SUR QUELQUES PROPRIÉTÉS

DES

GROUPES DE SUBSTITUTIONS D'ORDRE DONNÉ,

PAR M. EDMOND MAILLET,

Ingénieur des Ponts et Chaussées.

INTRODUCTION.

Quand on se donne *a priori* l'ordre d'un groupe de substitutions, ce groupe doit satisfaire dans bien des cas à certaines conditions : ainsi, un groupe d'ordre $p_1 p_2 \dots p_n p^\alpha$ où $p_1, p_2, \dots, p_n, p$ sont des nombres premiers différents et où $p_1 < p_2 < \dots < p_n < p$ est toujours composé et même résoluble (1).

Réciproquement, des propriétés d'un groupe étant données, son ordre doit satisfaire dans bien des cas à certaines conditions : ainsi, quand p^m est la plus haute puissance du nombre premier p qui divise l'ordre $\mathcal{G}$ d'un groupe G (2), ce groupe renfermera au moins un groupe d'ordre p^m; on aura

$$\mathcal{G} = p^m \nu (1 + np), \tag{1}$$

où ν est premier à p, et où $p^m \nu$ est l'ordre du groupe des substitutions de G qui sont permutables à un groupe de G d'ordre p^m; de plus, les divers groupes d'ordre p^m de G seront les transformés d'un d'entre eux par les substitutions de G (3).

(1) FROBENIUS, *Sitzungsberichte der k. p. Akademie der Wiss. zu Berlin*, 4 mai 1893.

(2) En général, quand nous désignerons par A, B, ..., G, H, ... des groupes de substitutions, nous désignerons par $\mathfrak{A}$, $\mathfrak{B}$, ..., $\mathcal{G}$, $\mathcal{H}$, ..., respectivement l'ordre de ces groupes.

(3) SYLOW, *Théorèmes sur les groupes de substitutions* (*Mathematische Annalen*, t. V, p. 584).

Nous nous proposons de donner ici un certain nombre de théorèmes relatifs aux deux problèmes généraux dont nous venons de parler; il nous arrivera, pour la facilité de l'exposé, d'établir et d'énoncer quelques propriétés déjà publiées soit explicitement, soit implicitement. Pour éviter *a priori* tout oubli à cet égard, nous renverrons aux œuvres de M. Jordan et en particulier à son *Traité des substitutions,* au *Traité des substitutions* de M. Netto, et aux divers Mémoires que nous aurons occasion de citer.

Parmi les propriétés que nous établirons, nous croyons devoir mentionner particulièrement les suivantes :

1° L'ordre $\mathcal{G}$ d'un groupe G de classe $N - u_0$ et de degré N divise le produit

$$\Theta = N(N-1)\dots(N-u_0).$$

Nous en donnons plusieurs démonstrations.

2° Dans la formule (1) de M. Sylow, quand $m > 1$ et $n < p$, G est composé, et ne peut être primitif que s'il est linéaire et de degré p^θ.

De plus, si l'on fait des hypothèses particulières sur le groupe d'ordre p^m contenu dans G, on trouve des conditions plus restrictives; ainsi :

3° Dans la formule (1) de M. Sylow, quand $m > 1$ et quand G contient une substitution d'ordre p^m, G ne peut être simple ou primitif que si $n \geq p^{m-1}$.

I.

M. Frobenius a généralisé la formule (1) précitée de M. Sylow ainsi qu'il suit (1) :

THÉORÈME. — *Soit* G *un groupe de substitutions d'ordre* $\mathcal{G}$ *en contenant deux autres* H *et* K *d'ordres* $\mathcal{H}$ *et* $\mathcal{K}$; *on aura*

$$\mathcal{G} = \mathcal{K}(N_1 + 2N_2 + \dots + qN_q + \dots). \tag{2}$$

La condition nécessaire et suffisante pour que $N_q \neq 0$ *est qu'il existe dans* K *un groupe d'ordre* $\frac{\mathcal{H}}{q}$ *maximum parmi les groupes de* K *qu'une substitution de* G *convenablement choisie transforme en un groupe de* H.

Nous avons d'ailleurs établi postérieurement le théorème ci-dessus dans le cas particulier où $H = K$ (2).

---

(1) *Ueber die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul* [*Journal für Mathematik,* t. CI, p. 281, formule (3)].

(2) *Thèse de Doctorat,* p. 114; Gauthier-Villars, 1892.

Nous allons démontrer la formule de M. Frobenius par un procédé semblable à celui qu'a employé M. Sylow pour obtenir sa formule.

Conservons les notations précédentes : soient z_1 une fonction rationnelle des lettres de G invariable par toutes les substitutions de K, mais variable par toute autre substitution;

$$z_1, z_2, \ldots, z_{\frac{G}{\mathfrak{H}}} \tag{3}$$

les $\frac{G}{\mathfrak{H}}$ valeurs différentes que prend z_1 quand on y opère les substitutions de G.

Effectuons dans les fonctions (3) les substitutions de H,

$$1, h_2, \ldots, h_{\mathfrak{H}}. \tag{4}$$

Ces substitutions faisant partie de G changeront une quelconque z_i des fonctions (3) en un certain nombre d'entre elles

$$z_i, z_{i_1}, \ldots, z_{i_{q-1}}, \tag{5}$$

dérivées de z_i par les substitutions de H. Ces dernières échangeront les fonctions (5) exclusivement entre elles; celles des substitutions de H qui laissent z_i, par exemple, immobile, formeront un groupe L de H, d'ordre $\mathfrak{l} = \frac{\mathfrak{H}}{q}$.

Par hypothèse, il existe une substitution g_i de G qui, opérée sur z_1, change z_1 en z_i; soit l_j une substitution quelconque de L : la substitution $g_i l_j g_i^{-1}$ laisse z_1 invariable, et par suite fait partie de K. Le groupe $g_i \mathrm{L} g_i^{-1}$, transformé de L par g_i^{-1} est donc contenu dans K, et il existe dans K un groupe $g_i \mathrm{L} g_i^{-1}$, d'ordre $\mathfrak{l} = \frac{\mathfrak{H}}{q}$, que la substitution g_i de G transforme en un groupe L de H.

Je dis que $g_i \mathrm{L} g_i^{-1}$ est maximum parmi les groupes de K qui jouissent de cette propriété par rapport à g_i, c'est-à-dire qu'il les contient tous. En effet, soit k une substitution de K que g_i transforme en une substitution $g_i^{-1} k g_i$ de H : cette dernière laissera z_i immobile et par suite fera partie de L; donc k fera partie de $g_i \mathrm{L} g_i^{-1}$.

En formant toutes les suites différentes analogues à (5), suites qui, ensemble, constituent la suite (3), désignant par N_q le nombre des suites (5)

différentes pour lesquelles q a la même valeur, et remarquant que deux suites différentes analogues à (5) n'ont aucune fonction commune, on a

$$\sum_{q} q\mathrm{N}_q = \frac{\mathcal{G}}{\mathfrak{K}},$$

c'est-à-dire la formule (2).

On peut rendre la formule (2) symétrique en $\mathcal{G}$ et $\mathfrak{K}$ en divisant les deux membres par $\mathcal{G}\mathfrak{K}$, et remarquant que L est maximum parmi les groupes de H que g_i^{-1} transforme en un groupe de K, et que son ordre est égal à celui de $g_i \mathrm{L} g_i^{-1}$. On obtient

$$(2\ bis)\quad \frac{\mathcal{G}}{\mathcal{G}\mathfrak{K}} = \frac{\mathrm{N}_1}{\mathcal{G}} + \frac{\mathrm{N}_2}{\left(\frac{\mathcal{G}}{2}\right)} + \ldots + \frac{\mathrm{N}_q}{\left(\frac{\mathcal{G}}{q}\right)} + \ldots = \frac{\mathrm{N}_1}{\mathcal{L}_1} + \frac{\mathrm{N}_2}{\mathcal{L}_2} + \ldots + \frac{\mathrm{N}_q}{\mathcal{L}_q} + \ldots .$$

C'est sous cette forme, à la notation près, que la formule a été donnée par M. Frobenius (1).

Remarque. — La condition nécessaire et suffisante pour que $\mathrm{N}_1 \neq 0$ est qu'il existe dans G une substitution transformant en H un groupe de K. Si donc $\mathcal{G}$ ne divise pas $\mathfrak{K}$, on aura $\mathrm{N}_1 = 0$. Au contraire, si H est contenu dans K, on aura toujours $\mathrm{N}_1 \neq 0$.

En particulier, quand $\mathrm{H} = \mathrm{K}$, $\mathrm{N}_1 \mathfrak{K}$ est l'ordre du groupe des substitutions de G qui sont permutables à K.

Corollaire I. — Si $\nu\mathfrak{K}$ est l'ordre du groupe des substitutions de G permutables à K, on aura

$$q\mathrm{N}_q \equiv 0 \pmod{\nu},$$

et G renfermera exactement $\frac{q\mathrm{N}_q}{\nu}$ transformés distincts de K ayant en commun avec H $\frac{\mathcal{G}}{q}$ substitutions.

Nous venons de voir que $g_i \mathrm{L} g_i^{-1}$ est maximum parmi les groupes de K que g_i transforme en un groupe L de H, c'est-à-dire que $g_i^{-1} \mathrm{K} g_i$ et H ont

(1) Bien que, dans la démonstration, interviennent des substitutions entre des lettres, on sait que ce théorème, comme d'autres de la théorie des substitutions, est applicable aux groupes plus généraux d'opérations tels que ceux considérés par exemple par M. Frobenius, un pareil groupe pouvant toujours se représenter par un groupe de substitutions transitif, dont l'ordre égale le degré, et qui lui est holoédriquement isomorphe.

en commun exactement les substitutions du groupe L. Réciproquement, si un transformé $g_i^{-1} K g_i$ de K par g_i a en commun avec H exactement les ξ substitutions d'un groupe L, la fonction z_i obtenue en effectuant g_i dans z_1 fait partie d'une suite de q fonctions analogues à (5), avec $q\xi = \beta$.

Dès lors, soit M le groupe des substitutions de G permutables à K, et $\mathfrak{M} = \nu\mathfrak{K}$;

$$1, m_2, \ldots, m_{\mathfrak{M}} \tag{6}$$

les substitutions de M. Les substitutions

$$g_i, m_2 g_i, \ldots, m_{\mathfrak{M}} g_i \tag{7}$$

sont telles que $g_i^{-1} K g_i = (m_\lambda g_i)^{-1} K (m_\lambda g_i)$, et sont différentes; par suite les fonctions analogues à z_i correspondantes font toutes partie de suites analogues à (5), pour lesquelles q a la même valeur.

Soit $g_{i'}$ une substitution de G différente des substitutions (7), la suite

$$g_{i'}, m_2 g_{i'}, \ldots, m_{\mathfrak{M}} g_{i'} \tag{8}$$

jouira des mêmes propriétés que la suite (7), et chacune de ses substitutions transformera K en un groupe $g_{i'}^{-1} K g_{i'} \neq g_i^{-1} K g_i$, sans quoi on verrait que $g_{i'}$, par exemple, doit faire partie de la suite (7).

En continuant de la sorte et n'opérant que sur des substitutions g_i, $g_{i'}$, $g_{i''}$, ..., pour lesquelles q a la même valeur, et telles que $g_{i''}$ par exemple ne fasse pas partie des suites (7) et (8), on répartit ces substitutions en un certain nombre de suites analogues à (7) et (8), renfermant chacune $\mathfrak{M} = \nu\mathfrak{K}$ substitutions. Ces suites n'ont deux à deux aucune substitution commune, car l'égalité $m_\lambda g_i = m_{\lambda'} g_{i'}$, par exemple, entraînerait $g_{i'} = m_{\lambda'}^{-1} m_\lambda g_i$ contrairement à l'hypothèse.

Le nombre A des substitutions de G, pour lesquelles q a la même valeur, est donc un multiple de $\nu\mathfrak{K}$.

D'autre part, le nombre des fonctions z_i correspondantes est $q\mathrm{N}_q$. Il y a, d'ailleurs, exactement $\mathfrak{K}$ substitutions de G qui changent z_1 en z_i par exemple, et, par suite, le nombre des substitutions de G différentes qui changent z_1 en une des fonctions z_i faisant partie des suites analogues à (5) pour lesquelles q a la valeur considérée est $\mathfrak{K} q \mathrm{N}_q$. Dès lors

$$\mathrm{A} = \mathfrak{K} q \mathrm{N}_q \equiv 0 \pmod{\nu\mathfrak{K}}$$

ou

$$q\mathrm{N}_q \equiv 0 \pmod{\nu}. \tag{9}$$

Le nombre des suites analogues à (7) et (8) est $\frac{\mathrm{A}}{\nu\mathfrak{K}} = \frac{q\mathrm{N}_q}{\nu}$; à chacune d'elles correspondra un transformé différent de K ayant en commun avec H exactement $\mathfrak{L} = \frac{\mathfrak{H}}{q}$ substitutions.

Corollaire II. — Quand $\mathrm{K} = \mathrm{H}$, on a

$$q\mathrm{N}_q \equiv 0 \pmod{\mathrm{N}_1}$$

et G renferme exactement $\frac{q\mathrm{N}_q}{\mathrm{N}_1}$ transformés distincts de K ayant en commun avec K $\frac{\mathfrak{K}}{q}$ substitutions.

Ce corollaire résulte de la remarque et du corollaire précédents.

Corollaire III. — Soit p^m la plus haute puissance d'un nombre premier p qui divise l'ordre $\mathfrak{G}$ d'un groupe G; un groupe H d'ordre p^α, avec $\alpha < m$, contenu dans G est toujours contenu dans un certain nombre d'autres groupes de G d'ordre p^α, avec $\alpha' > \alpha$, et en particulier dans un groupe de G d'ordre p^m.

Appliquons le théorème précédent, en faisant $\mathrm{H} = \mathrm{K}$, $\mathfrak{H} = p^\alpha$; d'après la formule (2)

$$\mathfrak{G} = p^\alpha(\mathrm{N}_1 + p\mathrm{N}_p + \ldots + p^\alpha \mathrm{N}_{p^\alpha}).$$

Par hypothèse, $\mathfrak{G} \equiv 0 \pmod{p^m}$, et, puisque $m > \alpha$,

$$\mathrm{N}_1 + p\mathrm{N}_p + \ldots + p^\alpha \mathrm{N}_{p^\alpha} \equiv \mathrm{N}_1 \equiv 0 \pmod{p}.$$

Or G renferme un groupe H'_1 d'ordre $p^\alpha \mathrm{N}_1$, formé des substitutions de G qui sont permutables à H; si $p^{\alpha'}$ est la plus haute puissance de p qui divise $p^\alpha \mathrm{N}_1$, on a $\alpha' > \alpha$, puisque $\mathrm{N}_1 \equiv 0 \pmod{p}$, et, d'après un théorème de M. Sylow, déjà cité [formule (1)], H'_1 contient un groupe H′ d'ordre $p^{\alpha'}$. Le groupe H′ contient d'ailleurs H, sans quoi le groupe dérivé de H et de H′ serait d'ordre $p^{\alpha'_1}$ avec $\alpha'_1 > \alpha'$, puisque H est permutable aux substitutions de H′; ce groupe dérivé serait alors contenu dans H'_1 dont l'ordre $p^\alpha \mathrm{N}_1$ serait divisible par $p^{\alpha'_1}$ contrairement à l'hypothèse.

Si maintenant $\alpha' < m$, on peut opérer sur H′ comme on l'a fait sur H; et ainsi de suite. On trouvera une suite de groupes d'ordres p^α, $p^{\alpha'}$, ...

croissants, et tels que chacun d'eux contienne les précédents; on finira par en trouver un d'ordre p^m parmi eux, puisque α, α', ... sont des nombres entiers croissants et $\leq m$, dont le nombre est limité.

THÉORÈME I. — *Soient* G *un groupe de substitutions,* p^m *la plus haute puissance du nombre premier* p *qui divise l'ordre* $\mathcal{G}$ *de* G. *On aura*

$$\mathcal{G} = p^m \nu (1 + n_1 p + \ldots + n_\alpha p^\alpha + \ldots + n_m p^m) \tag{10}$$

où $p^m \nu$ *est l'ordre du groupe des substitutions de* G *qui sont permutables à un groupe de* G *d'ordre* p^m.

La condition nécessaire et suffisante pour que $n_\alpha \neq 0$ *est qu'on puisse trouver dans* G *deux groupes d'ordre* p^m *ayant en commun exactement* $p^{m-\alpha}$ *substitutions. Il y a exactement* $n_\alpha p^\alpha$ *groupes d'ordre* p^m *ayant en commun avec un groupe d'ordre* p^m *exactement* $p^{m-\alpha}$ *substitutions.*

En effet, appliquons le théorème de M. Frobenius, en faisant H = K, $\mathcal{G} = p^m$; d'après la formule (2),

$$\mathcal{G} = p^m (\mathrm{N}_1 + p\mathrm{N}_p + \ldots + p^\alpha \mathrm{N}_{p^\alpha} + \ldots + p^m \mathrm{N}_{p^m}).$$

On sait qu'on a ici $\mathrm{N}_1 = \nu$; de plus, la formule (9) donne

$$p^\alpha \mathrm{N}_{p^\alpha} \equiv 0 \pmod{\nu}$$

et, puisque ν est premier à p, d'après un théorème de M. Sylow déjà cité [formule (1)], on peut poser

$$p^\alpha \mathrm{N}_{p^\alpha} = \nu . n_\alpha . p^\alpha,$$

n_α étant entier, en sorte que

$$\mathcal{G} = p^m \nu (1 + n_1 p + \ldots + n_\alpha p^\alpha + \ldots + n_m p^m). \tag{10}$$

Dans cette formule, la condition nécessaire et suffisante pour que $n_\alpha \neq 0$ est que N_{p^α} le soit, ou, d'après ce qu'on a vu aux corollaires I et II du théorème de M. Frobenius démontré précédemment, qu'il existe dans G, au moins un transformé de H par les substitutions de G ayant en commun avec H exactement $p^{m-\alpha}$ substitutions.

De plus, d'après un théorème de M. Sylow déjà cité [formule (1)], tous les groupes de G d'ordre p^m sont les transformés de H par les substitutions

de G. Les deux corollaires que nous venons d'utiliser montrent d'ailleurs qu'il existe exactement dans G $\frac{p^\alpha N_{p^\alpha}}{\nu} = n_\alpha p^\alpha$ transformés de H ayant chacun en commun, avec H, $p^{m-\alpha}$ substitutions. Donc G contiendra exactement $n_\alpha p^\alpha$ groupes d'ordre p^m ayant en commun avec H $p^{m-\alpha}$ substitutions et pas davantage.

Ce théorème donnera lieu, dans la suite, à un certain nombre d'applications.

THÉORÈME II. — *Soit* G *un groupe de substitutions de degré* N *et d'ordre* $\mathcal{G} = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$; $p_1, p_2, \dots, p_k$ *étant des nombres premiers différents; soient* $N - u_\lambda$, $N - u_{\lambda-1}$, ..., $N - u_1$, $N - u_0$ *les nombres différents qui expriment les degrés des divers groupes d'ordre* $p_1^{\alpha_1}$, $p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$ *contenus dans* G : *l'ordre* $\mathcal{G}$ *du groupe* G *divise le nombre*

$$\mathfrak{A} = (N - u_\lambda)(N - u_{\lambda-1}) \dots (N - u_1)(N - u_0).$$

D'après un théorème de M. Sylow, déjà employé, G contient un groupe H_i d'ordre $\mathcal{G}_i = p_i^{m_i}$; soient $(N - v_\mu)$, $(N - v_{\mu-1})$, ..., $(N - v_1)$, $(N - v_0)$ avec $v_\mu < v_{\mu-1} < \dots < v_1 < v_0$, les degrés des divers groupes d'ordre $p_i^{\alpha_i}$ contenus dans H_i (α_i pouvant prendre toutes les valeurs $\leq m_i$). Je dis que $p_i^{m_i}$ divise le nombre

$$\mathfrak{B}_i = (N - v_\mu)(N - v_{\mu-1}) \dots (N - v_1)(N - v_0).$$

En effet, quand $\mu = 0$, on voit facilement que cette propriété a lieu; admettons qu'elle soit vraie quand le produit $\mathfrak{B}_i$ ne renferme pas plus de μ facteurs, et montrons que la propriété a encore lieu quand $\mathfrak{B}_i$ renferme $\mu + 1$ facteurs.

Soit a_1 une lettre quelconque déplacée par H_i; ce groupe permute a_1 avec $p_i^{\alpha_i}$ des lettres qu'il déplace; il permutera de même une lettre b_1 différente des $p_i^{\alpha_i}$ précédentes avec $p_i^{\beta_i}$ lettres différentes de celles-ci, et ainsi de suite.

Soit α_i la plus petite des quantités $\alpha_i, \beta_i, \dots$; le degré de H_i étant, par hypothèse, $N - v_\mu$, on aura

$$p_i^{\alpha_i} + p_i^{\beta_i} + \dots = N - v_\mu \equiv 0 \pmod{p_i^{\alpha_i}}.$$

Désignons par J le groupe des substitutions de H_i qui laissent a_1 immobile : J sera de degré $< N - v_\mu$; la quantité qui joue à l'égard de J le même

rôle que $\mathfrak{v}_i$ à l'égard de H_i sera

$$\mathfrak{v}_i' = (N - c_\rho)(N - c_{\rho'})\ldots,$$

ne renfermera que des facteurs de $\mathfrak{v}_i$, puisque J est contenu dans H_i, et ne contiendra pas le facteur $(N - c_\mu)$. D'après l'hypothèse, l'ordre $\mathfrak{z}$ de J divisera $\mathfrak{v}_i'$. Or

$$\mathfrak{G}_i = p_i^{\alpha_i}.\mathfrak{z},$$

$p_i^{\alpha_i}$ divisant $N - c_\mu$ d'après ce qu'on a vu tout à l'heure. $\mathfrak{G}_i$ divisera donc $(N - c_\mu)\mathfrak{z}$, *a fortiori* $(N - c_\mu)\mathfrak{v}_i'$ et $\mathfrak{v}_i$.

Les divers groupes d'ordre $p_i^{m_i}$ contenus dans G étant d'ailleurs les transformés d'un d'entre eux par les substitutions de G sont tous semblables, et la quantité $\mathfrak{v}_i$ est la même pour tous.

Ceci posé, les k quantités $\mathfrak{v}_1$, $\mathfrak{v}_2$, ..., $\mathfrak{v}_k$ analogues à $\mathfrak{v}_i$ et correspondant respectivement aux groupes de G d'ordres $p_1^{m_1}$, $p_2^{m_2}$, ..., $p_k^{m_k}$ sont telles que

$$\mathfrak{v}_1 \equiv 0 \pmod{p_1^{m_1}}, \qquad \mathfrak{v}_2 \equiv 0 \pmod{p_2^{m_2}}, \qquad \ldots, \qquad \mathfrak{v}_k \equiv 0 \pmod{p_k^{m_k}}.$$

Le produit $\mathcal{G} = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$ divise donc le plus petit commun multiple des quantités $\mathfrak{v}_1, \mathfrak{v}_2, \ldots, \mathfrak{v}_k$, et *a fortiori* le nombre $\mathfrak{A}$, qui est évidemment multiple de ces k nombres.

Corollaire. — L'ordre $\mathcal{G}$ d'un groupe G de classe $N - u_0$ et de degré N divise le produit $\mathfrak{S} = N(N-1)\ldots(N-u_0)$.

En effet, d'après la définition de la classe (1), u_0 est la plus grande des quantités $u_\lambda, u_{\lambda-1}, \ldots, u_1, u_0$. Le nombre $\mathfrak{S}$ est donc un multiple de $\mathfrak{A}$, et, d'après le théorème précédent, $\mathcal{G}$ divise $\mathfrak{S}$.

On peut d'ailleurs établir ce corollaire directement :

Première démonstration. — Soient p un nombre premier qui divise $\mathcal{G}$; p^λ, p^μ, p^m les plus hautes puissances de p qui divisent respectivement $N(N-1)\ldots(N-u_0)$, $1.2\ldots(N-u_0-1)$, et $\mathcal{G}$; par suite, $p^{\lambda+\mu}$ la plus haute puissance de p qui divise $1.2\ldots N$. Il suffit évidemment de prouver que l'on a $m \leqq \lambda$.

D'après un théorème déjà employé, G contient un groupe K d'ordre $\mathfrak{K} = p^m$; le groupe symétrique F entre les N lettres de G contient de même un groupe L, d'ordre $\mathfrak{L} = p^{\lambda+\mu}$. D'après le corollaire III du théorème de

(1) M. Jordan a défini la classe d'un groupe le nombre minimum de lettres que déplace une substitution de ce groupe différente de l'unité.

M. Frobenius on peut choisir L de façon que K y soit contenu. De même, un groupe symétrique F′ entre $(N - u_0 - 1)$ des lettres de G contiendra un groupe K'_1, d'ordre $\mathfrak{K}'_1 = p^\mu$, lequel sera toujours contenu dans un groupe L′ de F, d'ordre $\mathfrak{L}' = p^{\lambda+\mu} = \mathfrak{L}$; on sait que L′ est un transformé de L par une substitution σ de F, en sorte que $\sigma L' \sigma^{-1} = L$, et, de même, $\sigma K'_1 \sigma^{-1} = K'$, K′ étant un groupe d'ordre $\mathfrak{K}' = p^\mu$, contenu dans L et de degré $N - u_0 - 1$. K′ n'aura donc en commun avec K, qui est de classe $\geqq N - u_0$, d'autre substitution que l'unité.

Soient maintenant

$$\begin{array}{llll} k_1 = 1, & k_2, & \ldots, & k_{p^m}, \\ k'_1 = 1, & k'_2, & \ldots, & k'_{p^\mu} \end{array}$$

les substitutions de K et de K′ respectivement. Les substitutions de la forme $k_j k'_{j'}$ sont toutes différentes, car $k_j k'_{j'} = k_l k'_{l'}$ entraîne $k_j^{-1} k_l = k'_{j'} k'^{-1}_{l'} = 1$, puisque K et K′ n'ont d'autre substitution commune que l'unité, et l'on ne peut avoir $k_j k'_{j'} = k_l k'_{l'}$ que si $k_j = k_l$, $k'_{j'} = k'_{l'}$, ou $j = l$, $j' = l'$.

Dès lors, les substitutions différentes de la forme $k_j k'_{j'}$ sont en nombre $\mathfrak{K}\mathfrak{K}' = p^{m+\mu}$; elles sont toutes contenues dans L, et, par suite, il faudra $p^{m+\mu} \leqq p^{\lambda+\mu}$ ou $m \leqq \lambda$ (1).

Deuxième démonstration. — Il suffit d'appliquer aux groupes F, F′, G, dont le premier contient les deux autres, le théorème de M. Frobenius, et d'établir que $\mathfrak{F}'\mathfrak{G}$ divise $\mathfrak{F}$, d'où l'on conclura que $\mathfrak{G}$ divise $\frac{\mathfrak{F}}{\mathfrak{F}'}$ ou $\mathfrak{S}$.

Nous allons montrer plus généralement que : *si deux groupes* F′ *et* G, *assujettis à la seule condition de n'avoir deux à deux d'autre substitution semblable que l'unité, sont contenus dans un même troisième* F, on a $\mathfrak{F} \equiv 0 \pmod{\mathfrak{F}'\mathfrak{G}}$.

En effet, d'après la formule (2),

$$\mathfrak{F} = \mathfrak{F}'(N_1 + 2N_2 + \ldots + qN_q + \ldots).$$

Ici q divise $\mathfrak{G}$, et l'on n'a $N_q \neq 0$ que s'il existe dans F′ un groupe d'ordre $\frac{\mathfrak{G}}{q}$ qu'une substitution de F transforme en un groupe de G; F′ et G ne renfermant d'autre substitution semblable que l'unité, on n'aura $N_q \neq 0$ que pour $\frac{\mathfrak{G}}{q} = 1$ ou $q = \mathfrak{G}$, ce qui donne bien

$$\mathfrak{F} = \mathfrak{F}'\mathfrak{G}.N_{\mathfrak{G}}.$$

(1) Comparez CAUCHY, *Exer. d'Anal. et de Phys. math.*, t. III, p. 248.

THÉORÈME III. — *Tout étant posé comme au théorème II (ou à son corollaire)* (1), *soient* $p_i^{\varphi_i}$ *et* $p_i^{\chi_i}$ *les plus hautes puissances du nombre premier* p_i *qui divisent respectivement* $\mathfrak{H}$ *et* $\frac{\mathfrak{H}}{N}$, u_λ *étant supposé égal à* o $\left(\text{qui divisent respectivement } \Theta \text{ et } \frac{\Theta}{N}\right)$. *Si* $m_i = \chi_i + \varepsilon_i$, *avec* $\varepsilon_i \geq$ o, G *permute une quelconque des lettres qu'il déplace avec* $\lambda_1 p_i^{\varepsilon_i}$ *lettres.*

Soit α une quelconque des lettres déplacées par G, τ le nombre des lettres que G substitue à α. On a $\mathcal{G} = \tau\mathcal{B}$, H étant le groupe des substitutions de G qui laissent α immobile.

Soit $p_i^{\psi_i}$ la plus haute puissance de p_i qui divise $\mathcal{B}$; on aura $\psi_i \leq \chi_i$, puisque H est de degré $< N$. Alors τ sera divisible par $p_i^{m_i - \psi_i} = p_i^{\varepsilon_i + \chi_i - \psi_i}$, et *a fortiori* par $p_i^{\varepsilon_i}$, ce qui permettra de poser

$$\tau = \lambda_1 p_i^{\varepsilon_i}.$$

Remarque. — En faisant varier i, et posant $\varepsilon_i =$ o quand $m_i < \chi_i$, on voit que τ sera divisible par $p_1^{\varepsilon_1}$, par $p_2^{\varepsilon_2}$, ..., par $p_k^{\varepsilon_k}$, c'est-à-dire que G permutera une quelconque des lettres qu'il déplace avec $\lambda' p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_k^{\varepsilon_k}$ lettres.

En particulier, soient $p_1, p_2, \dots, p_j$ les diviseurs premiers différents de N. On a évidemment

$$N = p_1^{\varphi_1 - \chi_1} p_2^{\varphi_2 - \chi_2} \dots p_j^{\varphi_j - \chi_j},$$

et si l'on a

$$m_1 = \varphi_1, \qquad m_2 = \varphi_2, \qquad \dots, \qquad m_j = \varphi_j,$$

on en conclura

$$\varepsilon_1 = \varphi_1 - \chi_1, \qquad \varepsilon_2 = \varphi_2 - \chi_2, \qquad \dots, \qquad \varepsilon_j = \varphi_j - \chi_j,$$

et $\lambda' p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_k^{\varepsilon_k}$ sera divisible par N, c'est-à-dire égal à N, en sorte que G sera transitif.

Corollaire. — $p_1, p_2, \dots, p_j$ étant les diviseurs premiers différents de N, si $p_1^{m_1}, p_2^{m_2}, \dots, p_j^{m_j}$ sont à la fois les plus hautes puissances des nombres premiers $p_1, p_2, \dots, p_j$ qui divisent $\mathcal{G}$ et Θ, le groupe G est transitif.

---

(1) Nous indiquons entre parenthèses les modifications à faire subir à l'énoncé du théorème quand on veut appliquer non le théorème II, mais son corollaire : les démonstrations sont d'ailleurs analogues.

Dans ce cas, si une propriété semblable a lieu pour le groupe H des substitutions de G qui laissent une lettre déterminée immobile, on en conclura que G est deux fois transitif, et ainsi de suite.

Les deux théorèmes précédents et leurs corollaires sont particulièrement susceptibles d'applications quand on veut étudier les propriétés d'un groupe G dont on se donne le degré, la classe et l'ordre; par exemple, quand on voudra étudier les groupes primitifs G d'ordre donné $\mathcal{G}$, de degré N et de classe $N - u_0$ (1).

II.

THÉORÈME I. — *Soient* G *un groupe de substitutions d'ordre*

$$\mathcal{G} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

$p_1, p_2, \dots, p_k$ *étant des nombres premiers différents,* H *un groupe contenu dans* G, *d'ordre* $\mathcal{S} = p_1^{\beta_1} p_2^{\beta_2} \dots p_i^{\beta_i}$ *avec* $i \leq k$.

Si tous les transformés de H *par les substitutions de* G *ont en commun un même groupe* L *d'ordre* $\mathcal{L} = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_j^{\gamma_j} > 1$, *les substitutions de* G *sont permutables à un groupe* M, *commun à tous les transformés de* H *par les substitutions de* G, *et qui contient* L.

En effet, soient

$$\text{(11)} \qquad \mathrm{H}, \quad \mathrm{H}_1, \quad \dots, \quad \mathrm{H}_\lambda$$

les divers transformés de H par les substitutions de G. Tout groupe H_ρ de la suite (11) est transformé par une substitution quelconque de G en un groupe H_σ de la même suite. Considérons un groupe I, contenant L, et formé de l'ensemble des substitutions communes à tous les groupes (11). Pour établir le théorème, il suffira de montrer que I est permutable aux substitutions de G, car on pourra prendre alors M = I.

Supposons que I ne soit pas permutable aux substitutions de G. On pourra trouver dans G une substitution g telle que $\mathrm{I}' = g^{-1}\mathrm{I}g$ soit différent de I. Le groupe I′ est commun à tous les groupes de la suite

$$\text{(12)} \qquad g^{-1}\mathrm{H}g, \quad g^{-1}\mathrm{H}_1 g, \quad \dots, \quad g^{-1}\mathrm{H}_\lambda g,$$

---

(1) *Voir* notre *Thèse de Doctorat,* 2e Partie, p. 49-104, au sujet des groupes transitifs de degré N et de classe N — 1, N — 2 ou N — 3.

puisque I est commun à tous les groupes (11). Mais la suite (11) contenant le transformé H_σ d'un quelconque H_ρ des groupes qu'elle renferme par une substitution quelconque de G, les groupes (12) coïncident, à l'ordre près, avec les groupes (11), en sorte que I′ est commun à tous les groupes (11). On en conclurait que le groupe (I, I′), dérivé de I et de I′, contient I, est $> \mathrm{I}$, et est commun à tous les groupes (11), en sorte que I ne contiendrait pas toutes les substitutions communes à tous les groupes (11), contrairement à l'hypothèse faite sur I.

Donc I est permutable aux substitutions de G.

THÉORÈME II. — *Tout étant posé comme à l'énoncé du théorème précédent, et* M *contenant* L, *et étant permutable aux substitutions de* G *et commun à tous les transformés de* H *par les substitutions de* G, *si* L *est permutable aux substitutions de* M, *les substitutions de* G *sont permutables à un groupe* M′, *commun à tous les transformés de* H *par les substitutions de* G, *qui contient* L, *et qui est d'ordre* $\mathfrak{M}' = p_1^{\delta_1} p_2^{\delta_2} \dots p_j^{\delta_j}$ *et contenu dans* M.

En effet, soit J un groupe d'ordre $\mathfrak{J} = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_j^{\varepsilon_j}$ contenu dans M, contenant L, permutable aux substitutions de M, et maximum parmi les groupes de M qui jouissent des mêmes propriétés et qui, en particulier, n'ont pas leur ordre divisible par d'autres nombres premiers que les diviseurs premiers $p_1, p_2, \dots, p_j$ de $\mathfrak{L}$. Pour établir le théorème, il suffira de montrer que J est permutable aux substitutions de G, car on pourra prendre alors $\mathrm{M}' = \mathrm{J}$.

Supposons que J ne soit pas permutable aux substitutions de G : on pourra trouver dans G une substitution g telle que $\mathrm{J}' = g^{-1}\mathrm{J}g$ soit différent de J. Le groupe J′ est contenu dans $g^{-1}\mathrm{M}g = \mathrm{M}$ et permutable à ses substitutions, en sorte que le groupe (J, J′), dérivé de J et de J′, est contenu dans M, comme J et J′, permutable aux substitutions de M, et contient L. Le groupe J étant permutable aux substitutions de M l'est à celles de J′; on voit donc facilement que J et J′ sont échangeables (1), et que l'ordre de (J, J′) est $\frac{\mathfrak{J}\mathfrak{J}'}{\mathfrak{R}} = \frac{\mathfrak{J}^2}{\mathfrak{R}} > \mathfrak{J}$, $\mathfrak{R}$ étant l'ordre du groupe R commun à J et à J′ (2). Ainsi, (J, J′) jouirait des mêmes propriétés que J, contiendrait J, et serait

(1) SERRET, *Algèbre supérieure*, t. II, p. 283.
(2) *Voir* notre *Thèse de Doctorat*, p. 104.

$> J$, contrairement à l'hypothèse faite sur J $\left(\frac{\mathfrak{d}^2}{\mathfrak{R}}\right.$ n'ayant d'autres facteurs premiers que ceux de $\mathfrak{d}\Big)$.

Donc J est permutable aux substitutions de G.

THÉORÈME III. — *Tout étant posé comme à l'énoncé du théorème I, et* M′ *étant un groupe commun aux transformés de* H *par les substitutions de* G, *contenant* L, *étant permutable aux substitutions de* G *et son ordre n'étant divisible par aucun facteur premier ne divisant pas* $\mathfrak{L}$, *si* L *est formé de substitutions échangeables à celles de* M′, *les substitutions de* G *sont permutables à un groupe* M″ *contenu dans* M′, *contenant* L, *et formé de substitutions échangeables.*

Nous supposons que M′ est permutable aux substitutions de G. De plus, L étant contenu dans M′ est formé de substitutions échangeables.

Nous considérons un groupe J_1, d'ordre $\mathfrak{d}_1 = p_1^{\eta_1} p_2^{\eta_2} \dots p_j^{\eta_j}$ contenant L, contenu dans M′, formé de substitutions échangeables à celles de M′, et maximum parmi les groupes qui jouissent des mêmes propriétés. Nous remarquerons que J_1 est formé de substitutions échangeables, et que, pour établir le théorème, il suffit de montrer que J_1 est permutable aux substitutions de G, car on pourra prendre alors $M'' = J_1$.

En raisonnant comme au théorème précédent, on voit que, si J_1 n'était pas permutable aux substitutions de G, on serait conduit à une contradiction.

Remarque I. — Soit L_1 un groupe quelconque contenu dans L; on peut tenter d'opérer sur L_1 comme on l'a fait sur L.

Dans le cas du théorème I, L_1 jouit des mêmes propriétés que L, et, par suite, ce théorème lui est applicable.

Dans le cas du théorème II, si L_1 est permutable aux substitutions de M, ou d'un groupe analogue qui le contienne, on peut lui appliquer le théorème II.

Dans le cas du théorème III, L_1 est permutable aux substitutions de M′; d'après le théorème II, on pourra trouver M'_1 contenant L_1, contenu dans M′, permutable aux substitutions de G et dont l'ordre n'ait d'autres diviseurs premiers que ceux de L_1. Mais les substitutions de L_1 sont échangeables à celles de M′, par suite à celles de M'_1; on pourra donc appliquer L_1 et à M'_1 le théorème III, et trouver un groupe M''_1 permutable aux sub-

stitutions de G, contenant L_1, contenu dans M'_1 et formé de substitutions échangeables. En particulier, si $\mathfrak{L}_1 = p_1^{\gamma_1}$, on aura $\mathfrak{M}''_1 = p_1^{\theta_1}$.

Remarque II. — Dans la démonstration du théorème précédent, on peut imposer à J_1, par suite à M'', certaines conditions plus restrictives, pourvu au moins que ces conditions soient remplies par L. Ainsi on pourra supposer que J_1, en outre des propriétés qu'on lui a attribuées, soit encore tel qu'il ne contienne que des substitutions de mêmes ordres que celles de L, à condition que J_1 soit toujours maximum parmi les groupes de M' jouissant des mêmes propriétés.

En appliquant le théorème III ainsi modifié au groupe L_1 considéré dans la remarque précédente, on voit que le groupe M''_1 ne contiendra que des substitutions de mêmes ordres que celles de L_1. Si en particulier L_1 ne contient que des substitutions d'ordre p_1, il en sera de même de M''_1. On peut donc énoncer le théorème suivant :

THÉORÈME IV. — *Tout étant posé comme à l'énoncé du théorème précédent et p_1 étant un diviseur premier quelconque de l'ordre $\mathfrak{L}$ de* L, *on aura dans* M' *un groupe* M''', *d'ordre $\mathfrak{M}''' = p_1^{\theta_1}$, formé de substitutions d'ordre p_1 échangeables, et permutable aux substitutions de* G.

Les théorèmes précédents donnent lieu à un certain nombre de corollaires.

Corollaire I. — Quand un groupe G est primitif, les divers transformés d'un groupe H de G par les substitutions de G auront en commun un groupe transitif, ou n'auront d'autre substitution commune que l'unité.

En effet, si ces divers transformés de H ont en commun quelque substitution autre que l'unité, ils ont en commun un groupe M permutable aux substitutions de G, d'après le théorème I, et M doit être transitif, puisque G est primitif (1).

Corollaire II. — Quand un groupe G est primitif, si le groupe M_1 des substitutions communes aux divers transformés d'un groupe H de G par les substitutions de G contient une substitution échangeable à celles de M_1, et d'ordre premier p, G contient un groupe d'ordre p^θ formé de toutes les substitutions de la forme

$$(13) \qquad |x_1, x_2, \ldots, x_\theta, \quad x_1 + \lambda_1, x_2 + \lambda_2, \ldots, x_\theta + \lambda_\theta| \qquad (\mathrm{mod}\, p)$$

(1) JORDAN, *Traité des substitutions*, p. 41.

permutable à ses substitutions, $\lambda_1, \lambda_2, \ldots, \lambda_\theta$ pouvant prendre chacun toutes les valeurs $0, 1, 2, \ldots, p-1 \pmod p$.

Par suite G est linéaire et de degré p^θ.

En effet, désignant par L_1 le groupe formé des puissances de la substitution de M_1 échangeable aux substitutions de M_1, on peut appliquer à L_1 les théorèmes I et II, puis à L_1 et au groupe M_1' obtenu, analogue à M', le théorème III, les remarques précédentes et le théorème IV. On voit ainsi que les substitutions de G sont permutables à un groupe M''', d'ordre $\mathfrak{M}''' = p^\theta$, formé de substitutions d'ordre p échangeables. Enfin, d'après le corollaire précédent, M''' est transitif.

Ceci posé, si une substitution de M''' différente de l'unité laissait quelque lettre immobile, en la transformant par les substitutions du groupe transitif M''' qui lui sont échangeables, on voit qu'elle doit laisser toutes les lettres immobiles, c'est-à-dire se réduire à l'unité. Donc M''' est transitif entre les lettres de G et d'ordre égal à son degré; le degré de G est donc p^θ.

Il ne reste plus qu'à faire voir que les substitutions de M''' sont de la forme indiquée. Or M. Jordan a montré (1) qu'un groupe transitif dont l'ordre et le degré sont égaux à p^θ et formé de substitutions d'ordre p échangeables était constitué, en choisissant convenablement la notation, de l'ensemble des substitutions de la forme indiquée (13); il en résulte immédiatement que G est un groupe linéaire.

Corollaire III. — Si p^m est la plus haute puissance du nombre premier p qui divise l'ordre $\mathcal{G}$ d'un groupe G, et si tous les groupes d'ordre p^m de G ont en commun un groupe L d'ordre $\mathcal{L} = p^\gamma > 1$, les substitutions de G sont permutables à un groupe M''' d'ordre $p^\theta > 1$, commun à tous les groupes de G d'ordre p^m, et qui est formé de substitutions échangeables et d'ordre p.

Si G est de plus primitif, il est linéaire et de degré p^θ.

En effet, d'après un théorème de M. Sylow déjà employé [formule (1)], les divers groupes d'ordre p^m de G sont les transformés d'un d'entre eux H par les substitutions de G. Ces groupes ont d'ailleurs en commun le groupe L d'ordre > 1, et, d'après le théorème I et sa démonstration, le groupe M, formé de l'ensemble des substitutions communes aux transformés de H par les substitutions de G, est permutable aux substitutions de G; le groupe M

(1) *Traité des substitutions*, p. 291.

est d'ailleurs d'ordre $\mathfrak{m} = p^n$, puisqu'il est contenu dans H d'ordre $\beta = p^m$.

Mais M. Sylow a montré (1) qu'un groupe M d'ordre p^n, p étant premier, renfermait toujours une substitution d'ordre p échangeable à toutes ses substitutions. On peut immédiatement appliquer le corollaire précédent, ce qui démontre la propriété, quand G est primitif.

Quand G n'est pas primitif, soit L_1 le groupe formé des puissances de la substitution échangeables à celles de M; on remarquera que ε_1 et $\mathfrak{m}$ ont le même diviseur premier unique p, et, par suite, qu'on peut appliquer à M et L_1 les théorèmes III et IV.

THÉORÈME V. — *Soient* G *et* G′ *deux groupes de substitutions; si* G *est permutable aux substitutions de* G′, *et* G′ *à celles de* G; *si de plus* H *est le groupe des substitutions communes à* G *et* G′, *et si* S *et* S′ *sont deux substitutions quelconques de* G *et* G′ *respectivement, on aura*

$$SS' = S'Sh,$$

h étant une substitution de H.

Bien que ce théorème soit contenu plus ou moins implicitement dans des démonstrations connues (2), nous croyons devoir l'énoncer, parce qu'il permet d'alléger certains raisonnements.

Considérons $S^{-1}S'^{-1}SS'$; par hypothèse, $S^{-1}S'S = S'_1$ fait partie de G′, et $S'^{-1}SS' = S_1$ fait partie de G. Donc

$$S^{-1}S'^{-1}SS' = S'^{-1}_1 S' = S^{-1}S_1$$

fait partie de G′ et de G, par suite de H, et l'on peut écrire

$$S^{-1}S'^{-1}SS' = h,$$

h faisant partie de H, ce qui donne bien

$$SS' = S'Sh.$$

Corollaire. — Si G et G′ n'ont d'autre substitution commune que l'unité, on aura $S'S = SS'$, c'est-à-dire que les substitutions de G seront échangeables à celles de G′ et réciproquement.

---

(1) Mémoire déjà cité, p. 587.

(2) JORDAN, *Traité des substitutions*, t. IV, Chap. I.

THÉORÈME VI. — *Soit p^m la plus haute puissance du nombre premier p qui divise l'ordre $\mathcal{G}$ d'un groupe* G, $\mathcal{G} = p^m \nu$ *l'ordre du groupe* H *des substitutions de* G *permutables à un groupe* L *d'ordre* $\mathcal{L} = p^m$ *contenu dans* G. *Un groupe* J, *dérivé de* H *et de son transformé* $g^{-1}\mathrm{H}g$ *par une substitution* g *de* G *contient* g, *et, par suite, l'ordre* $\mathcal{J}$ *de* J *est divisible par l'ordre de* g.

En effet, J contient le groupe $\mathrm{J}' = (\mathrm{H}, g^{-1}\mathrm{L}g)$ dérivé de H et du transformé $g^{-1}\mathrm{L}g$ de L par g, puisque H contient L et que $g^{-1}\mathrm{H}g$ contient $g^{-1}\mathrm{L}g$. Il nous suffira donc de montrer que J′ contient g.

Soient

$$1 = h_1, \quad h_2, \quad \ldots, \quad h_{\mathcal{J}} \tag{14}$$

les substitutions de H. Les substitutions de G qui transforment L en $g^{-1}\mathrm{L}g$ sont les substitutions

$$g = h_1 g, \qquad h_2 g, \qquad \ldots, \qquad h_{\mathcal{J}} g. \tag{15}$$

Le groupe J′ est contenu dans G; p^m est la plus haute puissance du nombre premier p qui divise $\mathcal{J}'$: donc, d'après un théorème de M. Sylow déjà employé [formule (1)], J′ contient une substitution σ qui transforme L en $g^{-1}\mathrm{L}g$, puisque L d'ordre p^m et $g^{-1}\mathrm{L}g$ sont contenus dans J′; mais ces deux groupes sont aussi contenus dans G, et, par suite, σ sera une des substitutions (15); J′ contiendra une substitution de la forme $h_i g$, et, comme il contient H, il contiendra toutes les substitutions de la forme $h_j^{-1} h_i g$, c'est-à-dire les substitutions (15) et en particulier g.

THÉORÈME VII. — *Soient* G *un groupe transitif,* H_α *le groupe des substitutions de* G *qui laissent une lettre* α *immobile,* H'_α *le groupe dérivé de toutes les substitutions (ou de tous les groupes) de* H_α *qui sont semblables à une ou plusieurs des substitutions (à un ou plusieurs des groupes) de* H_α, *qu'on choisira arbitrairement.*

Si N *est le degré de* G, *d celui de* H'_α, G *admet une répartition de ses lettres en systèmes de non-primitivité* $\mathrm{N} - d$ *à* $\mathrm{N} - d$, *et contient un groupe d'ordre* $(\mathrm{N} - d)\mathcal{G}_\alpha$, *contenant* H_α, *en sorte que* G *n'est pas primitif si* $\mathrm{N} - d > 1$.

En effet, d'après sa définition, H'_α est permutable aux substitutions de H_α.

Soit β une lettre de G différente de α; on peut toujours trouver dans G, qui est transitif, une substitution de la forme

$$\sigma = (\alpha\beta\ldots)\ldots. \tag{16}$$

Le transformé $\sigma^{-1}H_\alpha\sigma = H_\beta$ de H_α par σ contient $\sigma^{-1}H'_\alpha\sigma = H'_\beta$ et H'_β est dérivé de l'ensemble des substitutions (ou groupes) de H_β semblables aux substitutions choisies (ou aux groupes choisis). Dès lors, une autre substitution σ' de G, de la forme (16), donnera

$$\sigma'^{-1}H_\alpha\sigma' = H_\beta = \sigma^{-1}H_\alpha\sigma,$$
$$\sigma'^{-1}H'_\alpha\sigma' = H'_\beta = \sigma^{-1}H'_\alpha\sigma.$$

Donc aux N transformés

$$H_\alpha,\quad H_\beta,\quad \ldots \tag{17}$$

de H_α par les substitutions de G correspondront les N transformés

$$H'_\alpha,\quad H'_\beta,\quad \ldots \tag{18}$$

de H'_α par les substitutions de G.

H_α est de degré d; il laisse, par suite, $N - d$ lettres immobiles, et est dès lors contenu dans $N - d$ et $N - d$ seulement des groupes (17). D'ailleurs, si H'_α est contenu dans H_β par exemple, il devra, d'après sa définition, être identique à H'_β, et réciproquement. H'_α étant contenu dans $N - d$ des groupes (17) exactement, sera identique à $N - d$ des groupes (18) exactement. Ces derniers étant les transformés d'un d'entre eux par les substitutions de G seront identiques $N - d$ à $N - d$ exactement, et le nombre des groupes distincts de la suite (18) sera $\frac{N}{N-d}$.

Mais, si $\mathcal{G}_\alpha\nu$ est l'ordre du groupe des substitutions de G permutables à H'_α par exemple, le nombre des transformés distincts de H'_α par les substitutions de G est

$$\frac{G}{\mathcal{G}_\alpha\nu} = \frac{N}{\nu}.$$

Par suite

$$\frac{N}{\nu} = \frac{N}{N-d} \qquad \text{et} \qquad \nu = N - d.$$

G contient donc un groupe d'ordre $\mathcal{G}_\alpha(N - d)$ contenant H_α; d'après un

théorème de M. Walther Dyck (1), G admet une répartition de ses lettres en systèmes de non-primitivité $N - d$ à $N - d$, et G ne peut être primitif que si $N - d = 1$.

Remarque. — Bien que ce théorème ait été établi par M. Jordan (2), par des procédés analogues, nous avons cru devoir le donner : il contient, en effet, comme cas particuliers, d'autres théorèmes.

Si l'on choisit, par exemple, $H'_\alpha = H_\alpha$, on retrouve un théorème mentionné par M. Rudio (3). Si l'on suppose *a priori* G primitif, on retrouve un théorème de M. Netto (4).

Corollaire. — Si p est un nombre premier qui divise l'ordre $\mathcal{G}$ de G, et si N est le degré de G, le groupe H' dérivé de toutes les substitutions d'ordre p contenues dans G, semblables, et qui laissent une lettre donnée immobile, ne peut être de degré $N - d$ que si G admet une répartition de ses lettres en systèmes de non-primitivité $N - d$ à $N - d$.

G ne peut être primitif que si le groupe H' est de degré $N - 1$.

THÉORÈME VIII. — *Soient* G *un groupe quelconque de degré* N, p^m *la plus haute puissance du nombre premier* p *qui divise* $\mathcal{G}$, A *un groupe d'ordre* p^m *contenu dans* G *et de degré* $N - d (d > 0)$; $\beta_1, \beta_2, \ldots, \beta_d$ *les lettres de* G *que* A *ne déplace pas,* H_{β_1} *le groupe des substitutions de* G *qui laissent* β_1 *immobile,* ν' *l'ordre du groupe des substitutions de* H_{β_1} *permutables à* A, ν'' *le nombre des lettres* $\beta_i (i \leq d)$ *que* G *substitue à* β_1, ν *l'ordre du groupe des substitutions de* G *permutables à* A; *on a l'égalité*

$$\nu = \nu' \nu''.$$

La démonstration repose essentiellement sur un théorème de M. Sylow déjà employé [formule (1)], d'après lequel tout groupe d'ordre p^m contenu dans G est un transformé de A par une substitution de G.

Soit $\sigma = (\beta_1 \beta_i \ldots) \ldots$ une substitution de G qui remplace β_1 par une des d lettres

$$\beta_1, \quad \beta_2, \quad \ldots, \quad \beta_d. \tag{19}$$

(1) *Gruppentheoretische Studien* (*Math. Annalen,* t. XXII, p. 94). *Voir* aussi notre *Thèse de Doctorat,* p. 13.

(2) *Traité des substitutions,* p. 283-285.

(3) *Ueber primitive Gruppen* (*Journal für Mathematik,* t. CII, p. 1-8).

(4) *Untersuchungen aus der Theorie der Substitutionen Gruppen* (*Journal für Mathematik,* t. CIII, p. 333).

Le transformé $\sigma^{-1}H_{\beta_1}\sigma$ de H_{β_1} par σ est formé de l'ensemble des substitutions de G qui laissent β_i immobile, et, par suite, coïncide avec H_{β_i} et H_{β_i} contient A.

Au contraire, une substitution τ qui remplace β_1 par une lettre γ qui ne fait pas partie de (19) transforme H_{β_1} en H_γ, qui laisse γ immobile, et, par suite, ne contient pas A.

Dès lors, si G substitue $\varkappa$ lettres à β_1, dont ν'' lettres β_i appartenant à (19), parmi les $\varkappa$ groupes

$$(20) \qquad H_{\beta_1}, \quad \ldots, \quad H_{\beta_i}, \quad \ldots, \quad H_\gamma, \quad \ldots,$$

il y en a exactement ν'' qui contiennent A.

Supposons que parmi les groupes (20) il y en ait λ identiques à H_{β_1}. Les $\varkappa$ transformés (20) de H_{β_1} par les substitutions de G sont identiques λ à λ; il n'y en a que μ distincts si $\varkappa = \lambda\mu$, et dès lors $\mathcal{G} = \varkappa\mathcal{G}_{\beta_1} = \lambda\mu\mathcal{G}_{\beta_1}$.

Deux des groupes (20) ne peuvent être identiques que si tous deux contiennent A ou si aucun des deux ne le contient. Les ν'' groupes (20) qui contiennent A sont donc identiques λ à λ, et il y a exactement $\frac{\nu''}{\lambda}$ transformés distincts de H_{β_1} par G qui contiennent A.

Les groupes (20) étant transformés les uns dans les autres par les substitutions de G, tout transformé de A par G est de même contenu dans $\frac{\nu''}{\lambda}$ transformés distincts de H_{β_1} par G exactement.

D'autre part, H_{β_1} contient exactement $\frac{\mathcal{G}_{\beta_1}}{\nu'\mathcal{A}}$ transformés distincts de A par les substitutions de H_{β_1}; tout autre transformé de A distinct des précédents par une substitution de G ne peut faire partie de H_{β_1}, car tous les groupes semblables à A contenus dans H_{β_1} sont les transformés de A par les substitutions de H_{β_1}, puisque p^m est la plus haute puissance du nombre premier p qui divise $\mathcal{G}_{\beta_1}$, à cause de l'hypothèse $d > 0$.

Il en sera de même pour chacun des transformés distincts de H_{β_1} par G, en nombre μ. Le nombre des transformés distincts de A par les substitutions de G sera alors $\frac{\mu\mathcal{G}_{\beta_1}}{\rho\nu'\mathcal{A}}$, ρ désignant le nombre des transformés distincts de H_{β_1} par G qui contiennent simultanément, soit le groupe A, soit un de ses transformés par G, ce nombre ρ étant évidemment le même pour tous.

Mais le nombre des transformés distincts de A par les substitutions de G

est aussi $\frac{G}{\nu\mathfrak{H}}$. On en conclut

$$\frac{G}{\nu\mathfrak{H}} = \frac{\mu_\alpha\beta_{\alpha_1}}{\rho\nu'\mathfrak{H}} = \frac{G}{\rho\lambda\nu'\mathfrak{H}} \qquad \text{ou} \qquad \nu = \rho\lambda\nu'.$$

On a vu que $\rho = \frac{\nu''}{\lambda}$; on a donc bien $\nu = \nu'\nu''$.

Corollaire. — Si N est le degré de G, $N - d$ le degré d'un groupe A d'ordre p^m contenu dans G, et si $d > 0$, dans la formule (1) de M. Sylow, ν ne peut être égal à l'unité que si chacune des lettres laissées immobiles par A est permutée par G avec des lettres déplacées par A exclusivement.

Si G est transitif, ν ne peut être égal à l'unité que si $d = 1$; sinon ν est un multiple de d.

Ce corollaire est applicable pour toute valeur de p qui ne divise pas N, car on voit facilement que A ne peut être de degré N, que si N est divisible par p.

(*A suivre.*)