ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

EDMOND MAILLET

Sur quelques propriétés des groupes de substitutions d'ordre donné (suite et fin)

Annales de la faculté des sciences de Toulouse 1re série, tome 10, no 1 (1896), p. A5-A20

<http://www.numdam.org/item?id=AFST_1896_1_10_1_A5_0>

ANNALES

DE LA

FACULTÉ DES SCIENCES DE TOULOUSE.

SUR QUELQUES PROPRIÉTÉS DES GROUPES DE SUBSTITUTIONS D'ORDRE DONNÉ

(SUITE ET FIN) (1),

PAR M. EDMOND MAILLET,

Ingénieur des Ponts et Chaussées.

III.

Nous allons maintenant faire un certain nombre d'applications des théorèmes qui précèdent.

THÉORÈME I. — *Tout étant posé, comme au théorème I du* n° 1, *et m étant* >1, *on ne peut avoir* $n_\alpha = 0$ *pour* $\alpha > 1$, *quel que soit* α, *que si* G *contient un groupe d'ordre* $p^\theta > 1$ *permutable à ses substitutions et formé de substitutions d'ordre p échangeables.*

Supposons qu'on ait $n_\alpha = 0$ pour $\alpha > 1$ quel que soit α.

Si $n_1 = 0$, d'après un théorème de M. Sylow déjà employé [formule (1)], G contient un groupe unique d'ordre p^m permutable à ses substitutions, et par suite, un groupe d'ordre $p^\theta > 1$ permutable à ses substitutions et formé de substitutions d'ordre p échangeables, d'après le corollaire III du théorème IV, n° 2.

Si $n_1 \neq 0$, G renferme plusieurs groupes d'ordre p^m. D'après le théo-

(1) Voir *Annales de la Faculté des Sciences de Toulouse*, t. IX p. D.1.

rème I, n° 1, deux groupes différents d'ordre p^m, contenus dans G, ont en commun un groupe d'ordre p^{m-1}, sans quoi on aurait $n_\alpha \neq 0$ pour une valeur de $\alpha > 1$. Soient H, H′ deux groupes différents d'ordre p^m contenus dans G, P le groupe d'ordre p^{m-1} commun. D'après le corollaire III du théorème de M. Frobenius, on sait que P est permutable aux substitutions de H et de H′; par suite, à celles du groupe dérivé (H, H′); ce dernier groupe étant contenu dans G, p^m est la plus haute puissance de p, qui divise son ordre, et, d'après un théorème de M. Sylow [formule (1)], les groupes d'ordre p^m de (H, H′) sont les transformés de H par les substitutions de (H, H′) et, par suite, contiennent tous P.

Soient :

H″ un groupe de G d'ordre p^m non contenu dans (H, H′);
P_1 le groupe commun à H″ et H;
P_2 le groupe commun à H″ et H′.

Les groupes P_1 et P_2 sont d'ordre p^{m-1}. Je dis que H″ contient P et qu'on aura

$$P = P_1 = P_2;$$

sinon, $P \neq P_1 \neq P_2$, car si l'on avait $P_1 = P_2$, P_1 serait commun à H et H′, et l'on aurait $P = P_1$. Dès lors P_1 et P_2 étant contenus dans (H, H′), il en est de même du groupe (P_1, P_2) dérivé de P_1 et de P_2; mais (P_1, P_2) est contenu dans H″ et d'ordre $> p^{m-1}$, puisque P_1 et P_2 sont différents et d'ordre p^{m-1}. Donc $(P_1, P_2) = H''$ et H″ serait contenu dans (H, H′), contrairement à l'hypothèse. Il faut, par suite, supposer que H″ contient P.

Ainsi, tous les groupes de G d'ordre p^m doivent contenir P; d'après le corollaire III du théorème IV, n° 2, on conclut encore que G renferme un groupe d'ordre $p^\theta > 1$ permutable à ses substitutions et formé de substitutions d'ordre p échangeables.

Corollaire I. — Si $m > 1$ et $n_\alpha = 0$ pour $\alpha > 1$, G ne peut être simple (1).

Corollaire II. — Si $m > 1$ et $n_\alpha = 0$ pour $\alpha > 1$, G ne peut être primitif que s'il est linéaire et de degré p^θ.

(1) Nous supposons toujours, pour chaque corollaire, les choses posées comme au théorème lui-même.

Ce dernier corollaire résulte de la considération du corollaire III du théorème IV, n° 2.

THÉORÈME II. — *Tout étant posé comme au théorème I du* n° 1, *soit* $m > 1$ *et supposons un groupe de* G *d'ordre* p^m *formé de substitutions échangeables; quand une au plus des quantités* n_α *est* $\neq 0$, *ou bien on aura* $n_m \neq 0$, *ou bien* G *contiendra un groupe d'ordre* $p^\theta > 1$ *permutable à ses substitutions et formé de substitutions d'ordre* p *échangeables.*

Le raisonnement est analogue à celui du théorème précédent; tous les groupes de G d'ordre p^m sont formés de substitutions échangeables.

Quand $n_\alpha = 0$, quel que soit α, la propriété résulte encore d'un théorème de M. Sylow [formule (1)].

Quand n_α n'est différent de 0 que pour une valeur de α égale à β et $\neq m$, deux groupes H et H′ d'ordre p^m différents, et contenus dans G, ont en commun exactement un groupe P_β d'ordre $p^{m-\beta}$. Les substitutions de P_β étant échangeables à celles de H et de H′, par suite à celles de (H, H′), on voit facilement que P_β est commun à tous les groupes d'ordre p^m de (H, H′).

Enfin, un groupe H″, d'ordre p^m, contenu dans G, mais non dans (H, H′), contiendra encore P_β. Tous les groupes de G d'ordre p^m contiendront P_β et G renfermera encore un groupe d'ordre $p^\theta > 1$ permutable à ses substitutions et formé de substitutions d'ordre p échangeables.

Corollaire I. — G ne peut être simple que si $m = 1$, ou si $n_m \neq 0$, ou si deux des quantités n_α sont $\neq 0$.

Corollaire II. — G ne peut être primitif que si $m = 1$, ou si $n_m \neq 0$, ou si deux des quantités n_α sont $\neq 0$, ou si G est linéaire et de degré p^θ.

THÉORÈME III. — *Tout étant posé comme au théorème I du* n° 1, *soient* N *le degré de* G, $N - u_0$ *sa classe; si un groupe de* G *d'ordre* p^m *est formé de substitutions échangeables et si* $n_\alpha \neq 0$ *pour une valeur de* $\alpha < m$, *on aura* $u_0 \geq p$ *ou* $N \geq p^m(p^\alpha + 1)$.

En effet, supposons que, pour une valeur de α égale à β, on ait $n_\beta \neq 0$. Formons, comme au théorème précédent, le groupe $J = (H, H')$.

D'après la formule (10), J sera d'ordre

$$\vartheta = p^m v'(1 + n'_1 p + \ldots + n'_\beta p^\beta + \ldots).$$

Les deux groupes H et H′, contenus dans J, ayant, par hypothèse, exactement les $p^{m-\beta}$ substitutions de P_β communes, on aura $n'_\beta \neq 0$, d'après le théorème I, n° 1.

Supposons qu'on puisse trouver une lettre a_1 déplacée par P_β et laissée immobile par une substitution T de J. Soit $S = (a_1, a_2, \ldots), \ldots$ une substitution de P_β; S est échangeable aux substitutions de J, puisqu'elle l'est à celles de H et de H′, et est d'ordre $\geq p$. Les substitutions

$$T, \quad S^{-1}TS, \quad S^{-2}TS^2, \quad \ldots, \quad S^{p-1}TS^{p-1}$$

sont toutes égales, et T laisse immobiles les p lettres différentes que

$$1 = S^0, S^1, S^2, \ldots, S^{p-1}$$

substituent à a_1. On aura donc $u_0 \geq p$.

Supposons qu'une lettre a_1, déplacée par P_β, ne soit laissée immobile par aucune substitution de J. On voit facilement que J permute transitivement a_1 avec $\mathfrak{z}$ lettres différentes $a_1, a_2, \ldots, a_\mathfrak{z}$; par suite, G, qui contient J, est de degré $\geq \mathfrak{z} \geq p^m(p^\beta + 1)$, puisque $n'_\beta \neq 0$, ce qui démontre le théorème.

Si, en particulier, β est la plus petite valeur de α pour laquelle $n_\alpha \neq 0$, on obtient même, en serrant la question d'un peu plus près, le corollaire suivant, que nous nous contenterons d'énoncer :

Corollaire. — *Si β est la plus petite valeur de α pour laquelle $n_\alpha \neq 0$, et si $p > 2$, on aura $u_0 \geq p$ ou $N \geq p^m(2p^\beta + 1)$, sauf si $p^\beta + 1 = 2^\mu$.*

Théorème IV. — *Tout étant posé comme au théorème I du* n° 1, *si* G *contient une substitution d'ordre p^m et si $m > 1$,* G *contiendra un groupe d'ordre p permutable à ses substitutions, sauf quand $n_m \neq 0$.*

Soient $m > 1$ et $n_m = 0$. Deux groupes différents H et H′ d'ordre p^m, contenus dans G, ont en commun exactement un groupe P_α, d'ordre $p^{m-\alpha}$, avec $m - \alpha > 0$. Mais H est formé des puissances d'une substitution S d'ordre p^m, et les seules substitutions d'ordre p, que H contient, sont les puissances de $S^{p^{m-1}}$. P_α, contenant une substitution d'ordre p, contient $S^{p^{m-1}}$, et cette substitution est commune à tous les groupes de G d'ordre p^m, puisque $n_m = 0$.

D'après le corollaire III du théorème IV, n° 2, G contient un groupe

d'ordre $p^\theta > 1$ permutable à ses substitutions, et formé de substitutions d'ordre p échangeables. Ce groupe d'ordre p^θ étant commun à tous les groupes de G d'ordre p^m est contenu dans H et, par suite, est formé des puissances de $S^{p^{m-1}}$. Donc $\theta = 1$.

Le raisonnement précédent ne serait pas applicable, si l'on avait $n_\alpha = 0$, quel que soit α. Mais on sait qu'alors G contient un groupe unique H, d'ordre p^m permutable à ses substitutions, et, en raisonnant comme tout à l'heure, on voit encore que G contient un groupe d'ordre p permutable à ses substitutions.

Corollaire I. — Quand $m > 1$, G ne peut être simple que si $n_m \neq 0$.

Corollaire II. — Quand $m > 1$, G ne peut être primitif que si $n_m \neq 0$.

Si, en effet, G est primitif, et si $n_m = 0$, G contient un groupe d'ordre p permutable à ses substitutions et qui, d'après un théorème de M. Jordan (1), devrait être transitif. G serait donc de degré p, et ne pourrait avoir son ordre divisible par p^m avec $m > 1$.

Corollaire III. — Si G est simple, p^m est $<$ le plus grand diviseur de $\frac{\mathcal{G}}{p^m}$ inférieur à $\frac{\mathcal{G}}{p^m}$ [théorème dû à M. O. Hölder (2)].

En effet, d'après la formule (10),

$$\mathcal{G} = p^m \varphi (1 + n_1 p + \ldots + n_m p^m),$$

et $n_m \neq 0$, même quand $m = 1$ (sauf bien entendu le cas de $\mathcal{G} = p$ que nous écartons).

Si $\varphi > 1$, $\frac{\mathcal{G}}{p^m}$ est divisible par $(1 + n_1 p + \ldots + n_m p^m)$, qui est $< \frac{\mathcal{G}}{p^m}$ et $> p^m$. Le corollaire a lieu.

Soit donc $\varphi = 1$.

Supposons que H ne soit pas maximum dans G. Alors H est contenu dans un groupe F contenu dans G et $\mathcal{H} < \mathcal{F} < \mathcal{G}$. G, étant simple, est holoédriquement isomorphe (3) à un groupe transitif de degré $\frac{\mathcal{G}}{\mathcal{H}}$, qui contient une substitution d'ordre p^m, comme G, en sorte que $\frac{\mathcal{G}}{\mathcal{H}} > p^m$, puisque $\frac{\mathcal{G}}{\mathcal{F}}$

(1) *Traité des Substitutions*, p. 41.

(2) *Mathematische Annalen*, t. XL, p. 55 et suiv.

(3) W. Dyck, *Math. Annalen*, t. XXII, p. 94. — *Voir* aussi notre *Thèse de Doctorat*, p. 12.

est premier à p. Donc

$$p^m = \mathcal{H} < \frac{\mathcal{G}}{\mathcal{F}} \qquad \text{et} \qquad \frac{\mathcal{G}}{p^m} > \frac{\mathcal{G}}{\mathcal{F}} \qquad \text{avec} \qquad \frac{\mathcal{G}}{p^m} \equiv 0 \left(\text{mod } \frac{\mathcal{G}}{\mathcal{F}}\right),$$

ce qui montre que le corollaire a encore lieu.

Supposons que H soit maximum dans G. Le groupe G est holoédriquement isomorphe à un groupe primitif G′ de degré $\frac{\mathcal{G}}{p_m}$.

G′ est de classe $\frac{\mathcal{G}}{p^m} - 1$; en effet, si cela n'a pas lieu, deux groupes H'_1, H'_2 de G′ (1), formés chacun de l'ensemble des substitutions de G′, qui laissent immobiles respectivement une lettre a'_1 ou a'_2 de G′ ne seront pas de classe $\frac{\mathcal{G}}{p^m} - 1$. H'_1 contiendra une substitution différente de l'unité et qui laissera une lettre $\neq a'_1$ immobile. Choisissons a'_2 identique à cette lettre. Les deux groupes H'_1, H'_2 auront, en commun, une substitution différente de l'unité; cette substitution sera échangeable à celles de H'_1 et de H'_2; par suite à celles du groupe dérivé (H'_1, H'_2), qui coïncide avec G′, puisque H'_1 est maximum dans G′. Ce dernier groupe ne serait donc pas simple, contrairement à l'hypothèse, et G′ est de classe $\frac{\mathcal{G}}{p^m} - 1$. Par suite, il contient exactement (2) $\frac{\mathcal{G}}{p^m} - 1$ substitutions déplaçant $\frac{\mathcal{G}}{p^m}$ lettres et régulières, qui sont d'ordre premier à p.

Il ne reste plus qu'à raisonner, comme le fait M. O. Hölder, si $\frac{\mathcal{G}}{p^m} = q^{m'}$ (q premier), G′ appartient à ce que nous avons appelé (3) la première catégorie des groupes transitifs de classe $\frac{\mathcal{G}}{p^m} - 1$ et de degré $\frac{\mathcal{G}}{p^m}$ et est composé. Sinon, soit q le plus grand diviseur premier de $\frac{\mathcal{G}}{p^m}$. D'après la formule (2),

$$\mathcal{G} = q(N_1 + 2N_2 + \dots),$$

les groupes K et H, relatifs à cette formule (2), étant ici formés des puis-

---

(1) H'_1 et H'_2 sont tous deux de degré $\frac{\mathcal{G}}{p^m} - 1$, d'après le théorème VII, n° 2.

(2) *Voir* notre *Thèse de Doctorat*, p. 49-50.

(3) *Thèse de Doctorat*, p. 50 et 55.

sances de la même substitution de G' d'ordre q. G' renferme au moins $\frac{G}{qN_1}$ groupes transformés différents de ce groupe d'ordre q, c'est-à-dire au moins $\frac{G}{qN_1}(q-1)$ substitutions d'ordre q. Soit q_1 un diviseur premier de $\frac{G}{p^m}$ différent de q; on aura

$$\frac{G}{qN_1}(q-1) \geqq \frac{G}{qN_1} q_1.$$

Mais

$$\frac{G}{p^m} - 1 > \frac{G}{qN_1}(q-1)$$

et

$$\frac{G}{p^m} > \frac{G q_1}{qN_1},$$

ou

$$\frac{G}{qN_1} < \frac{G}{q_1 p^m}.$$

G étant simple et renfermant un groupe d'ordre qN_1 est holoédriquement isomorphe (1) à un groupe transitif de degré $\frac{G}{qN_1}$; ce groupe renfermant une substitution d'ordre p^m, son degré est $\geqq p^m$ et

$$\frac{G}{qN_1} \geqq p^m,$$

ce qui donne

$$p^m < \frac{G}{p^m}\frac{1}{q_1}$$

et le corollaire est complètement démontré.

THÉORÈME V. — *Tout étant posé comme au théorème I du* n° 1, *si* G *est transitif et de degré* $N \not\equiv 0 \pmod p$, *soient* H *un groupe d'ordre* p^m *de* G, *permutant les lettres qu'il déplace transitivement* p^{λ_1} *à* p^{λ_1}, p^{λ_2} *à* p^{λ_2}, ..., *et* $\lambda_1 \geqq \lambda_2 \geqq \ldots$: *une des quantités* n_α *avec* $\alpha \geqq \lambda_1$ *est* $\not\equiv 0$.

En effet, on peut toujours trouver une lettre b déplacée par H, et permutée par H avec p^{λ_1} lettres; soit a une lettre non déplacée par H.

G étant transitif contient toujours une substitution de la forme

$$S = \begin{pmatrix} a, \ldots \\ b, \ldots \end{pmatrix}.$$

---

(1) W. DYCK, *Math. Annalen*, t. XXII, p. 94. — *Voir* aussi notre *Thèse de Doctorat*, p. 12.

Le groupe $S^{-1}HS$, transformé de H par S, ne déplace pas b et est d'ordre p^m. Or, le groupe des substitutions de H qui laissent b immobile est d'ordre $p^{m-\lambda_1}$; donc H et $S^{-1}HS$ ont, en commun au plus, un groupe d'ordre $p^{m-\lambda_1}$, et il ne reste plus, pour établir le théorème, qu'à appliquer le théorème I du n° 1.

Si, en particulier, $\lambda_1 = m$, ce qui arrive toujours quand H a son degré égal à sa classe, on aura $n_m \not\equiv 0$.

Remarque. — En s'appuyant sur ce théorème et sur le théorème II précédent, on retrouve des résultats compris dans le théorème I précédent.

En effet, si $\lambda_1 > 1$, le théorème I a lieu, à condition d'y supposer G transitif et $N \not\equiv 0 \pmod{p}$. Supposons $\lambda_1 = 1$, par suite $\lambda_1 = \lambda_2 = \ldots = 1$.

Soit T une substitution de H; on a

$$T = T_1 T_2 \ldots,$$

$T_1, T_2, \ldots$ étant les cycles de T, qui sont tous d'ordre p, puisque $\lambda_1 = \lambda_2 = \ldots = 1$.

Toute substitution T' de H, qui contient dans un de ses cycles T'_1 des lettres de T_1, par exemple, est telle que ce cycle est une puissance T_1^{α} de T_1; en effet, si cela n'a pas lieu, ou T'_1 ne contiendra que des lettres de T_1, et l'on déduira facilement de T et de T' une substitution contenue dans H, laissant une des lettres de T_1 immobile et en permutant entre elles quelques autres, par suite d'ordre non diviseur de $\mathfrak{H} = p^m$, ce qui est absurde; ou T'_1 contiendra à la fois des lettres de T_1 et des lettres ne faisant pas partie de T_1, ce qui exigerait $\lambda_1 > 1$ contrairement à l'hypothèse. T'_1 doit donc être une puissance T_1^{α} de T_1.

Dès lors, si $T_1, T_2, \ldots; T'_1, T'_2, \ldots; \ldots$ sont les cycles des diverses substitutions de H différents et qui ne sont pas deux à deux puissances l'un de l'autre, ces cycles n'ont deux à deux aucune lettre commune; les substitutions circulaires $T_1, T_2, \ldots; T'_1, T'_2, \ldots; \ldots$ sont échangeables et le groupe dérivé contient H et est formé de substitutions échangeables. H est donc formé de substitutions échangeables, et l'on peut appliquer à G le théorème II précédent, ce qui conduit encore au théorème I précédent, quand on y suppose G transitif et $N \not\equiv 0 \pmod{p}$.

On conclut de là facilement ce théorème I, d'une manière générale, pour le cas où G est simple; on n'a besoin, en effet, que de l'établir pour un groupe holoédriquement isomorphe à G. Or, G, étant simple, est toujours

holoédriquement isomorphe à un groupe transitif G' de degré $N \not\equiv 0 \pmod{p}$ (1), auquel on peut appliquer ce que nous venons de dire.

THÉORÈME VI. — *Tout étant posé comme au théorème I du* n° 1, *soit* $N \not\equiv 0 \pmod{p}$ *le degré de* G *et* $N - u_0$ *sa classe. Si une seule des quantités* $N-1, N-2, \ldots, N-u_0$ *est divisible par* p, *on a* $n_m \neq 0$ (*ce qui doit toujours avoir lieu si* G *est transitif*) *ou* $\nu > 1$.

En effet, soit H un groupe de G d'ordre p^m, et ρp le degré de H; on a $\rho p \geq N - u_0$, d'après la définition de la classe (2), et, par suite, ρp est l'un des nombres $N-1, N-2, \ldots, N-u_0$. Une lettre b, déplacée par H, sera permutée par H avec p^{λ_1} lettres; si $\lambda_1 < m$, le groupe des substitutions de H qui laissent b immobile est d'ordre $p^{m-\lambda_1} > 1$, de degré $\rho' p$ avec $\rho' < \rho$, et il faudrait $\rho' p > N - u_0$. Il y aura donc, parmi les nombres $N-1, N-2, \ldots, N-u_0$, au moins deux multiples de p, contrairement à l'hypothèse. Donc $\lambda_1 = m$.

b est une lettre arbitrairement choisie parmi celles que H déplace. Si l'on peut trouver une lettre a de G non déplacée par H, et telle qu'il existe une substitution

$$S = \begin{pmatrix} a, & \ldots \\ b, & \ldots \end{pmatrix}$$

dans G, on verra, en raisonnant comme au théorème précédent, que la seule substitution de H qui laisse b immobile est l'unité, que toutes les substitutions de $S^{-1}HS$ laissent b immobile, et, par suite, que H et $S^{-1}HS$ n'ont d'autre substitution commune que l'unité; ces groupes étant tous deux d'ordre p^m, on aura, d'après le théorème I du n° 1, $n_m \neq 0$. On peut remarquer d'ailleurs que S existe toujours quand G est transitif.

Si l'on ne peut trouver aucune substitution de la forme S, les lettres a, a', ... que H laisse immobiles sont déplacées par G, puisque G est de degré N, et permutées exclusivement entre elles par les substitutions de G : on voit d'abord qu'il faudra $N - 1 \not\equiv 0 \pmod{p}$; de plus, d'après le théorème VIII du n° 2, il faudra $\nu > 1$.

THÉORÈME VII. — *Tout étant posé comme au théorème I du n° 1, si* G *est* k *fois transitif, de degré* $N \not\equiv 0 \pmod{p}$, *de classe* $N - u_0$, *et si, de plus, il y a* l *multiples de* p *parmi les nombres* $N-1, N-2, \ldots,$

(1) W. DYCK, *loc. cit.* — *Voir* aussi notre *Thèse de Doctorat*, p. 12 et 19.
(2) JORDAN, *Théorèmes sur les groupes primitifs* (*Journal de Liouville*), 1871.

$N - u_0$, *une des quantités* n_α *avec* $\alpha \geqq \frac{l'm}{l}$ *est* $\neq 0$, *l'étant la plus petite des trois quantités* k, l *et* $N - \rho p$, ρp *étant le degré d'un groupe* H *de* G *d'ordre* p^m.

En effet,, ρp est $\leqq$ au plus grand des multiples de p compris parmi les nombres $N - 1$, ..., $N - u_0$; supposons que H permute ses ρp lettres transitivement p^{λ_1} à p^{λ_1}, p^{λ_2} à p^{λ_2}, avec $\lambda_1 \geqq \lambda_2 \geqq \ldots$.

Soient b une lettre que H permute avec p^{λ_1} lettres, a une lettre que H ne déplace pas, H_1 le groupe des substitutions de H qui laissent b immobile. G étant transitif, on aura une substitution de la forme

$$S = \begin{pmatrix} a, & \ldots \\ b, & \ldots \end{pmatrix}.$$

Supposons que H_1 permute les $\rho_1 p$ lettres qu'il déplace (avec $\rho_1 < \rho$) transitivement $p^{\lambda_1^{(1)}}$ à $p^{\lambda_1^{(1)}}$, $p^{\lambda_2^{(1)}}$ à $p^{\lambda_2^{(1)}}$, ..., avec $\lambda_1^{(1)} \geqq \lambda_2^{(1)} \geqq \ldots$. Si l'on a à la fois $k > 1$, $N - \rho p > 1$ et $\mathfrak{H}_1 > 1$, on pourra toujours trouver une lettre $a_1 \neq a$ que H ne déplace pas, et une substitution de la forme S qui remplace a_1 par une lettre $b_1 \neq b$ permutée par H_1 avec $p^{\lambda_1^{(1)}}$ lettres.

En continuant de la sorte, on forme une suite de groupes H, H_1, ..., H_j, ..., $H_{l'}$; H_j permute transitivement les $\rho_j p$ lettres qu'il déplace (avec $\rho_j < \rho_{j-1} < \ldots < \rho_1 < \rho$) $p^{\lambda_1^{(j)}}$ à $p^{\lambda_1^{(j)}}$, $p^{\lambda_2^{(j)}}$ à $p^{\lambda_2^{(j)}}$, ..., avec

$$\lambda_1^{(j)} \geqq \lambda_2^{(j)} \geqq \ldots;$$

si b_j est permutée par H_j avec $p^{\lambda_1^{(j)}}$ lettres, H_{j+1} est formé de l'ensemble des substitutions de H_j qui laissent b_j immobile; si, de plus, a_j est laissée immobile par H, on peut trouver une substitution de la forme S

$$S = \begin{pmatrix} a, & a_1, & \ldots, & a_j, & \ldots \\ b, & b_1, & \ldots, & b_j, & \ldots \end{pmatrix},$$

où a, a_1, ..., a_j sont des lettres différentes laissées immobiles par H et où b, b_1, ..., b_j sont des lettres différentes déplacées par H. Les conditions de l'existence d'un groupe H_j et d'une substitution S jouissant des propriétés ci-dessus sont qu'on ait à la fois

$$k > j, \quad N - \rho p > j \qquad \text{et} \qquad \mathfrak{H}_j > 1.$$

On finira donc toujours par trouver dans la suite H, H_1, ..., H_j, ..., $H_{l'}$ un groupe $H_{l'}$ pour lequel on n'aura pas à la fois $k > l'$, $N - \rho p > l'$ et

$\mathfrak{H}_{l'} > 1$. Les groupes de cette suite étant d'ailleurs de degrés ρp, $\rho_1 p$, ..., $\rho_{l'-1} p$, $\mathfrak{H}_{l'}$ et chacun de ces nombres étant plus petit que le précédent, les nombres ρp, $\rho_1 p_1$, ..., $\rho_{l'-1} p$ sont des multiples de p compris parmi les nombres $N-1$, $N-2$, ..., $N-u_0$ et l'on a $l' \leq l$.

Considérons maintenant les deux groupes $S^{-1}HS$ et H : $S^{-1}HS$ laisse b immobile, et, par suite, ne peut avoir en commun avec H que des substitutions du groupe H_1 ; $S^{-1}HS$ laisse b_1 immobile, et, par suite, ne peut avoir en commun avec H et H_1 que des substitutions du groupe H_2 ; ... ; $S^{-1}HS$ laisse $b_{l'-1}$ immobile, et, par suite, ne peut avoir en commun avec H, H_1, ..., $H_{l'-1}$ que des substitutions du groupe $H_{l'}$.

Si donc nous montrons que l'ordre $\mathfrak{H}_{l'}$ de $H_{l'}$ est $\leq p^{m\left(1-\frac{l'}{l}\right)}$, quand $\mathfrak{H}_{l'} > 1$, l'application du théorème I du n° 1 donnera immédiatement notre théorème.

Or si l'on ne veut pas se préoccuper de la substitution S, c'est-à-dire des deux conditions $k > j$, $N - \rho p > j$, on peut prolonger la suite H, H_1, ..., $H_{l'}$ jusqu'à ce qu'on tombe sur un groupe $H_{m'}$ pour lequel $\mathfrak{H}_{m'} = 1$. Soit

$$\text{(20)} \qquad H, H_1, \ldots, H_i, \ldots, H_{m'},$$

la nouvelle suite obtenue qui comprend la première.

D'après ce qui a été dit précédemment, on aura

$$\text{(21)} \qquad \begin{cases} \lambda_1 \geq \lambda_2 \geq \ldots, \\ \lambda_1^{(1)} \geq \lambda_2^{(1)} \geq \ldots, \\ \ldots\ldots\ldots\ldots\ldots \\ \lambda_2^{(j)} \geq \lambda_2^{(j)} \geq \ldots, \\ \ldots\ldots\ldots\ldots\ldots \\ \lambda_1^{(m'-1)} \geq \lambda_2^{(m'-1)} \geq \ldots, \end{cases}$$

et

$$\text{(22)} \qquad \begin{cases} \mathfrak{H} = p^{\lambda_1} \mathfrak{H}_1, \\ \mathfrak{H}_1 = p^{\lambda_1^{(1)}} \mathfrak{H}_2, \\ \ldots\ldots\ldots\ldots\ldots \\ \mathfrak{H}_j = p^{\lambda_1^{(j)}} \mathfrak{H}_{j+1}, \\ \ldots\ldots\ldots\ldots\ldots \\ \mathfrak{H}_{m'-1} = p^{\lambda_1^{(m'-1)}} \mathfrak{H}_{m'} = p^{\lambda_1^{(m'-1)}} > 1, \end{cases}$$

puisque $\mathfrak{H}_j > \mathfrak{H}_{j+1}$ quel que soit j.

On tirera de là

$$\mathfrak{H} = p^{\lambda_1} p^{\lambda_1^{(1)}} \dots p^{\lambda_1^{(l'-1)}} \mathfrak{H}_{l'} = p^m$$

et

$$\mathfrak{H}_{l'} = p^{\lambda_1^{(l')}} \dots p^{\lambda_1^{(m'-1)}}.$$

De plus,

$$\lambda_1 \geqq \lambda_1^{(1)} \geqq \dots \geqq \lambda_1^{(l'-1)} \geqq \lambda_1^{(l')} \dots \geqq \lambda_1^{(m'-1)}.$$

On en déduit facilement

$$\mathfrak{H}_{l'} \leqq p^{m\left(1-\frac{l'}{m'}\right)}.$$

Or on peut voir qu'on a $m' \leqq l$ comme on a vu $l' \leqq l$; donc

$$\mathfrak{H}_{l'} \leqq p^{m\left(1-\frac{l'}{l}\right)}.$$

Nous avons vu qu'alors le théorème a lieu.

On remarquera, d'après ce qui précède, que, si $\mathfrak{H}_{l'} = 1$, $l' = m'$ et $\alpha = m$; si $l' = k$, $\alpha \geqq \frac{k}{l} m$; si $l' = N - \rho p$, $\alpha \geqq \frac{N - \rho p}{l} m$.

En appliquant ce théorème pour divers cas, on en déduit de nombreux corollaires; nous citerons les suivants :

Corollaire I. — Si G est transitif avec $N \not\equiv 0 \pmod p$, et si parmi les nombres $N-1$, $N-2$, ..., $N-u_0$ il n'y en a qu'un qui soit divisible par p, il faut $n_m \neq 0$.

Corollaire II. — Si G est transitif avec $N \not\equiv 0 \pmod p$, et si parmi les nombres $N-1$, $N-2$, ..., $N-u_0$ il n'y en a que deux qui soient divisibles par p, une des quantités n_α avec $\alpha \geqq \frac{m}{2}$ est $\neq 0$; si en même temps G est deux fois transitif et $N-1 \not\equiv 0 \pmod p$, il faut $n_m \neq 0$.

Le théorème VII est d'ailleurs une extension du théorème V précédent.

Applications.

Les théorèmes qui précèdent permettent de traiter complètement l'application de la formule (10) au cas où $m = 2$.

Soit p^2 la plus haute puissance de p (p étant premier), qui divise l'ordre g d'un groupe G. On sait, d'après un des théorèmes de M. Sylow (1),

(1) Mémoire déjà cité, p. 587.

qu'un groupe H de G d'ordre p^2 est formé de substitutions échangeables. Nous pouvons donc alors appliquer en particulier les théorèmes II et III.

THÉORÈME VIII. — *Soit p^2 la plus haute puissance du nombre premier p qui divise l'ordre $\mathcal{G}$ d'un groupe* G; *on aura*

$$\mathcal{G} = p^2 \varphi(1 + n_1 p + n_2 p^2).$$

Si $n_2 = 0$, G *contiendra un groupe d'ordre p ou p^2 permutable à ses substitutions et ne pourra être primitif que s'il est linéaire et de degré p^2.*

Si $n_1 \neq 0$ et $p > 2$, N *étant le degré de* G, *et* $N - u_0$ *sa classe, on aura, soit $u_0 \geq p$ ou $N \geq p^2(2p + 1)$ quand $p + 1 \neq 2^\mu$, soit $u_0 \geq p$ ou $N \geq p^2(p + 1)$ quand $p + 1 = 2^\mu$.*

Corollaire I. — Si G est simple, on a $n_2 \neq 0$.

Corollaire II. — Si G est degré ρp^2 $(p > 2)$ avec $\rho < p$, on aura $u_0 \geq p$, quand $n_1 \neq 0$.

On pourrait déduire encore des théorèmes précédents d'autres propriétés pour le groupe G; nous n'insisterons pas.

Énonçons encore le théorème suivant :

THÉORÈME IX. — *Pour un groupe* G *transitif de degré p^3 et de classe $p^3 - u_0$ avec $u_0 < p$ la formule* (10) *se réduit à*

$$\mathcal{G} = p^3 \varphi(1 + n_3 p^3).$$

On peut surtout appliquer avec fruit les théorèmes qui précèdent dans l'étude des groupes primitifs G de degré N et de classe $N - u_0$, quand u_0 a une valeur donnée, car le plus grand nombre des théorèmes précédents est applicable aux nombres premiers diviseurs de $\mathcal{G}$ qui sont $> u_0$. Voici des exemples :

THÉORÈME X. — *ρ étant donné, un groupe primitif* G *de classe* $N - 2$ *et de degré* $N = \rho p^2$ *(p premier) ne peut exister en général que s'il est deux fois transitif et si $\rho p^2 = q^m + 1$ (q premier).*

Les exceptions n'ont lieu que pour des valeurs de p limitées en fonction de ρ.

Nous considérerons seulement le cas de $\rho = 1$; la démonstration est la même, quel que soit ρ, en supposant $p > \rho$ et $p > 2$.

Quand $p > 2$ et $\rho = 1$, on peut appliquer à G le théorème VIII précédent et son corollaire II. On a

$$\mathcal{G} = p^2 \varphi(1 + n_2 p^2).$$

Si $n_2 = 0$, G n'est pas de classe $p^2 - 2$, puisque alors G étant primitif est linéaire et de degré p^2.

Soit $n_2 > 0$. D'après le corollaire du théorème II, n° 1, $\mathcal{G}$ divise $p^2(p^2-1)(p^2-2)$ et l'on peut écrire

$$p^2 \nu (1 + n_2 p^2) l = p^2 (p^2-1)(p^2-2),$$

d'où

$$l\nu(1 + n_2 p^2) = (p^2-1)(p^2-2),$$

$$l\nu \equiv 2 \pmod{p^2} \quad \text{ou} \quad l\nu = 2 + \lambda p^2,$$

ce qui donne

$$(2 + \lambda p^2)(1 + n_2 p^2) = (p^2-1)(p^2-2).$$

Or si $\lambda > 0$, le premier membre est supérieur à p^4 et le deuxième inférieur à p^4, puisque $n_2 > 0$, et l'égalité précédente est impossible.

Soit $\lambda = 0$.

$$2(1 + n_2 p^2) = (p^2-1)(p^2-2)$$

et $l\nu = 2$.

Si $l = 1$, $\nu = 2$, G est trois fois transitif, puisque son ordre est

$$p^2(p^2-1)(p^2-2),$$

son degré p^2 et sa classe $p^2 - 2$ (théorème III, n° 1 et corollaire); si $l = 2$,

$$\nu = 1, \quad \mathcal{G} = \frac{p^2(p^2-1)(p^2-2)}{2}.$$

Or on sait (1) que l'ordre d'un groupe transitif de degré p^2 et de classe $p^2 - 2$ est de la forme

$$\mathcal{G} = p^2(\mathfrak{K}\sigma + 1)\mathfrak{K},$$

où $\mathfrak{K}$ est l'ordre du groupe des substitutions qui laissent deux lettres immobiles, $\mathfrak{K}$ divisant $p^2 - 2$ et $\mathfrak{K}\sigma + 1$ divisant $p^2 - 1$. Dès lors $\mathfrak{K}$ est le plus grand commun diviseur de $\frac{\mathcal{G}}{p^2}$ et $p^2 - 2$, puisque p est impair, et l'on aurait

$$\mathfrak{K} = p^2 - 2, \quad \text{d'où} \quad \mathfrak{K}\sigma + 1 = \frac{p^2-1}{2},$$

résultat évidemment absurde.

On doit donc supposer $l = 1$, $\nu = 2$ et G trois fois transitif. On sait (2)

(1) *Voir* notre *Thèse de Doctorat*, p. 69-70.

(2) JORDAN, *Recherches sur les substitutions* (*Journal de Liouville*; 1872).

qu'il faut $p^2 - 1 = q^\mu$, q étant un nombre premier ; p étant impair, il faut

$$p^2 - 1 = (p+1)(p-1) = 2^\mu = 2^3 \quad \text{et} \quad p = 3.$$

Donc :

Corollaire. — Un groupe de degré p^2 (p premier impair) et de classe $p^2 - 2$ primitif est trois fois transitif et de degré 9.

En appliquant de même le théorème IX aux groupes primitifs de degré p^3 et de classe $p^3 - 2$, on verrait qu'on doit avoir $p^3 - 1 = 2^\mu$ quand p est impair; or $p^3 - 1 = (p^2 + p + 1)(p - 1)$ ne peut être égal à 2^μ puisque $p^2 + p + 1 =$ un nombre impair quand p est impair. Donc :

THÉORÈME XI. — *Il n'existe aucun groupe primitif de degré p^3 (p premier impair) et de classe $p^3 - 2$.*

THÉORÈME XII. — *Soit* G *un groupe transitif de degré ρp (p premier et $\rho < p$), de classe $\rho p - u_0$ (avec $u_0 < p$); dans la formule* (1) *de M. Sylow qui correspond à* G, *si $n > 0$, p est limité supérieurement en fonction de ρ, u_0 et n.*

D'après la formule (1) de M. Sylow

$$\mathcal{G} = p^\nu (np + 1) \quad \text{et} \quad n > 0$$

par hypothèse.

D'après le corollaire du théorème II, n° 1, G divise le produit

$$\rho p (\rho p - 1)(\rho p - 2) \dots (\rho p - u_0),$$

et $np + 1$ divise le produit

$$\rho (\rho p - 1)(\rho p - 2) \dots (\rho p - u_0).$$

Soit δ le plus petit commun multiple de ρ et de n : un diviseur commun à $\rho p - j$ et à $np + 1$ est un diviseur commun à $\frac{\delta}{\rho}(\rho p - j)$ et $\frac{\delta}{n}(np + 1)$. Le plus grand commun diviseur de $\rho p - j$ et $np + 1$ divise donc $\frac{\delta}{\rho}(\rho p - j)$ et $\frac{\delta}{n}(np + 1)$, et, par suite, leur différence

$$\frac{\delta}{n} + \delta \frac{j}{\rho} = \delta \left(\frac{1}{n} + \frac{j}{\rho} \right).$$

Le plus grand commun diviseur de

$$np + 1 \qquad \text{et} \qquad \rho (\rho p - 1)(\rho p - 2) \dots (\rho p - u_0),$$

qui est $np+1$, divisera le produit

$$\rho\delta^{u_0}\left(\frac{1}{n}+\frac{1}{\rho}\right)\left(\frac{1}{n}+\frac{2}{\rho}\right)\cdots\left(\frac{1}{n}+\frac{u_0}{\rho}\right),$$

en sorte que

$$p<\rho\frac{\delta^{u_0}}{n}\left(\frac{1}{n}+\frac{1}{\rho}\right)\left(\frac{1}{n}+\frac{2}{\rho}\right)\cdots\left(\frac{1}{n}+\frac{u_0}{\rho}\right),$$

ce qui montre le théorème.

En particulier quand $\rho=1$ on a $\delta=n$, et $np+1$ doit diviser le produit

$$(n+1)(2n+1)\ldots(u_0n+1).$$

Remarque I. — On peut établir un théorème analogue pour un groupe G remplissant toutes les conditions énoncées au théorème ci-dessus, sauf celle d'être transitif, à condition que ce groupe G ait son ordre divisible par p.

Remarque II. — Le théorème VIII et ses corollaires permettent d'établir un théorème analogue pour les groupes de degré ρp^2 (p premier et $\rho<p$), de classe ρp^2-u_0 (avec $u_0<p$).

Remarque III. — Le théorème IX permet d'établir un théorème analogue pour les groupes de degré p^3 (p premier) transitifs, de classe p^3-u_0 (avec $u_0<p$).

28 mai 1894.