cdot \frac{(y_{p-2}-y_0)(y_{p-2}-y_1)\cdots(y_{p-2}-y_{\alpha-1})}{(y_{p-1}-y_0)(y_{p-1}-y_1)\cdots(y_{p-1}-y_{\alpha-1})}.$$

Cette congruence, linéaire en y_0 et $\psi(y_0)$, peut être mise sous la forme suivante

$$\psi(y_0) \equiv \frac{Ay_0 + B}{Cy_0 + D}. \tag{9}$$

Or on peut évidemment remplacer y_0 par chacun des nombres $y_\alpha, y_{\alpha+1}, \ldots, y_{p-3}$, sans autre changement; de plus la congruence (9) est aussi satisfaite en remplaçant y_0 par y_{p-1} ou par y_{p-2}, puisque par là (8) est satisfaite identiquement. Donc on a

$$\psi(y) \equiv \frac{Ay + B}{Cy + D} \tag{10}$$

pour $y \equiv y_0, y_\alpha, y_{\alpha+1}, \ldots, y_{p-1}$; le nombre de ces valeurs, $p - \alpha + 1$, est au moins égal à 4.

En traitant y_1 comme on a traité y_0, on tire de (8) une nouvelle congruence

$$\psi(y) \equiv \frac{A'y + B'}{C'y + D'},$$

qui a lieu pour les valeurs suivantes de y:

$$y_1, y_\alpha, y_{\alpha+1}, \ldots, y_{p-1}.$$

Donc on a

$$\frac{Ay + B}{Cy + D} \equiv \frac{A'y + B'}{C'y + D'}$$

pour les valeurs $y_\alpha, y_{\alpha+1}, \ldots, y_{p-1}$, dont le nombre est égal ou supérieur à 3, donc cette congruence est identique, c'est-à-dire que la congruence (10) est satisfaite par $y \equiv y_1$. On démontre de la même manière qu'elle

est satisfaite par $y \equiv y_2, y_3, \ldots, y_{\alpha-1}$. Donc enfin elle est satisfaite par toute valeur de y; comme d'ailleurs $\phi(y)$ ne peut être infini, ni constant, on conclut que

$$C \equiv 0, \qquad \phi(y) \equiv cy + d.$$

En reportant cette valeur dans (8), il vient

$$f(y_{p-1}) \equiv f(y_{p-2});$$

y_{p-1} et y_{p-2} étant arbitraires, cela veut dire que $f(y)$ est une constante. Donc on a

$$U = | x, y \quad ax + f_1(y), cy + d |.$$

Par ce résultat on est en mesure de traiter en même temps tous les cas où $\alpha > 1$, $\alpha < p - 2$. En effet la substitution U ne peut être de l'ordre p où p^2 que si $a \equiv c \equiv 1 \pmod{p}$, mais alors U est contenue dans I_0. Par suite ce groupe n'a aucun groupe de l'ordre $p^{\alpha+1}$ en commun avec un autre des groupes I_r. On peut donc conclure que, si $\alpha > 1$, $\alpha < p - 2$, on a

$$O = p^{\alpha+2}\pi(n'p^2 + 1).$$

Quand $p > 3$, $\alpha = p - 2$, on sait que I_0 ne peut avoir qu'un seul groupe K en commun avec d'autres groupes I_r. En désignant par $n_1 p + 1$ le nombre des groupes I_r qui contiennent K, on a

$$O = p^p\pi(n_1 p + 1)(n'p^2 + 1),$$

où $p^p\pi(n_1 p + 1)$ est l'ordre du groupe G_1, formé de celles des substitutions de G qui sont permutables à K. Comme ces substitutions remplacent les éléments d'un même cycle par ceux d'un autre cycle, il existe un groupe G_1' du degré p, isomorphe à G_1, et de l'ordre

$$p\pi_1(n_1 p + 1),$$

π_1 désignant le nombre des valeurs que prend la constante b dans les expressions $| x, y \quad ax, by |$ ou $\left| x, y \quad bx + E\left(\frac{by}{p}\right), by \right|$ des substitutions de H'. En effet, les seules substitutions de G_1 qui ne permutent pas les cycles c_y sont les $| x, y \quad ax + f_1(y), y |$. Parmi les substitutions de G_1, celles qui sont de l'ordre p ou p^2 ont la forme $| x, y \quad x + f_1(y), \phi(y) |$,

et sont par conséquent échangeables à ϑ_0; donc G_1 contient un groupe G_2 dont les substitutions sont échangeables à ϑ_0, et dont l'ordre est $p^n\pi_2(n_1p+1)$, π_2 désignant le nombre des substitutions de G qui sont de la forme $|x, y \quad x, by|$. Par suite G_1' contient un groupe de l'ordre

$$p\pi_2(n_1p+1).$$

Particulièrement, si G est de la seconde espèce, on a $\pi_2 = 1$, d'où $n_1 = 0$; donc

$$O = p^n\pi(n'p^2+1).$$

On verra plus loin qu'on a $n' = 0$ dans tous les cas où $\alpha = p-2$, $p > 3$.

Si $\alpha = p-1$, on a

$$O = p^{p+1}\pi(n_1p+1)(n'p^2+1),$$

et l'on sait, comme dans le cas précédent, que G contient un groupe non primitif G_1 de l'ordre $p^{p+1}\pi(n_1p+1)$. Il existe bien un groupe G_1' du degré p, isomorphe à G_1, mais comme celui-ci peut contenir des substitutions de la forme $|x, y \quad xf(y)+f_1(y), y|$, qui, quoique étrangères à H, ne déplacent pas les cycles c_y, l'ordre de G_1' n'est pas généralement un multiple de $p(n_1p+1)$.

§ 4. *Conséquences tirées de la primitivité ou de la non-primitivité des groupes.*

18. Il résulte des travaux de M. JORDAN (Journal für Mathematik, Bd. **79**, et Bulletin de la Soc. Math., t. **1**) que, pour les plus grandes valeurs de α, le groupe G ne peut être primitif, quand il ne contient pas le groupe alterné. En effet, d'après une formule du premier des Mémoires cités (p. 256), le degré n d'un groupe primitif, ne contenant pas le groupe alterné, mais contenant une substitution de l'ordre p à q cycles, doit vérifier l'inégalité

$$n < q(p+q)\log q + \frac{q(p-q)}{2} + p + 3q,$$

où l'on a supposé $q > 2$; si $q = 2$ on a

$$n \leq 2p+3,$$

et si $q = 1$,

$$n \leqq p + 2.$$

Dans notre cas on a $n = p^2$; comme le groupe contient la substitution ϑ_α, qui est composée de $p - \alpha$ cycles de p lettres, on peut faire $q = p - \alpha$. En supposant $\alpha = p - 1$, on a $q = 1$; donc, ayant $p^2 > p + 2$, le groupe G ne peut être primitif, sans contenir le groupe alterné. En faisant $\alpha = p - 2$, on a $q = 2$; il faudra donc que $p^2 \leqq 2p + 3$, d'où $p = 3$; donc si $\alpha = p - 2$, le groupe ne peut être primitif excepté pour $p = 3$.

Pour les autres valeurs de q, on trouve que le groupe ne peut être primitif, quand on a

$$p > \tfrac{1}{2} q \log q + \tfrac{1}{4} q + \tfrac{1}{2}$$

$$+ \tfrac{1}{2} q \log q \sqrt{1 + \frac{5}{\log q} - \frac{7}{4(\log q)^2} + \frac{2}{q \log q} + \frac{13}{q(\log q)^2} + \frac{1}{(q \log q)^2}}.$$

Quand $q \geqq 7$, le radical est inférieur à 2, de sorte que l'inégalité précédente peut être remplacée par celle-ci:

$$p > \tfrac{3}{2} q \log q + \tfrac{1}{4} q + \tfrac{1}{2}.$$

En calculant, pour chaque valeur de q, la limite de p, on en déduit celle que α ne peut dépasser, quand le groupe est primitif sans contenir le groupe alterné. Voici les résultats pour les premières valeurs de p.

p	$\lim(\alpha)$	p	$\lim(\alpha)$	p	$\lim(\alpha)$
3	1	13	8	29	20
5	2	17	11	31	22
7	4	19	12	37	27
11	7	23	15	41	30.

Dans le Mémoire inséré au Bulletin de la Société Mathématique M. Jordan a donné, pour les valeurs de q inférieures à 6, une limite plus resserrée, savoir

$$n \leqq pq + q + 1,$$

en supposant $p > q$. On en tire, en faisant $n = p^2$,

$$p = q + 1.$$

Il s'ensuit que, lorsque $p = 5$ et $p = 7$, la vraie limite de α est 1. Ainsi, p étant > 3, G ne peut être primitif quand $\alpha = p - 3$.

Quand par les raisons qui viennent d'être exposées, ou par d'autres, on sait que le groupe G est non-primitif, la distribution des éléments en systèmes est une de celles qu'admet le groupe I_0. En particulier, si $\alpha > 0$, les systèmes sont formés par les éléments qui répondent à une même valeur du second indice.

Les groupes non-primitifs méritent une étude spéciale, non seulement parce que, dans certains cas, ils sont les seuls possibles, mais aussi parce qu'un groupe primitif peut en contenir un autre qui ne l'est pas, et que la connaissance de ce dernier peut être utile à l'étude du premier.

19. Supposons que G soit non-primitif, les éléments se groupant en p systèmes, $\Sigma_0, \Sigma_1, \ldots, \Sigma_{p-1}$, où Σ_η contient les éléments pour lesquels le second indice est congru à η. Soit Γ le groupe contenant les substitutions de G qui ne déplacent pas les systèmes, et désignons de plus par γ_η le groupe partiel entre les éléments $u_{0,\eta}, u_{1,\eta}, \ldots, u_{p-1,\eta}$ qu'on obtient par les substitutions de Γ. Tous ces groupes γ_η sont du même ordre, et se déduisent de l'un d'entre eux, en le transformant par les substitutions de G. Nous désignerons l'ordre de γ_η par

$$p\pi_1(mp + 1),$$

π_1 étant le nombre des substitutions de la forme

$$| x \quad x\phi(\eta) |$$

contenues dans γ_η. Soit enfin γ'_η le groupe dérivé de $| x \quad x + 1 |$ et de ses transformées par les substitutions de Γ; γ'_η sera contenu dans γ_η et permutable à ses substitutions; son ordre sera

$$p\pi'_1(mp + 1),$$

π'_1 étant un diviseur de π_1.

Γ contient la substitution ϑ_α, qui ne déplace que les éléments des $p - \alpha$ derniers systèmes; mais il ne contient pas de substitution de l'ordre p, qui en déplace moins. Il est même facile de démontrer, qu'aucune substitution de Γ, quel que soit son ordre, laisse immobiles les éléments

de plus de α systèmes. En effet, supposons que la substitution S ne déplace que les éléments de m systèmes, et faisons

$$S = s_a \cdot s_b \ldots s_f,$$

s_i désignant une substitution entre les éléments du système Σ_i. En transformant S successivement par toutes les substitutions de Γ, on a une série de substitutions:

$$S' = s'_a \cdot s'_b \ldots s'_f,$$
$$S'' = s''_a \cdot s''_b \ldots s''_f,$$
$$\ldots\ldots\ldots\ldots$$

Or le groupe qui dérive des $s_a, s'_a, s''_a, \ldots$, étant permutable aux substitutions du groupe primitif γ_a, est nécessairement transitif; donc il contient une substitution de l'ordre p, et par suite le groupe γ'_a. En multipliant un certain nombre des substitutions $S, S', S'', \ldots$, on peut donc trouver une nouvelle substitution

$$S_1 = \sigma_a \cdot \sigma_b \ldots \sigma_f,$$

où l'ordre de σ_a est égal à p. En élevant S_1 à une puissance convenable, on a une substitution de l'ordre p, ne déplaçant que les éléments de m systèmes au plus, donc

$$m \geqq p - \alpha,$$

ce qui justifie notre assertion.

En faisant $S = \vartheta_a$, le groupe Δ_a dérivant de $S, S', S'', \ldots$ aura évidemment pour ordre $p\pi'_1(mp + 1)$. Si maintenant $\pi'_1 > 1$, ce groupe contient une substitution φ qui transforme ϑ_a en ϑ_a^r, r étant différent de l'unité. Or, en supposant $\alpha > 0$, Γ contient la substitution

$$\vartheta_{a-1} = c_{a-1} \cdot c_a^{(a)_{a-1}} \cdot c_{a+1}^{(a+1)_{a-1}} \ldots c_{p-1}^{(p-1)_{a-1}},$$

et par conséquent celles-ci

$$\varphi^{-1}\vartheta_{a-1}\varphi = c_{a-1} \cdot c_a^{r(a)_{a-1}} \cdot c_{a+1}^{r(a+1)_{a-1}} \ldots c_{p-1}^{r(p-1)_{a-1}},$$

$$\varphi^{-1}\vartheta_{a-1}^{-1}\varphi\vartheta_{a-1}^r = c_{a-1}^{r-1},$$

dont la dernière ne déplace que les éléments de $\Sigma_{\alpha-1}$; donc il faut que $\alpha = p - 1$.

Il est donc démontré que pour $\alpha > 0$, $\alpha < p - 1$, on a nécessairement $\pi_1' = 1$, et par suite, $m = 0$. Dans tous ces cas Γ' ne peut donc contenir d'autres substitutions d'ordre p que les produits des c_i^r, c'est-à-dire les substitutions $\vartheta_0'^{r_0}\vartheta_1'^{r_1}\ldots\vartheta_\alpha'^{r_\alpha}$. Les substitutions de G sont évidemment permutables à Γ', et par suite au groupe $(\vartheta_0, \vartheta_1, \ldots, \vartheta_\alpha)$; or il a été démontré, au numéro 17, que si $\alpha > 0$, $\alpha < p - 2$, les seules substitutions de cette espèce qui puissent être contenues dans G, sont celles de H. Donc, si le groupe G est non-primitif, α étant > 0 et $< p - 2$, il se confond avec H, et par suite on a

$$O = p^{\alpha+2}\pi.$$

La même chose a encore lieu si $p = 3$, $\alpha = p - 2 = 1$, comme on le voit aisément.

Quand $p > 3$, $\alpha = p - 2$, les substitutions de G doivent avoir la forme

$$|\, x, y \quad ax + f(y), \phi(y) \,|;$$

il faut donc que le nombre n' de la formule du numéro 17 soit nul.

Si $\alpha = p - 1$, le groupe Δ_α se confond avec γ'_{p-1}. Le groupe Γ en contient un autre Γ'' de l'ordre $[p\pi_1'(mp + 1)]^p$; or Γ' ne contient évidemment pas d'autres substitutions de l'ordre p que celles de Γ''; par suite l'ordre de Γ sera

$$p^p \pi_1'^p \pi_1''(mp + 1)^p,$$

ou $\pi_1'\pi_1'' = \pi_1$ est le nombre des substitutions de la forme $|\, x, y \quad ax, y \,|$ contenues dans G. Donc enfin on a

$$O = p^{p+1}\pi_1'^p\pi_1''\pi_2(mp + 1)^p(m_1 p + 1),$$

π_2 étant le nombre des valeurs que prend la constante b dans l'expression $|\, x, y \quad ax, by \,|$ des substitutions de H. Chacun des nombres

$$p\pi_1'\pi_1''(mp + 1), \; p\pi_1'(mp + 1), \; p\pi_2(m_1 p + 1)$$

est l'ordre d'un groupe du degré p.

20. Reprenons maintenant les groupes primitifs où $\alpha > 0$, $\alpha < p-3$. Nous désignons par I'_m le groupe intransitif de l'ordre $p^{\alpha+1}$ contenu dans I_m, et par $c_m, c'_m, c''_m, \ldots, c_m^{(p-1)}$ les cycles de la substitution $\vartheta_0^{(m)}$, qui est échangeable à toutes les substitutions de I_m. Ainsi chaque substitution de I'_m est un produit de puissances d'un certain nombre des $c_m^{(i)}$.

Commençons par les groupes de la première espèce, en recherchant si I_0 et I_1 peuvent contenir un même groupe K de l'ordre p^2. Si K était intransitif, il serait contenu dans I'_0 et I'_1. Or nous allons démontrer que, quelle que soit l'espèce de G, les groupes I'_0 et I'_1 ne peuvent avoir de substitution commune.

En effet, une substitution commune à I'_0 et à I'_1 est le produit d'un nombre de cycles au moins égal à $p-\alpha$. Donc parmi les cycles de I'_0 il y a certainement $p-\alpha$ qui se confondent avec $p-\alpha$ cycles de I'_1, et qui seront désignés par

$$c_0^{(\alpha)}, c_0^{(\alpha+1)}, \ldots, c_0^{(p-1)};$$

les lettres de ces cycles forment autant de systèmes communes à I_0 et I_1. D'autre part les systèmes de I_1 ne peuvent pas tous se confondre avec ceux de I_0. En effet, s'il en était ainsi, le groupe qui dérive des substitutions de I_0 et de I_1 serait de l'ordre $p^{\alpha+2}\pi'(mp+1)$, m étant différent de zéro, et il serait non-primitif, ce qui est impossible (n° 19). On peut donc supposer que le cycle c_0 contienne les lettres

$$a_1, a_2, \ldots, a_p,$$

c_1 celles-ci

$$a_1, a_2, \ldots, a_{p-q}, \qquad b_1, b'_1, \ldots, b_1^{(q-1)},$$

où

$$p-q \geqq 2, \qquad q \geqq 1;$$

car évidemment c_1 contient plus d'une lettre de l'un au moins des systèmes de I_0. Le groupe I'_0 contient une substitution S_0 qui déplace les lettres de $p-\alpha$ systèmes choisis arbitrairement; on peut donc supposer que S_0 déplace $a_1, a_2, \ldots, a_p$ et les lettres de $p-\alpha-1$ des cycles $c_0^{(\alpha)}, c_0^{(\alpha+1)}, \ldots, c_0^{(p-1)}$. En désignant généralement par C_m un produit de puissances d'un certain nombre de ces derniers cycles, on a

$$S_0 = c_0 \cdot C_0.$$

De même I_1' contient une substitution

$$S_1 = c_1 \,.\, C_1.$$

Si maintenant $q > 1$, soit c_1^r la puissance de c_1 qui remplace $b_1^{(q-2)}$ par $b_1^{(q-1)}$; la substitution

$$S_1' = S_1^{-r} S_0 S_1^r = c_1^{-r} c_0 c_1^r \,.\, C_0$$

ne déplace pas $b_1^{(q-1)}$, mais elle déplace nécessairement une au moins des lettres $b_1, b_1', \ldots, b_1^{(q-2)}$. Si elle en déplace plus d'une, on déduit de la même manière une nouvelle substitution qui en déplace moins, et ainsi de suite, jusqu'à ce qu'on soit parvenu à une substitution dont le premier cycle contient $p - 1$ des lettres a, par exemple $a_2, a_3, \ldots, a_p$, avec une seule des $b_1^{(i)}$. Par conséquent il est permis de supposer $q = 1$.

Cela posé, soit T une substitution de I_0' qui, en laissant $a_1, a_2, \ldots, a_p$ immobiles, permute b_1 circulairement avec $p-1$ autres lettres $b_2, b_3, \ldots, b_r$. En transformant S_1 successivement par les $p - 1$ puissances de T, on obtient les substitutions

$$S_2 = c_2 \,.\, C_1, \qquad S_3 = c_3 \,.\, C_1, \quad \ldots, \quad S_r = c_p \,.\, C_1,$$

où c_i est une substitution circulaire des lettres $a_2, a_3, \ldots, a_p, b_i$. Le groupe $(S_0, S_1, \ldots, S_p)$ permute les lettres $a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_p$ d'une manière $p + 1$ fois transitive; par conséquent il contient une substitution V qui échange entre eux a_2 et a_3, en laissant $a_1, a_4, \ldots, a_p$ immobiles. Comme nous n'avons fait aucun usage de l'ordre des lettres a, il est permis de supposer

$$S_0 = (a_1, a_2, a_3, a_4, \ldots, a_p) C_0,$$

d'où

$$V^{-1} S_0 V = (a_1, a_3, a_2, a_4, \ldots, a_p) C_0.$$

Donc le groupe G contient la substitution $V^{-1} S_0 V \,.\, S_0^{-1}$, qui se réduit à $(a_1 a_2 a_3)$, donc il est non-primitif, symétrique ou alterné. Cela étant contre l'hypothèse, I_0' et I_1' n'ont pas de substitution commune.

Le groupe K ne peut donc être intransitif. S'il est transitif, il dérive de deux substitutions échangeables entre elles:

$$\vartheta_0, \qquad \vartheta_1^{m_1} \vartheta_2^{m_2} \ldots \vartheta_\alpha^{m_\alpha} t.$$

Le groupe I_1 contient une substitution ϑ_0' échangeable à toutes les autres; comme il n'existe pas de groupe du degré p^2 et de l'ordre p^3, contenant exclusivement des substitutions échangeables entre elles, ϑ_0' est contenu dans K; donc on peut faire

$$\vartheta_0' = \vartheta_0^{m_0}\vartheta_1^{m_1}\vartheta_2^{m_2}\dots\vartheta_\alpha^{m_\alpha}t.$$

Le groupe I_1 est complètement déterminé par les substitutions ϑ_0' et $t' = \vartheta_0$. En le transformant par la substitution

$$\Theta = \vartheta_1^{a_1}\vartheta_2^{a_2}\dots\vartheta_\alpha^{a_\alpha},$$

on a un nouveau groupe, déterminé par les substitutions

$$\Theta^{-1}\vartheta_0'\Theta = \vartheta_0^{m_0+a_1}\vartheta_1^{m_1+a_2}\dots\vartheta_{\alpha-1}^{m_{\alpha-1}+a_\alpha}\vartheta_\alpha^{m_\alpha}t, \qquad \Theta^{-1}t'\Theta = \vartheta_0.$$

Parmi les groupes qu'on obtient de cette manière, ceux qui répondent à une même combinaison de valeurs de $a_2, a_3, \dots, a_\alpha$ ont en commun avec I_0 un même groupe d'ordre p^2. Le nombre de ces derniers groupes est $hp^{\alpha-1}$, et le nombre des groupes $I_1, I_2, \dots$ qui les contiennent est hp^α, h étant le nombre des valeurs que peut avoir m_α. Pour le déterminer, supposons que I_1 soit défini par les substitutions

$$\vartheta_0' = \vartheta_\alpha^{m_\alpha}t = |\,x, y \quad x + m_\alpha(y)_\alpha, y + 1\,|, \qquad t' = |\,x, y \quad x + 1, y\,|,$$

et faisons

$$\xi = x - m_\alpha(y)_{\alpha+1};$$

on trouve

$$\vartheta_r = |\,\xi, y \quad \xi + (y)_r, y\,|, \qquad t = |\,\xi, y \quad \xi - m_\alpha(y)_\alpha, y + 1\,|,$$
$$\vartheta_0' = |\,\xi, y \quad \xi, y + 1\,|, \qquad t' = |\,\xi, y \quad \xi + 1, y\,|.$$

Comme nous supposons $\alpha > 0$, les groupes I_0 et I_1 contiennent respectivement les deux substitutions

$$|\,\xi, y \quad \xi + y, y\,|, \qquad |\,\xi, y \quad \xi, y + \xi\,|,$$

donc G, contenant les deux, contient toutes les substitutions linéaires et

homogènes en ξ et y dont les déterminants sont congrus à 1 (mod p), entre autres la suivante

$$\left|\xi, y \quad r\xi, \frac{1}{r}y\right| \quad \text{ou} \quad \left|x, y \quad rx - m_\alpha\left\{r(y)_{\alpha+1} - \left(\frac{y}{r}\right)_{\alpha+1}\right\}, \frac{1}{r}y\right|.$$

Or, cette substitution, étant permutable à I_0, appartient à H, donc le coefficient de $y^{\alpha+1}$ dans le développement de $m_\alpha\left\{r(y)_{\alpha+1} - \left(\frac{y}{r}\right)_{\alpha+1}\right\}$, à savoir

$$\frac{m_\alpha(r^{\alpha+2} - 1)}{r^{\alpha+1}.\,2\,.\,3\,\ldots\,(\alpha+1)},$$

est divisible par p; comme r peut avoir toute valeur non congrue à zéro, on doit avoir $m_\alpha \equiv 0 \pmod p$, à moins que α ne soit égal à $p-3$.

Comme nous supposons $\alpha < p-3$, nous avons donc $h=0$ ou $h=1$, et dans le dernier cas nous savons que G contient les $p-1$ substitutions $\left|x, y \quad rx, \frac{1}{r}y\right|$ et généralement toute substitution de la forme

$$\begin{vmatrix} x & ax+by+c \\ y & dx+ey+f \end{vmatrix}$$

où $ae - bd \equiv 1 \pmod p$; ces substitutions forment un groupe d'ordre $p^3(p^2-1)$.

On a vu, au commencement du numéro 17, que deux des groupes I ne peuvent contenir un même groupe transitif dont le degré surpasse p^2. En vertu de ce qui a été dit au numéro 6, on peut donc préciser comme il suit l'expression de l'ordre de G:

Quand $\alpha > 0$, $\alpha < p-3$, et G est de la première espèce, son ordre est exprimé par l'une des formules suivantes:

$$O = p^{\alpha+2}\pi(n'p^{\alpha+1}+1),$$

$$O = p^{\alpha+2}\pi(n'p^{\alpha+1}+p^\alpha+1).$$

Dans le cas de la première formule, G ne contient d'autres substitutions linéaires que celles de H; c'est ce qu'on voit de la même manière que pour $\alpha = 1$ (n° 15). Dans la seconde formule le nombre $n'p^{\alpha+1}+p^\alpha+1$ est divisible par $p+1$; en effet, on voit facilement que le nombre des

groupes d'ordre p^2, contenus chacun dans $p+1$ des groupes I_r, est égal à $\frac{(n'p^{\alpha+1}+p^\alpha+1)p^{\alpha-1}}{p+1}$.

Quand G est de la seconde espèce, deux quelconques des groupes I_r ne peuvent avoir d'autre substitution commune que l'identique; car s'ils en avaient, ils contiendraient une même substitution de l'ordre p, laquelle appartiendrait à I_0' et à I_1'; mais on a vu, au commencement de ce numéro, que cela est impossible. Donc si G est de la seconde espèce, α étant >1, et $<p-3$, on a comme pour $\alpha=1$,

$$O = p^{\alpha+2}\pi(n'p^{\alpha+2}+1).$$

§ 5.

21. Recherchons de quelle manière un groupe primitif du degré p^2 peut être composé. Nous désignerons par H le groupe que nous avons plus haut appelé H', en gardant du reste les notations précédentes. Le groupe primitif dont il est question dérive des substitutions des groupes $I_0, I_1, \ldots, I_{np}$ et H, ce que nous exprimerons en écrivant

$$G = (I_0, I_1, \ldots, I_{np}, H);$$

son ordre est

$$O = p^{\alpha+2}\pi(np+1).$$

Supposons que G contienne un groupe G', permutable à ses substitutions et, par suite, transitif. Dénotons les groupes contenus dans G', ainsi que leurs ordres, en accentuant les lettres relatives aux groupes correspondants contenus dans G; on a

$$G' = (I_0', I_1', \ldots, I_{n'p}', H'),$$

$$O' = p^{\alpha'+2}\pi'(n'p+1).$$

On sait que chacun des groupes I_r' est contenu dans un des I_r; nous allons démontrer que I_r' est permutable aux substitutions de chaque groupe I_r qui le contient. En transformant les I_r' successivement par toutes les substitutions de I_0, on obtient un groupe entre les I_r', dont l'ordre est une puissance de p; comme leur nombre est $n'p+1$, l'un

au moins d'entre eux, par exemple I'_0, est invariable par ces transformations. Par conséquent I'_0 est contenu dans I_0, car autrement le groupe (I_0, I'_0) serait de l'ordre $p^{\alpha+2+m}$, ce qui est absurde. De plus on a $\alpha = \alpha'$ ou $\alpha = \alpha' + 1$; en effet, si $\alpha > \alpha' + 1$, on aurait

$$I'_0 = (\vartheta_0, \vartheta_1, \ldots, \vartheta_{\alpha'}, \vartheta^a_{\alpha'+1}\vartheta^b_{\alpha'+2}\ldots\vartheta^f_{\alpha-1}\vartheta^g_\alpha t);$$

en transformant ce groupe par ϑ_α, on aurait le suivant

$$(\vartheta_0, \vartheta_1, \ldots, \vartheta_{\alpha'}, \vartheta^a_{\alpha'+1}\vartheta^b_{\alpha'+2}\ldots\vartheta^{f+1}_{\alpha-1}\vartheta^g_\alpha t),$$

qui diffère de I'_0, ce qui est impossible. Il faut donc que $\alpha = \alpha'$ ou $\alpha = \alpha' + 1$, et dans les deux cas I'_0 est évidemment permutable aux substitutions de chacun des groupes I_r qui le contient.

Premier cas, $\alpha = \alpha'$. Comme I'_r est identique au groupe I_r qui le contient, on a évidemment $n' = n$,

$$O' = p^{\alpha+2}\pi'(np + 1).$$

Le groupe H' est contenu dans H et permutable à ses substitutions, car le groupe transformé de H' par une substitution de H est contenu dans H et G', et par conséquent il ne peut être que H'.

Inversement, si G', ayant pour ordre $p^{\alpha+2}\pi'(np + 1)$, est contenu dans G, et si, en outre, H' est permutable aux substitutions de H, G' est permutable à celles de G; c'est ce qu'on voit presque immédiatement en remarquant qu'on a $G = (G', H)$. Si l'on excepte les groupes de la première espèce où $\alpha = 0$, la condition relative au groupe H' peut être omise, puisque les substitutions de H sont échangeables entre elles. D'ailleurs, si G' n'est pas nécessairement permutable aux substitutions de G, le groupe $(I'_0, I'_1, \ldots, I'_{np})$, contenu dans G', l'est toujours.

Les facteurs de composition de G sont donc: 1°, les facteurs de composition du groupe $\frac{G}{G'}$, 2°, ceux de G' (voir, pour la notation, le Mémoire de M. JORDAN: *Sur la limite de transitivité*, § 2, Bulletin de la Société Mathématique, t. 1). Si l'on excepte le cas où, α étant égal à zéro, H est icosaédrique, les facteurs qui naissent du groupe $\frac{G}{G'}$ sont des nombres premiers. Quand H est icosaédrique, H' peut l'être aussi, et dans ce cas les facteurs de composition qui précèdent ceux de G'

sont encore des nombres premiers; si non, H' ne contient que des substitutions de la forme $|x, y \quad ax, ay|$.

Second cas, $\alpha = \alpha' + 1$. Chacun des groupes I_r ne peut contenir qu'un seul des groupes I'_r. En effet si I'_0 et I'_1 étaient contenus dans I_0, on aurait

$$I'_0 = (\vartheta_0, \vartheta_1, \ldots, \vartheta_{\alpha-1}, \vartheta_\alpha^m t),$$

$$I'_1 = (\vartheta_0, \vartheta_1, \ldots, \vartheta_{\alpha-1}, \vartheta_\alpha^{m'} t);$$

donc G' contiendrait $\vartheta_\alpha^m t$ et $\vartheta_\alpha^{m'} t$, et par suite $\vartheta_\alpha^{m-m'}$, ce qui est contre l'hypothèse. Or, on a vu que deux des groupes I_r ne peuvent contenir un même groupe transitif de l'ordre $p^{\alpha+1}$ que dans le seul cas où $\alpha = 1$, G est de la première espèce et où l'on a

$$O = p^3\pi(p + 1)(n_1 p^2 + 1).$$

Donc, si l'on fait abstraction de ce cas, il faut que $n = n'$,

$$O' = p^{\alpha+1}\pi'(np + 1).$$

Comme G' est permutable aux substitutions de I_0, le groupe G en contient un autre G'' de l'ordre $p^{\alpha+2}\pi'(np + 1)$; d'après ce qui précède G'' est permutable aux substitutions de G, et évidemment G' est permutable à celles de G''; donc les facteurs de composition de G sont: 1°, les diviseurs premiers de $\frac{\pi}{\pi'}$, 2°, le nombre p, 3°, les facteurs de composition de G'.

Si le groupe G' est lui-même composé, la série des décompositions est arrêtée, au plus tard, quand on est parvenu à un groupe de l'ordre $p^2\pi_r(np + 1)$, où π_r est un nombre premier. En effet on ne rencontrera pas le cas qui a été excepté, comme le font voir les expressions de O trouvées au numéro précédent. Donc, à part l'exception signalée, le nombre n a la propriété de se conserver dans le cours des décompositions. Un groupe dont l'ordre est exprimé par la formule

$$O = p^{\alpha+2}\pi(n'p^{\alpha+1} + p^\alpha + 1),$$

α étant supérieur à 1, n'entre jamais dans ce cas. On aurait en effet $O' = p^{\alpha+1}\pi'(n'p^{\alpha+1} + p^\alpha + 1)$, et par conséquent G' ne contiendrait d'autres

substitutions linéaires que celles de H'; mais d'autre côté il contiendrait nécessairement la substitution $|x, y \quad x, y + x|$ (n° 20), ce qui est une contradiction.

Considérons enfin le cas d'exception. On a

$$O = p^3\pi(p + 1)(n_1p^2 + 1), \qquad O' = p^2\pi'(n'p + 1).$$

Désignons par Γ le groupe d'ordre $p^3\pi(p + 1)$ formé des substitutions linéaires de G, et soient $I_0, I_1, \ldots, I_p$ les groupes d'ordre p^3 contenus dans Γ. On a vu que l'un des groupes $I'_0, I'_1, \ldots, I'_{n'p}$ est contenu dans I_0, et que, par suite, il a la forme $(\vartheta_0, \vartheta_1^m t)$; donc G' contient la substitution ϑ_0. Dans un autre des groupes I_r les substitutions échangeables à toutes les autres sont les t^m; on peut donc conclure que G' contient t. Donc parmi les groupes I'_r se trouve le suivant: $(\vartheta_0, t) = I'_0$, qui est contenu dans les $p + 1$ groupes $I_0, I_1, \ldots, I_p$. D'autre part I'_0, étant permutable aux substitutions de tout groupe I_r qui le contient, ne peut être contenu dans aucun des groupes $I_{p+1} \ldots I_{np}$. Il s'ensuit que chacun des I'_r est contenu dans $p + 1$ des I_r. Donc on a

$$O' = p^2\pi'(n_1p^2 + 1).$$

Quand $p = 3$, il n'existe d'autres groupes du genre que nous considérons, que ceux où $n_1 = 0$, c'est-à-dire ceux qui sont contenus dans le groupe linéaire. Pour les autres valeurs de p, le groupe Δ qui renferme les substitutions linéaires et homogènes dont le déterminant est congru à $1 \pmod p$, et qui est contenu dans G, a pour facteurs de composition $\frac{p(p^2-1)}{2}$ et 2. Les substitutions de Δ sont permutables à I'_0 et par suite à H'. On en peut conclure que H' ne contient que des substitutions de la forme $|x, y \quad ax, ay|$. En effet toute substitution de H' peut être écrite sous la forme ST, où S appartient à Δ, et où T a la forme $|x, y \quad ax, y|$. Or comme Δ contient la substitution

$$\varphi = \left|x, y \quad rx, \frac{1}{r}y\right|,$$

H' contiendra $\varphi^{-1}S\varphi T$ et par suite $\varphi^{-1}S\varphi \cdot S^{-1}$; cette substitution, faisant partie d'un groupe contenu dans Δ et permutable à ses substitutions, ne peut être que 1 ou $|x, y \quad -x, -y|$. Mais la dernière alternative

ne peut avoir lieu pour toutes les valeurs de r, comme on le voit aisément; pour les autres il faut donc que $\varphi^{-1}S\varphi = S$; mais alors S est canonique en x et y, donc

$$S = \left| x, y \quad ax, \frac{1}{a}y \right|.$$

Par conséquent les substitutions de H' sont de la forme

$$U = | x, y \quad ax, by |;$$

mais, puisque Δ contient la substitution ϑ_1, H' contient la suivante

$$\vartheta_1^{-1} U \vartheta_1 . U^{-1} = \left| x, y \quad x + \frac{b-a}{a}y, y \right|,$$

ce qui exige que $b \equiv a \pmod{p}$.

Les premiers groupes composants de G sont ceux de $\frac{G}{G'}$; or ce groupe est isomorphe au groupe contenant les substitutions linéaires et homogènes de G. Donc, si l'on suppose que H contienne des substitutions dont le déterminant est non résidu quadratique de p, et qu'on désigne par $\pi'\pi''$ le nombre des substitutions de H qui ont la forme $|x, y \quad ax, ay|$ les facteurs de composition de G seront: $2, \frac{p(p^2-1)}{2}$, les facteurs premiers de π'', les facteurs de composition de G', et l'on aura

$$\pi = 2\pi'\pi''(p-1).$$

Si au contraire H ne contient que des substitutions dont les déterminants sont résidus, le premier facteur (2) doit être omis, et l'on aura $\pi = \pi'\pi''(p-1)$. Le nombre n n'a pas ici la propriété d'être conservé en passant du groupe G au groupe G'; mais cette propriété appartient toujours au nombre N, défini par l'équation

$$O = p^m P(Np + 1),$$

P désignant l'ordre du groupe formé de celles des substitutions de G qui sont linéaires en x et y ou en $\xi \pmod{p^2}$, suivant l'espèce du groupe.

22. Voici une autre conséquence de ce qui précède, qui sans avoir beaucoup d'importance, présentera peut-être quelque intérêt, vu qu'on ne

connaît qu'un très petit nombre de cas où l'on peut reconnaître la résolubilité d'un groupe de son ordre seul:

Tout groupe dont l'ordre est p^2q ou p^2q^2, p et q étant des nombres premiers inégaux, est résoluble.

Soit G un groupe de l'ordre p^2q; il en contient un autre H, de l'ordre q. Désignons par y_0 une fonction rationnelle des éléments, invariable par les substitutions de H, mais variable par toute autre substitution; cette fonction prend, par les substitutions de G, un nombre p^2 de valeurs différentes, $y_0, y_1, \ldots, y_{p^2-1}$. En opérant dans ces fonctions les substitutions de G, on a un groupe G' entre les y, lequel est transitif et isomorphe à G. L'ordre de G' est p^2 ou p^2q. Dans le premier cas H est permutable aux substitutions de G; comme les facteurs de composition de G' sont p, p, ceux de G sont p, p, q. Si l'ordre de G' est p^2q, ce groupe en contient un autre I' de l'ordre p^2; en désignant par $p^2\pi$ l'ordre du groupe qui contient les substitutions de G' permutables à I', on a une équation de la forme

$$p^2q = p^2\pi(np + 1).$$

Or, on ne peut avoir $\pi = 1$, puisque alors n serait nul, donc il faut que $\pi = q, n = 0$; c'est-à-dire que les substitutions de G' sont toutes permutables à I'; par conséquent les facteurs de composition de G' qui sont en même temps ceux de G, sont q, p, p. Dans les deux cas G est donc résoluble.

Si l'ordre de G est p^2q^2, on obtient comme plus haut un groupe G' du degré p^2 isomorphe à G; son ordre est p^2, p^2q ou p^2q^2. Dans les deux premiers cas G' est résoluble, et par suite aussi G. Dans le troisième on a, comme ci-dessus, une équation de la forme

$$p^2q^2 = p^2\pi(np + 1),$$

et l'on peut supposer $q > p$. Or on ne peut avoir $\pi = 1$, donc il faudrait que q divisât π; mais π est un diviseur de $(p-1)^2(p+1)$, nombre dont aucun diviseur premier ne surpasse p, à moins que p ne soit égal à 2. Mais cette supposition est inadmissible, puisque l'ordre d'un groupe du quatrième degré est un diviseur de 24. Ainsi le troisième cas peut être évité. Le théorème est donc démontré.

22. La détermination du groupe que nous avons désigné par H permet de resserrer un peu, dans quelques cas spéciaux, la limite de transitivité des groupes, assignée par M. JORDAN dans son Mémoire sur ce sujet, inséré au Bulletin de la Société Mathématique, t. **1**. En effet, si dans le théorème III du Mémoire cité, on fait $m = 2$, $n = 0$, on démontre, en suivant le raisonnement de M. JORDAN, que si un groupe du degré $p^2q + k$, où $q < p$, $q < k$, est plus de k fois transitif sans contenir le groupe alterné, k ne pourra surpasser 5, si le nombre premier p est de l'une des formes $10h \pm 1$; il ne pourra surpasser 4, si p est égal à 5 ou qu'il soit de l'une des formes $10h \pm 3$. Les mêmes règles sont encore valables, quand le degré est $pq + k$, où $q < k$, $q < p^2$. Si l'on fait $q = 1$, et qu'on suppose en même temps que l'ordre du groupe partiel qui laisse $k + 1$ éléments immobiles, soit divisible par p, k ne peut même dépasser 2. C'est là une proposition analogue à l'élégant théorème I du Mémoire de M. JORDAN, et elle se démontre de la même manière.