JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

CAMILLE JORDAN

Sur les groupes d'ordre $p^m q^2$

Journal de mathématiques pures et appliquées 5e série, tome 4 (1898), p. 21-26.

<http://www.numdam.org/item?id=JMPA_1898_5_4__21_0>

Sur les groupes d'ordre $p^m q^2$;

PAR M. CAMILLE JORDAN.

M. Sylow a démontré qu'un groupe d'ordre p^m (p premier, $m > 1$) est nécessairement composé.

M. Frobenius a étendu cette proposition aux groupes d'ordre $p^m q$ (q premier et différent de p).

Nous allons montrer qu'elle subsiste encore pour les groupes d'ordre $p^m q^2$.

1. Rappelons d'abord quelques propositions fondamentales, dues à M. Sylow et qui nous serviront de point de départ :

1° Un groupe G, dont l'ordre est divisible par p^m (sans l'être par p^{m+1}), contient des sous-groupes H, H', ... d'ordre p^m.

2° Ces groupes sont les transformés d'un seul d'entre eux par les diverses substitutions de G.

3° Tout sous-groupe d'ordre p^α ($\alpha \leqq m$) contenu dans G est contenu dans l'un au moins des groupes H, H', ...; il peut être commun à plusieurs d'entre eux.

4° Si p^α est l'ordre maximum des sous-groupes communs aux groupes H, H', ..., considérés deux à deux, le nombre b des groupes H, H', ... sera congru à 1 suivant le module $p^{m-\alpha}$.

5° Si $p^m a$ est l'ordre du groupe formé par celles des substitutions de G qui sont permutables à H, l'ordre de G sera égal à $p^m ab$.

M. Sylow établit ensuite qu'un groupe H d'ordre p^m est composé en montrant qu'il contient nécessairement des substitutions échangeables à toutes celles de H.

On pourrait arriver au même résultat en se fondant sur le lemme suivant, qui nous sera utile :

2. Lemme. — *Si un groupe* H *d'ordre p^m contient un sous-groupe* I *d'ordre p^α, les substitutions de* H *permutables à* I *formeront un groupe d'ordre p^β, où $\beta > \alpha$.*

En effet, si β était égal à α, les transformés I, I', ... de I par les substitutions de H seraient en nombre $p^{m-\alpha}$ et chacun d'eux jouirait comme H de la propriété de n'être permutable qu'à ses propres substitutions.

Énumérons, d'autre part, les groupes I, I', ... en associant dans une même classe ceux que les substitutions de I transforment les uns dans les autres. Le groupe I, constamment transformé en lui-même, restera isolé. Tout autre groupe I' donnera $p^{\alpha-\alpha'}$ transformés, si $p^{\alpha'}$ est l'ordre du sous-groupe formé par les substitutions communes à I et à I' (car ce sont les seules, par hypothèse, qui soient permutables à I'); α' étant $< \alpha$, le nombre des groupes contenus dans la classe de I' serait un multiple de p; de même pour chacune des autres classes. On aurait donc la relation impossible

$$p^{m-\alpha} \equiv 1 \pmod p.$$

3. Théorème. — *Un groupe* G, *d'ordre $p^m q^2$, est composé.*

Il contient, en effet, des sous-groupes d'ordre p^m, en nombre 1, q ou q^2.

S'il n'en contient qu'un seul, H, il sera invariant et G sera composé.

4. S'il en contient q, $H_1, \ldots, H_q$, les substitutions de G les permuteront les uns dans les autres. Ces déplacements formeront un groupe de degré q et isomorphe à G.

Mais tout groupe G (d'ordre $p^m q^2$) qui admet un isomorphe Γ dont le degré d soit $< 2q$ est composé. Car l'ordre de Γ divisant $d!$ ne pourra être divisible par q^2. L'isomorphisme sera donc mériédrique, et G contiendra un sous-groupe invariant, formé par celles de ses substitutions qui correspondent à la substitution 1 du groupe Γ.

5. Admettons enfin que G contienne q^2 sous-groupes H, H', ..., d'ordre p^m.

Si ces groupes, considérés deux à deux, n'ont d'autre substitution commune que l'unité, ils contiendront en tout $q^2(p^m - 1)$ substitutions dont l'ordre est une puissance de p; elles seront distinctes par hypothèse; donc G contiendra exactement q^2 substitutions dont l'ordre soit premier à p. Mais il contient au moins un sous-groupe g d'ordre q^2. Celui-ci sera évidemment formé des q^2 substitutions en question. Il sera donc unique de son espèce. Il sera donc invariant et G sera composé.

6. Admettons au contraire que parmi les groupes H, H', ... il en est qui aient des substitutions communes autres que l'unité. Soit I un sous-groupe d'ordre maximum p^α parmi ceux qui sont contenus à la fois dans plusieurs groupes de la suite H, H', ...; et soient $H_1, H_2, \ldots, H_l$ ceux des groupes de cette suite qui contiennent I.

Soient respectivement

$$K_1, \quad K_2, \quad \ldots, \quad K_l, \quad \Gamma$$

les groupes formés par celles des substitutions des groupes

$$H_1, \quad H_2, \quad \ldots, \quad H_l, \quad G,$$

qui sont permutables aux substitutions de I; soient enfin

$$p^{\beta_1}, \quad p^{\beta_2}, \quad \ldots, \quad p^\beta q^\lambda$$

les ordres de ces groupes.

Les groupes $K_1, K_2, \ldots, K_l$ seront tous différents, car leur ordre est $> p^\alpha$ (2). Si deux d'entre eux, K_1 et K_2 étaient identiques, H_1 et H_2 auraient plus de p^α substitutions communes, contre l'hypothèse.

Ils se confondent respectivement avec les sous-groupes

$$\mathfrak{K}_1, \quad \mathfrak{K}_2, \quad \ldots$$

d'ordre p^β que contient le groupe Γ.

En effet, K_1, par exemple, étant contenu dans Γ, sera nécessairement contenu dans l'un au moins des sous-groupes $\mathfrak{K}$, tel que $\mathfrak{K}_1$. Celui-ci devra lui-même être contenu dans l'un des groupes H. Ce dernier, ayant plus de p^α substitutions communes avec H_1, se confondra avec lui; mais K_1 contient toutes les substitutions communes à Γ et à H_1; il contiendra donc $\mathfrak{K}_1$; étant lui-même contenu dans $\mathfrak{K}_1$, il lui sera identique.

On aura par suite $\beta = \beta_1 = \beta_2 = \ldots > \alpha$.

7. Réciproquement, soit $\mathfrak{K}_i$ l'un quelconque des sous-groupes $\mathfrak{K}$. Il sera contenu dans l'un des groupes H et dans un seul, car son ordre est $> p^\alpha$. Ce dernier groupe appartiendra à la suite

$$H_1, \quad \ldots, \quad H_l$$

de ceux qui contiennent I. En effet, $\mathfrak{K}_1$ contient K_1 qui contient lui-même I. Ce sous-groupe invariant sera contenu dans les transformés de $\mathfrak{K}_1$ par les substitutions de Γ; or, $\mathfrak{K}_i$ est l'un de ces transformés.

Soit donc H_i celui des groupes H qui contient $\mathfrak{K}_i$. Le groupe K_i formé par les substitutions communes à H_i et à Γ contiendra $\mathfrak{K}_i$. Ayant le même ordre que ce dernier groupe, il se confondra avec lui.

8. Remarquons enfin que $\mathfrak{K}_i$ étant contenu dans un seul groupe H, à savoir H_i, toute substitution de G permutable à $\mathfrak{K}_i$ le sera à H_i. Or les groupes H étant en nombre q^2, chacun d'eux n'est permutable qu'à ses propres substitutions. Donc celles des substitutions de Γ qui sont permutables à $\mathfrak{K}_i$ seront communes à Γ et à H_i, et, par suite, appartiendront à $\mathfrak{K}_i$. Le nombre des groupes $\mathfrak{K}_1, \mathfrak{K}_2, \ldots, \mathfrak{K}_l$ sera donc q^λ. Donc

$$l = q^\lambda.$$

Le nombre des groupes H qui ont en commun le sous-groupe I sera donc égal à q^λ. Mais il est > 1 par hypothèse; donc $\lambda = 1$ ou 2.

Si $\lambda = 2$, I étant commun à tous les groupes H sera un sous-groupe invariant de G qui ne sera pas primitif.

9. Jusqu'ici nous n'avons guère fait que suivre la marche adoptée par M. Frobenius pour l'étude des groupes d'ordre $p^m q$. Mais une considération nouvelle est nécessaire pour traiter le cas où $\lambda = 1$, qu'il nous reste à examiner.

On a dans ce cas q^2 groupes H d'ordre p^2; q d'entre eux contiennent le sous-groupe I; celui-ci, transformé par les substitutions de G, donnera $\frac{p^m q^2}{p^\beta q} = p^{m-\beta} q$ transformés distincts I, I', ... dont chacun sera contenu dans q groupes H.

Réciproquement chacun des q^2 groupes H devra contenir $p^{m-\beta}$ sous-groupes de la suite I, I', ...

10. En particulier, les q groupes $H_1, \ldots, H_q$ qui contiennent I (et n'ont aucune autre substitution commune) contiendront en tout

$$1 + q(p^{m-\beta} - 1)$$

sous-groupes de la suite I, I', ... tous distincts. Il restera donc $q - 1$ sous-groupes $I', \ldots, I^{q-1}$ qui ne figurent dans aucun des groupes $H_1, \ldots, H_q$ où I figure.

Les substitutions permutables à I, en nombre $p^{m-\beta} q$, transformant les groupes $H_1, \ldots, H_q$ les uns dans les autres, transformeront exclusivement entre eux les sous-groupes $I', \ldots, I^{q-1}$ qui n'y figurent pas et cela de δ manières différentes, δ étant un diviseur commun à $p^{m-\beta} q$ et à $(q-1)!$

Les substitutions permutables à la fois à chacun des q sous-groupes $I, I', \ldots, I^{q-1}$ seront en nombre $\frac{p^{m-\beta} q}{\delta}$, nombre divisible par q.

11. Associons au contraire à I un système de $q - 1$ autres sous-groupes quelconques $I_1, \ldots, I_{q-1}$. L'un au moins de ces sous-groupes, I_1 par exemple, figurera dans l'un des groupes $H_1, \ldots, H_q$, par exemple dans H_1. Les substitutions permutables à la fois à $I, I_1, \ldots, I_{q-1}$ le seront à H_1; car c'est le seul des groupes H qui contienne à la fois I et I_1. Mais les groupes H étant en nombre q^2, chacun d'eux ne sera permutable qu'à ses propres substitutions, en nombre p^m. L'ordre du groupe formé par les substitutions permutables à la fois à $I, I_1, \ldots, I_{p-1}$ sera donc un diviseur de p^m.

12. Ainsi à chaque sous-groupe I correspond un groupe unique Δ jouissant de la double propriété suivante : 1° il a pour ordre un multiple de q; 2° ses substitutions sont permutables à q sous-groupes I, I', ..., I^{q-1} transformés de I. La symétrie de cet énoncé montre qu'à chacun de ces q sous-groupes correspondra le même groupe Δ.

Les sous-groupes I étant au nombre de $p^{m-\beta} q$, il y aura seulement $p^{m-\beta}$ groupes Δ, qui seront permutés les uns dans les autres par les substitutions de G.

Leurs déplacements forment un groupe $\mathcal{G}$ isomorphe à G et de degré $p^{m-\beta}$.

Or, on a

$$q^2 \equiv 1 \mod p^{m-\alpha}.$$

Donc, $p^{m-\alpha}$ divise q^2-1; et, comme $q+1$ et $q-1$ ont pour plus grand commun diviseur 2, il divisera $2(q-1)$ ou $2(q+1)$ et ne pourra surpasser ce dernier nombre. Donc

$$p^{m-\beta} \leqq \frac{2(q+1)}{p^{\beta-\alpha}} < 2q \qquad (\text{car } \beta > \alpha).$$

Donc G, admettant un isomorphe $\mathcal{G}$ de degré $< 2q$, sera composé.