Théorèmes sur les groupes de substitutions.

Par M. L. Sylow à Frederikshald en Norvege.

On sait que si l'ordre d'un groupe de substitutions est divisible par le nombre premier n, le groupe contient toujours une substitution d'ordre n. Ce théorème important est contenu dans un autre plus général que voici: „Si l'ordre d'un groupe est divisible par n^α, n étant premier, le groupe contient un faisceau partiel d'ordre n^α“. La démonstration même du théorème fournit quelques autres propriétés générales des groupes de substitutions. J'y ajouterai encore quelques propositions moins générales qui s'y ratachent ou qui en écoulent, dont quelques unes pourtant sont déjà connues par un travail de M. E. Mathieu.

Les notations et les termes employés sont ceux de M. C. Jordan.

1. Si G est un groupe de substitutions dont l'ordre N est divisible par le nombre premier n, on sait que G contient une substitution d'ordre n, mais nous pouvons supposer plus généralement qu'il contienne un groupe g d'ordre n^α, dont par conséquent chaque substitution est d'un ordre diviseur de n^α. Nous désignerons les substitutions de g par

$$1\ \theta_1\ \theta_2 \ldots .$$

tandis que les substitutions de G en général seront désignées par

$$1\ \psi_1\ \psi_2 \ldots .$$

Enfin nous supposerons que G ne contient aucun groupe partiel dont l'ordre est une puissance de n supérieure à n^α. Or G contient toujours des substitutions permutables à g, savoir les substitutions de ce dernier elles-mêmes, mais il est possible qu'il en contient un nombre plus grand; en tous cas ces substitutions forment un groupe γ, qui contient g, et dont l'ordre sera désigné par $n^\alpha \nu$; ce nombre est à son tour un diviseur de N; nous pouvons donc faire:

$$N = n^\alpha \nu h .$$

Les substitutions du groupe γ seront désignées par

$$1\ \varphi_1\ \varphi_2 \ldots .$$

Les θ sont donc comprises parmi les φ, ainsi que celles-ci parmi les ψ.

Cela posé, nous allons d'abord démontrer que le nombre ν doit être premier à n. Soient $x_0\, x_1\, x_2 \ldots$ les lettres que le groupe G permute entre elles, et soit y_0 une fonction rationnelle des x, invariable par les substitutions de g mais variable par toute autre substitution. Cette fonction prend par les substitutions de γ les ν valeurs différentes

$$y_0\, y_1\, y_2 \ldots y_{\nu-1}.$$

Chacune de ces fonctions est invariable par les substitutions de g mais variable par toute autre substitution. En effet, si y_1 se déduit de y_0 par la substitution φ_1, y_1 est invariable par le groupe transformé de g par φ_1, mais variable par toute autre substitution; mais φ_1 étant permutable à g, le groupe transformé se confond avec g. Or si l'on opère dans les y les substitutions de γ, on aura entre ces quantités un groupe γ' nécessairement transitif et isomorphe à γ. Pour en avoir l'ordre il faut diviser celui de γ par le nombre des substitutions φ qui n'altèrent aucune des y, c'est-à-dire par n^α. L'ordre de γ' est donc ν. Si maintenant ν était divisible par n, γ' devrait contenir une substitution d'ordre n; une substitution correspondante φ_1 de γ devrait remplir la condition

$$\varphi_1{}^n = \theta_a.$$

Mais puisque φ_1 est permutable à g, on voit que dans ce cas les substitutions $\theta_q \varphi_1{}^p$ formeraient un groupe d'ordre $n^{\alpha+1}$ contenu dans G. Cela étant contraire à l'hypothèse, on conclut que ν est premier à n.

Notons ici que les θ sont les seules substitutions de γ dont les ordres sont des puissances de n. En effet, si φ_1 est une substitution de γ étrangère à g, les substitutions $\theta_q \varphi_1{}^p$ forment un groupe dont l'ordre est égal à $n^\alpha m$, m désignant l'exposant de la puissance la moins élevée de φ_1 qui appartient à g. Or on voit sans peine que les seules puissances de φ_1 qui appartiennent à g sont celles dont les exposants sont des multiples de m, d'où il suit immédiatement que m est un diviseur de l'ordre de φ_1. Si donc l'ordre de φ_1 était une puissance de n, on aurait $m = n^\beta$, ce qui est impossible, le groupe des $\theta_q \varphi_1{}^p$ ne pouvant être d'ordre $n^{\alpha+\beta}$.

Le nombre h n'est pas non plus divisible par n. Pour le faire voir imaginons une fonction rationnelle des x invariable par les substitutions de γ, mais variable par toute autre substitution. Soit z_0 cette fonction, et représentons par

$$z_0\, z_1\, z_2 \ldots z_{h-1}$$

les h valeurs qu'elle prend par les substitutions de G. Effectuons dans les z les substitutions de g; par cela z_0 ne varie pas, mais chacune des autres z prend un nombre de valeurs qui est un diviseur de l'ordre de g, c'est-à-dire une puissance de n. Cette puissance ne peut se réduire à l'unité; si par exemple z_1 était invariable par g

et que z_1 se déduise de z_0 par la substitution ψ_1, z_0 devrait être invariable par le groupe transformé de g par ψ_1^{-1}; or, le seul groupe d'ordre n^α contenu dans γ étant g, ψ_1^{-1} devrait être permutable à g, ce qui n'a pas lieu. Si donc on partage les fonctions $z_1 \ldots z_{h-1}$ en systèmes, en réunissant ensemble celles qui se permutent entre elles par les substitutions de g, le nombre de fonctions contenues dans chaque système sera une puissance de n. Par conséquent le nombre h est de la forme $np+1$. L'ordre de g égale donc la plus grande puissance de n qui divise l'ordre de G. Les résultats obtenus se résument ainsi:

Théorème I. Si n^α désigne la plus grande puissance du nombre premier n qui divise l'ordre du groupe G, ce groupe contient un autre g de l'ordre n^α; si de plus $n^\alpha\nu$ désigne l'ordre du plus grand groupe contenu dans G dont les substitutions sont permutables à g, l'ordre de G sera de la forme $n^\alpha\nu\,(np+1)$.

2. Évidemment g n'est pas le seul groupe d'ordre n^α contenu dans G, excepté seulement le cas $p=0$. Mais on pourrait demander si G en contient d'autres que g et ses transformés par les substitutions de G. Voilà ce que nous allons rechercher. Soit g' un groupe d'ordre n^α contenu dans G mais différent de g, et soient

$$1\ \theta_1'\ \theta_2' \ldots .$$

ses substitutions. Effectuons ces substitutions dans les fonctions z, et réunissons en systèmes celles qui par cela s'échangent entre elles. Comme nous l'avons déjà dit, le nombre des fonctions contenues dans chaque système doit être un diviseur de n^α; on doit donc avoir une égalité de la forme

$$np+1 = n^a + n^b + n^c + \cdots$$

n^a, n^b, n^c ... désignant le nombre des fonctions contenues dans les divers systèmes. Mais cela exige qu'au moins un des exposants $a\ b\ c \ldots$ soit nul; en d'autres termes, il faut qu'au moins une des fonctions z soit invariable par toutes les substitutions de g'. Soit z_k cette fonction, et supposons qu'elle se déduise de z_0 par la substitution ψ_k. On z_k n'est invariable que par les substitutions $\psi_k^{-1}\varphi_a\psi_k$; de plus $\psi_k^{-1}\varphi_a\psi_k$ est semblable à φ_a, et parmi les φ_a il n'y a que les θ dont les ordres sont des puissances de n. Il faut donc qu'on ait

$$\theta_b' = \psi_k^{-1}\theta_a\psi_k$$

pour toutes les valeurs de b. Le groupe g' est donc le transformé de g par ψ_k.

Si d'ailleurs on remplace ψ_k par $\varphi_r\psi_k$, on a évidemment le même groupe transformé. De l'autre côté ψ_k ne peut être remplacée que par $\varphi_r\psi_k$. En effet, si l'on a

$$\psi_l^{-1}\theta_a\psi_l = \psi_k^{-1}\theta_b\psi_k$$

pour toute valeur de a, il s'ensuit

$$\psi_k \psi_l^{-1} \theta_a \psi_l \psi_k^{-1} = \theta_b$$

d'où l'on conclut

$$\psi_l \psi_k^{-1} = \varphi_r$$

ou

$$\psi_l = \varphi_r \psi_k .$$

On peut donc énoncer ce théorème:

Théorème II. Tout étant posé comme au théorème précédent, le groupe G contient précisément $np + 1$ *groupes distincts d'ordre* n^α*; on les obtient tous en transformant l'un quelconque d'entre eux par les substitutions de G, tout groupe étant donné par* $n^\alpha \nu$ *transformantes distinctes.*

Par un raisonnement analogue on voit que tout groupe contenu dans G d'ordre n^β, β étant moindre que α, est le transformé d'un groupe contenu dans g par une substitution de G, et qu'il y a *au moins* $n^\alpha \nu$ manières de l'obtenir par transformation. Il est en effet possible qu'il y en ait plus, puisque de la relation

$$\psi_k \psi_l^{-1} \theta_a \psi_l \psi_k^{-1} = \theta_b$$

on ne peut conclure

$$\psi_l \psi_k^{-1} = \varphi_r$$

à moins qu'elle n'ait lieu pour toute valeur de a.

3. Nous allons maintenant nous occuper du groupe g. Formons les transformées des substitutions $1 \theta_1 \theta_2 \ldots$ par une d'elles; comme par cela on ne fait que les reproduire dans un autre ordre, on a une substitution entre les substitutions θ elles mêmes. Si on les transforme successivement par toutes les substitutions de g, on a un groupe de substitutions; cela résulte en effet immédiatement de l'identité:

$$\theta_b^{-1} \theta_a^{-1} \theta_r \theta_a \theta_b = (\theta_a \theta_b)^{-1} \theta_r (\theta_a \theta_b) .$$

Le groupe entre les θ qu'on obtient de cette manière est nécessairement intransitif, la substitution identique au moins étant invariable par les transformations; mais il y a aussi d'autres substitutions invariables, comme nous allons voir. En effet on peut réunir en systèmes celles des substitutions qui s'échangent entre elles par les transformations; cela fait, les transformations produiront un groupe transitif entre les substitutions de chaque système. Or le nombre de substitutions θ contenues dans un système est un diviseur de l'ordre du groupe correspondant; mais on voit par un raisonnement familier que l'ordre de ce groupe est égal à n^α divisé par le nombre des transformations qui ne font varier aucune des substitutions du système considéré. Ainsi donc le nombre de substitutions contenues dans chaque système est une puissance de n. La substitution identique étant invariable, on doit avoir une égalité de la forme

$$n^\alpha = 1 + n^a + n^b + \cdots$$

où $1 n^a n^b \ldots$ sont les nombres des substitutions des divers systèmes. Cela exige qu'au moins $n-1$ des exposants $ab\ldots$ soient nuls. Il y a donc dans le groupe g au moins n substitutions, y comprise la substitution identique, qui sont invariables; en d'autres termes il y a dans g au moins n substitutions échangeables à toutes les substitutions du groupe.

Or puisque, deux substitutions étant échangeables, leurs puissances le sont également, il y aura toujours parmi les substitutions échangeables à toutes les autres une substitution d'ordre n. Soit θ_0 cette substitution, et soit y_0 une fonction rationnelle des x, invariable par θ_0^i mais variable par toute autre substitution, et représentons par

$$y_0\ y_1\ y_2\ \ldots\ldots$$

les $n^{\alpha-1}$ valeurs qu'elle prend par les substitutions de g. En effectuant dans les y les substitutions de g on aura entre ces fonctions un groupe isomorphe à g, dont l'ordre est évidemment $n^{\alpha-1}$. En vertu de ce qui vient d'être démontré ce groupe doit contenir une substitution d'ordre n échangeable à toutes les substitutions du groupe. Soit maintenant θ_1 une substitution correspondante de g. Effectuée n fois de suite θ_1 doit ramener toutes les y à leurs places primitives, donc

$$\theta_1^n = \theta_0^a.$$

De plus, si ϑ désigne une substitution quelconque de g, θ_1 doit produire entre les y la même substitution que sa transformée par ϑ, c'est-à-dire, on a

$$\vartheta^{-1}\theta_1\vartheta = \theta_0^b\theta_1.$$

Les substitutions $\theta_0^i\theta_1^k$ constituent évidemment un groupe d'ordre n^2. Si maintenant on forme une fonction rationnelle des x invariable par les $\theta_0^i\theta_1^k$, mais variable par toute autre substitution, et qu'on raisonne sur cette fonction, comme nous avons raisonné sur y_0, on voit que g doit contenir une substitution θ_2 qui remplit les conditions

$$\theta_2^n = \theta_0^c\theta_1^d$$
$$\vartheta^{-1}\theta_2\vartheta = \theta_0^e\theta_1^f\theta_2.$$

En continuant ainsi on démontre le théorème suivant:

Théorème III. Si l'ordre d'un groupe est n^α, n étant premier, une substitution quelconque ϑ du groupe peut être exprimée par la formule

$$\vartheta = \theta_0^i\theta_1^k\theta_2^l\ldots\theta_{\alpha-1}^r$$

où

$$\theta_0^n = 1$$
$$\theta_1^n = \theta_0^a$$
$$\theta_2^n = \theta_0^b\theta_1^c$$
$$\theta_3^n = \theta_0^d\theta_1^e\theta_2^f$$
$$\cdots\cdots\cdots$$

et où l'on a

$$\vartheta^{-1}\theta_0\vartheta = \theta_0$$
$$\vartheta^{-1}\theta_1\vartheta = \theta_0^{\beta}\theta_1$$
$$\vartheta^{-1}\theta_2\vartheta = \theta_0^{\gamma}\theta_1^{\delta}\theta_2$$
$$\vartheta^{-1}\theta_3\vartheta = \theta_0^{\varepsilon}\theta_1^{\zeta}\theta_2^{\eta}\theta_3$$
$$\cdots\cdots\cdots\cdots$$

On voit que les facteurs de composition du groupe sont tous égaux à n, nous pouvons donc énoncer comme corollaire la proposition suivante:

Si l'ordre d'une équation algébrique est une puissance d'un nombre premier, l'équation est résoluble par radicaux.

Supposons que le groupe g soit transitif et que le nombre des lettres soit égal à n^{β}. Dans ce cas la substitution que nous avons nommée θ_0 est régulière, c'est-à-dire qu'elle déplace toutes les lettres, et que toutes ces cycles en contiennent un même nombre; car autrement elle ne serait pas évidemment échangeable à toutes les substitutions du groupe. De plus le groupe sera imprimitif; en effet les substitutions remplaceront les lettres contenues dans un même cycle de θ_0 par des lettres d'un même cycle. Donc l'équation le partagera par la résolution d'une équation de degré $n^{\beta-1}$ en $n^{\beta-1}$ équations de degré n. Évidemment les groupes de ces dernières équations, ainsi que celui de l'équation auxiliaire, ne contiendront que des substitutions dont les ordres sont des puissances de n; les équations de degré n seront par suite abéliennes. Donc:

Théorème IV. Si le degré d'une équation irréductible est n^{β}, n étant premier, et que l'ordre de son groupe soit également une puissance de n, l'une quelconque de ses racines se déterminera par une suite de β équations abéliennes de degré n.

Pour le cas $n = 2$ cette dernière proposition a été démontrée par M. J. Petersen (Om de Ligninger, der kunne löses ved Kvadratrod etc. Kjöbenhavn 1871).

Ces résultats peuvent même être généralisés. En effet, si l'ordre du groupe d'une équation est égal à $n^{\alpha}m$, m étant moindre que n, on a, en employant le théorème I, $p = 0$, $m = \nu$. Par suite toutes les substitutions du groupe sont permutables au groupe partiel que nous avons désigné par g. Le groupe se réduit donc à g, si l'on adjoint les fonctions que nous avons désignées par $y_0 y_1 \ldots$, et qui sont les racines d'une équation dont l'ordre et le degré sont égaux à m. Si donc l'équation auxiliaire est résoluble par radicaux, l'équation donnée l'est également. De là s'ensuit comme conséquence immédiate:

Théorème V. Si l'ordre d'une équation algébrique est

$$n^{\alpha}n_1^{\alpha_1}n_2^{\alpha_2}n_3^{\alpha_3}\ldots,$$

n n_1 n_2 n_3 .... étant premiers, si de plus on a

$$n > n_1^{\alpha_1} n_2^{\alpha_2} n_3^{\alpha_3} \ldots .$$
$$n_1 > n_2^{\alpha_2} n_3^{\alpha_3} \ldots .$$
$$n_2 > n_3^{\alpha_3} \ldots .$$

l'équation est résoluble par radicaux.

4. De ce qui précède on tire aussi une démonstration simple du théorème de M. E. Mathieu: *Tout groupe transitif entre n^α lettres, n désignant un nombre premier, contient une substitution régulière d'ordre n.* (Voir le journal de M. Liouville 1861.)

Soit G un groupe transitif de degré $n^\alpha m$, et soit N son ordre. Or N est divisible par $n^\alpha m$; faisons donc

$$N = n^{\alpha+\beta} m N',$$

N' étant supposé premier à n; soit de plus G' le groupe d'ordre $n^\beta N'$ qui contient les substitutions de G qui ne déplacent pas x_0. Maintenant G contient un groupe g d'ordre $n^{\alpha+\beta}$, et les substitutions de ce dernier qui ne déplacent pas x_0 forment un groupe g', dont nous désignerons l'ordre par n^γ. Or g' est évidemment contenu dans G', donc on a

$$\gamma \leqq \beta .$$

Mais si l'on désigne par r le nombre des places qui sont successivement occupées par x_0, quand on effectue toutes les substitutions de g, on a, comme on sait,

$$r n^\gamma = n^{\alpha+\beta}$$

donc
$$r \geqq n^\alpha .$$

Le nombre r est nécessairement une puissance de n; d'ailleurs ce qui vient d'être démontré pour x_0 a aussi lieu pour chacune des x. Donc chaque lettre prend par le groupe g un nombre de places qui est une puissance de n égale ou supérieure à n^α.

Si maintenant on suppose $m = 1$, on voit que g doit être transitif. Cela étant, g doit contenir une substitution régulière comme nous l'avons déjà dit. Le théorème est donc démontré.

Il y a un autre cas où l'on peut également démontrer l'existence de substitutions régulières. Supposons en effet $\alpha = 1$ avec $m < n$. Puisque $n^2 > mn$, on conclut que chaque lettre prend par les substitutions de g précisément n places différentes. Si donc m réunit dans un même système les lettres qui s'échangent entre elles, on aura m systèmes de n lettres chacun. Soit maintenant c un cycle d'une substitution de g, c représentera une substitution circulaire des n lettres d'un même système. Or si une autre substitution de g fait subir aux mêmes lettres un déplacement, ce déplacement ne sera autre chose qu'une puissance de c, car dans le cas contraire on pourrait des deux substitutions dériver une troisième qui ne soit pas d'ordre n. Soit donc θ une substitution de g, on a

$$\theta = c_1 c_2 \ldots . c_r$$

c_k désignant une substitution circulaire entre les lettres du $k^{\text{ième}}$ système. Si maintenant $r < m$, le groupe g doit contenir une substitution θ_1 qui permute les lettres du $(r+1)^{\text{ième}}$ système, et d'après ce qui vient d'être dit on a

$$\theta_1 = c_1^{\delta} c_2^{\varepsilon} \ldots c_r^{\zeta} c_{r+1} c_{r+2} \ldots . c_s ,$$

les nombres $\delta\ \varepsilon \ldots \zeta$ pouvant être nuls. On en tire

$$\theta^p \theta_1 = c_1^{p+\delta} c_2^{p+\varepsilon} \ldots c_r^{p+\zeta} c_{r+1} c_{r+2} \ldots c_s .$$

Or, puisque le nombre des systèmes est inférieur à n, on peut déterminer p de sorte qu'aucun des nombres $p+\delta$, $p+\varepsilon, \ldots p+\zeta$ ne soit égal à zéro. On obtient ainsi une substitution ayant $r+s$ cycles. Si $r+s < m$, on déterminera de la même manière une substitution de g qui a plus de $r+s$ cycles; en continuant ainsi on finira par trouver une substitution régulière.

Théorème VI. Une groupe transitif entre n m lettres, n étant premier, et $m < n$, contient une substitution régulière d'ordre n.

En vertu de ces deux théorèmes tout groupe transitif entre un nombre de lettres moindre de 12 contient des substitutions régulières. Mais déjà pour le degré 12 il existe des groupes transitifs qui en sont dépourvus. Ainsi les substitutions du groupe dérivé de

$$\theta_0 = (x_0 x_1 x_2)\ (x_3 x_4 x_5)\ (x_6 x_7 x_8)$$
$$\theta_1 = (x_3 x_4 x_5)\ (x_6 x_8 x_7)\ (x_9 x_{10} x_{11})$$
$$\varphi = (x_0 x_3 x_6 x_9 x_1 x_4 x_8 x_{11})\ (x_2 x_5 x_7 x_{10})$$

sont semblables les unes à θ_0, les autres aux puissances de φ. Un autre exemple est le groupe dérivé de $\theta_0\ \theta_1$ et des substitutions suivantes

$$(x_0 x_3 x_1 x_4)\ (x_2 x_5)\ (x_6 x_9 x_7 x_{11})\ (x_8 x_{10})$$
$$(x_0 x_7 x_1 x_6)\ (x_2 x_8)\ (x_3 x_9 x_4 x_{11})\ (x_5 x_{10}) .$$

Ces deux groupes sont d'ordre 72, et caractérisent des équations résolubles par radicaux.

5. Considérons maintenant les groupes transitifs de degré premier. Soit n le degré, N l'ordre du groupe. Puisque N est divisible par n mais non divisible par n^2, on a

$$N = n\nu\ (np+1)$$

Supposons les lettres rangées dans un ordre tel qu'une substitution circulaire du groupe est exprimée par

$$\theta = |k \quad k+1| ;$$

alors les substitutions permutables au groupe dérivé de θ sont de la forme

$$|k \quad ak+b|$$

Or nv est égal à l'ordre de ce dernier groupe, donc v est égal au nombre des substitutions du groupe donné qui sont de la forme $|k\ ak|$; v est donc un diviseur de $n-1$. On a donc ce théorème:

Théorème VII. L'ordre d'un groupe transitif entre un nombre premier de lettres est de la forme $nv\,(np+1)$, *où* n *est le degré,* $np+1$ *le nombre des substitutions régulières essentiellement différentes, c'est-à-dire, qui ne sont pas des puissances les unes des autres, et où* v *est le nombre des substitutions de la forme* $|k\ ak|$, *une substitution circulaire quelconque étant désignée par* $|k\ \ k+1|$.

Ces résultats sont en partie connus par les recherches de M. E. Mathieu, qui a démontré que le nombre des substitutions circulaires essentiellement différentes est de la forme $np+1$, et qu'il y en a au moins $\frac{N}{nv}$, un tel nombre pouvant être déduit des $|k\ \ k+b|$ en les transformant par les substitutions du groupe. Ce qu'il faut ajouter aux propositions de M. Mathieu pour avoir le théorème ci-dessus c'est donc que toutes les substitutions circulaires peuvent être déduite de la manière mentionnée, un point sur lequel M. Mathieu semble avoir conservé des doutes.

Qu'on se rapelle ici ces deux propositions également dues à M. E. Mathieu:

1) *Si* $p>0$, v *ne peut être égal à* 1.
2) *Si* $p>0$, *et que* n *soit de la forme* $4h+3$, v *ne peut être égal à* 2.

Étant donné l'ordre N d'un groupe transitif entre n lettres, notre théorème permet de déterminer le nombre des substitutions circulaires et le nombre des substitutions permutables au groupe dérivé d'une substitution circulaire. En effet v, étant moindre que n, est complètement déterminé par la congruence

$$\frac{N}{n} \equiv v \bmod n;$$

et puis on a

$$np+1 = \frac{N}{nv}.$$

Prenons pour exemple le groupe du degré $\frac{q^r-1}{q-1}$, q étant un nombre premier, que l'on peut déduire du groupe linéaire à r indices. Si r est un nombre premier impair, il peut arriver que $\frac{q^r-1}{q-1}$ est un nombre premier. Faisons donc

$$n = \frac{q^r-1}{q-1}$$

$$N = \frac{q^r-1}{q-1}(q^r-q)(q^r-q^2)\ldots(q^r-q^{r-1}).$$

Or on voit aisément que q est une racine primitive de la congruence

$$z^r \equiv 1 \bmod n;$$

par suite on a

$$z^{r-1} + z^{r-2} + \ldots + z + 1 \equiv (z-q)(z-q^2)\ldots(z-q^{r-1}).$$

Si maintenant on fait

$$z \equiv q^r \equiv 1,$$

on obtient

$$(q^r - q)(q^r - q^2)\ldots(q^r - q^{r-1}) \equiv r.$$

c'est-à-dire

$$\frac{N}{n} \equiv r$$

Si donc on choisit les indices de sorte qu'une substitution circulaire est représentée par $|k \;\; k+1|$, le groupe contiendra r substitutions de la forme $|k \;\; ak|$ savoir les $|k \;\; q^i k|$; le nombre des substitutions circulaires essentiellement différentes sera $\frac{q^r - q}{r}(q^r - q^2)\ldots(q^r - q^{r-1})$.

La formule $N = n\nu(np+1)$ réduit considérablement le nombre des diviseurs du produit $2 \cdot 3 \ldots n$ propres à désigner l'ordre d'un groupe transitif. Si par exemple on fait $n = 7$, ν doit être égal à 6 ou à 3, excepté pour les équations résolubles par radicaux. Mais s'il existe un groupe d'ordre $7(7p+1)6$, il y en a aussi un d'ordre $7(7p+1)3$ contenant celles des substitutions du premier groupe qui équivalent à un nombre pair de transpositions. Pour avoir les valeurs de $7p+1$ il suffit donc d'examiner le cas $n = 3$; donc $7p+1$ doit être un diviseur du nombre $2.5.4.3$, et par conséquent égal à un des nombres 1, 2^3, 5.3, $5.3.2^3$, dont le troisième doit être rejeté, puisqu'il n'y a pas de groupe d'ordre 5.3 entre 6 lettres. Pour $n = 11$ il n'y aura que 15 cas à examiner etc.

Examinons maintenant la composition des groupes en question. Soient donc G et H deux groupes transitifs, et soit G contenu dans H et permutable à ses substitutions. Soit de plus $n(np+1)\nu$ l'ordre de G, et désignons par $\theta_0\theta_1 \ldots \theta_{np}$ ses substitutions circulaires essentiellement différentes. G contient donc les $np+1$ groupes d'ordre n: θ_0^r, θ_1^r, $\ldots \theta_{np}^r$. Si l'on transforme ces groupes par une substitution circulaire quelconque de H, qui sera désignée par θ', on doit les reproduire dans un autre ordre; on à donc une substitution entre les $np+1$ groupes. Mais on voit sans peine que si un groupe θ_i^r n'est pas invariable par la transformation, il doit faire partie d'un cycle de n groupes. Donc au moins un des groupes est invariable par la transformation. Si nous supposons que c'est θ_0^r, ce groupe est permutable à θ', d'où l'on conclut

$$\theta' = \theta_0^b.$$

En effet, si l'on choisit les indices de sorte que

$$\theta_0 = |k \quad k+1|,$$

il n'y a parmi les $n(n-1)$ substitutions $|k \quad ak+b|$, seules permutables à θ_0^r, que les $|k \quad k+b|$ qui sont d'ordre n. Toutes les substitutions circulaires de H font donc partie de G.

Réciproquement, si G et H contiennent les mêmes substitutions circulaires et que H contienne G, H est composé avec G. Soit toujours $n(np+1)\nu$ l'ordre de G, celui de H sera $n(np+1)\nu\nu_1$, ν_1 étant un diviseur de $\frac{n-1}{\nu}$. Les substitutions de la forme $|k \quad ak|$ contenues dans H sont les puissances d'une seule d'entre elles; désignons celle-là par φ; celles qui appartiennent à G seront par conséquent les puissances de φ^{ν_1}. Or il est facile à voir que H dérive des substitutions $\theta_0\,\theta_1 \ldots \theta_{np}\,\varphi$. En effet le groupe dérivé de ces substitutions est contenu dans H; de l'autre côté son ordre ne peut être moindre que $n(np+1)\nu\nu_1$, puisqu'il a $np+1$ substitutions circulaires et $\nu\nu_1$ substitutions $|k \quad ak|$. De même G dérive des substitutions $\theta_0\,\theta_1 \ldots \theta_{np}\,\varphi^{\nu_1}$. G est donc permutable aux substitutions de H, s'il est permutable à φ. Or cela a lieu, car premièrement les transformées de $\theta_0\,\theta_1 \ldots \theta_{np}$ par φ sont des substitutions circulaires appartenant à H et par suite à G; secondement φ^{ν_1} est échangeable à φ.

Ainsi nous avons démontré le théorème suivant:

Théorème VIII. Pour qu'un groupe transitif de degré premier soit composé avec un groupe partiel, il faut et il suffit que le second groupe possède toutes les substitutions circulaires du premier.

Soit donnée une équation dont le groupe est H. Si l'on forme une fonction des racines invariable par les substitutions de G, mais variable par toute autre substitution, elle sera évidemment racine d'une équation abélienne de degré ν_1. En adjoignant cette fonction on réduit le groupe de l'équation à G.

Si donc une équation irréductible de degré n est composée, elle devient simple par l'adjonction de la racine d'une équation abélienne, dont le degré est un diviseur de $n-1$.

En supposant $p=0$, on retombe sur une propriété connue des équations résolubles par radicaux.