BULLETIN DE LA S. M. F.

ED. MAILLET

Sur les groupes échangeables et les groupes décomposables

Bulletin de la S. M. F., tome 28 (1900), p. 7-16

<http://www.numdam.org/item?id=BSMF_1900__28__7_0>

SUR LES GROUPES ÉCHANGEABLES ET LES GROUPES DÉCOMPOSABLES;

Par M. Edmond Maillet.

I.

Dans une Note antérieure (1) nous avons appelé un groupe D *décomposable* quand l'on peut y trouver deux sous-groupes A et B d'ordre > 1, tous deux $< D$ et tels que toute substitution d de D soit le produit d'une substitution a de A, par une b de B; on indique cette propriété en écrivant $D = AB = A \times B$. D sera dit le produit de A par B; A et B sont des facteurs de D : on a évidemment $D = AB = BA$.

Tout groupe est-il décomposable? A défaut d'un criterium de *décomposabilité*, on pourrait étudier les groupes connus : il y a là tout un sujet de recherches.

Nous ne prétendons pas résoudre ici la question (2), tout en nous proposant d'étudier un certain nombre des propriétés de la décomposabilité des groupes. Parmi les groupes dont nous nous sommes occupé, nous n'avons trouvé d'autres groupes indécomposables que ceux formés des puissances d'une substitution circulaire d'ordre p^m (p premier).

II.

DÉCOMPOSABILITÉ DE CERTAINS GROUPES.

1° *Groupes primitifs composés.* — Un pareil groupe G est toujours décomposable, car tout sous-groupe invariant K de G est transitif (3), et si H est le sous-groupe des substitutions de G

(1) *Note sur les substitutions* (*Bulletin de la Société Mathématique*, t. XXIV; 1896). La plupart des considérations de la Note actuelle s'appliquent aussi bien aux groupes d'opérations qu'aux groupes de substitutions. Divers auteurs ont déjà envisagé les groupes échangeables, par exemple Serret et M. Frobenius.

(2) Nous croyons au contraire, sous réserve de vérification, l'avoir résolue par l'affirmative pour les groupes de transformations de Lie.

(3) Jordan, *Traité des Substitutions*, p. 41.

qui laissent une même lettre de G immobile on a $G = H \times K$, avec $H < G$, $K < G$ (¹).

2° *Groupes composés quelconques.* — D'après les mêmes remarques, soient G un pareil groupe, H un sous-groupe invariant maximum de G:

α. Si l'on peut trouver un sous-groupe invariant H′ de G non contenu dans H, on a $G = H \times H'$. En effet, si h et h' sont les ordres de H et H′, k l'ordre du groupe K des substitutions communes à H et H′, l'ordre du groupe (H, H′) dérivé de H et de H′ est $\frac{hh'}{k} > h$, en sorte que (H, H′) = G, puisque (H, H′) est invariable par les substitutions de G; alors les substitutions de G sont toutes de la forme $\eta\eta'$, η appartenant à H, η' à H′.

β. Si H est à la fois maximum dans G et invariable par les substitutions de G, et si l'on peut trouver un sous-groupe H′ de G non contenu dans H, on a encore $G = H \times H'$. En particulier un groupe d'ordre p^m non formé des puissances d'une substitution circulaire d'ordre p^m est décomposable. Au contraire, le groupe des puissances d'une substitution circulaire d'ordre p^m est indécomposable.

3° *Groupes d'ordre $p^m q^n$ (p et q premiers différents).* — Un pareil groupe G contient un sous-groupe P d'ordre p^m, un Q d'ordre q^n. On a $G = P \times Q$.

4° *Groupes de degré p^m (p premier) et d'ordre $\neq p^n$.* — Soit G un pareil groupe : si H_α est le groupe des substitutions de G qui laissent une même lettre α immobile, $p^{m'}$ la plus haute puissance de p qui divise l'ordre g de G, G renferme un sous-groupe P d'ordre $p^{m'}$, et $G = P \times H_\alpha$.

(¹) *Voir* notre Note précitée où nous montrons que le problème de la recherche des sous-groupes transitifs des isomorphes holoédriques et transitifs d'un groupe donné est compris dans celui de la recherche des décompositions de ce groupe en un produit de deux sous-groupes, et lui est équivalent quand le groupe donné est simple.

5° *Groupes d'ordre* $4h+2$. — G renferme un sous-groupe d'ordre 2 et un sous-groupe invariant d'ordre $2h+1$ dont il est le produit.

6° *Groupe alterné* G *de n éléments.* — Il est décomposable. En effet, on sait qu'il suffit d'établir l'existence d'un sous-groupe transitif A de G. Si alors B est le groupe alterné de $n-1$ éléments, $G = A \times B$.

a. n impair. On prend pour A le groupe des puissances d'une substitution d'ordre n.

b. n pair et $= 4h$. On prend pour A le groupe dérivé des substitutions

$$\gamma = (a_1 a_2 \ldots a_{2h})(a_{2h+1} \ldots a_{4h}),$$
$$\gamma' = (a_1 a_{2h+1}) \ldots (a_{2h} a_{4h}).$$

c. n pair et $= 4h+2 = 2p$.

On prend pour A le groupe dérivé (¹) de la substitution

$$\gamma = (a_1 a_2 \ldots a_p)(a_{p+1} \ldots a_{2p}),$$

et des substitutions

$$(a_i a_{p+i})(a_j a_{p+j}) \qquad (i \neq j,\ i, j = 1, 2, \ldots, p).$$

7° *Groupe symétrique de n éléments.* — Il est décomposable. En effet, on a $G = A \times B$, B étant le groupe symétrique de $n-1$ éléments, A le groupe des puissances d'une substitution circulaire d'ordre n.

Il résulte de là cette conclusion intéressante :

L'ensemble des groupes décomposables est plus étendu que l'ensemble des groupes primitifs composés, puisque tout groupe primitif composé est décomposable et que les groupes alternés sont décomposables.

(¹) Ce groupe est d'ordre $2^{p-1}p$ et, d'après un théorème de Mathieu (*Journal de Mathématiques,* 1861), généralisé par M. Sylow, contient $2^{p-1} = 1 + np$ sous-groupes d'ordre p. On en conclut $2^{p-1} \equiv 1 \pmod p$, théorème dû à Fermat. Cette démonstration n'est qu'un cas particulier de la démonstration du théorème de Fermat [$a^p \equiv a \pmod p$ quel que soit a], que nous avons donnée dans notre *Thèse de Dootorat* (Gauthier-Villars; 1892, p. 116), en nous appuyant sur le théorème de Mathieu et de M. Sylow

Nous énoncerons encore les propriétés suivantes, dont les démonstrations ne sont qu'indiquées :

LEMME. — *Si deux sous-groupes* H_1 *et* H_2, *d'ordres* h_1 *et* h_2, *d'un groupe* G *d'ordre* g, *sont tels que le plus petit commun multiple de* h_1 *et* h_2 *est* g, *on a* $G = H_1 \times H_2$.

On voit, en effet, de suite que le groupe (H_1, H_2), dérivé de H_1 et H_2, contient au moins g substitutions qui sont le produit d'une substitution de H_1 par une de H_2.

THÉORÈME. — *Si un groupe primitif* G *de degré* n *est indécomposable, il possède au moins deux isomorphes holoédriques et primitifs de degrés différents et différents de* n.

En effet, soient p un diviseur premier de n, p^α la plus haute puissance de p qui divise l'ordre g de G. G contient au moins un sous-groupe maximum H d'ordre h divisible par p^α, et auquel correspond (¹) un isomorphe holoédrique et primitif Γ de G, de degré $\frac{g}{h}$ premier à p et $\neq n$.

Soit q un autre diviseur premier quelconque de n, q^β la plus haute puissance de q qui divise g : si $h \equiv 0 \pmod{q^\beta}$, quel que soit le diviseur q de n, le lemme précédent montre que G est décomposable.

Si donc G n'est pas décomposable, on peut trouver q tel que $n \equiv 0 \pmod{q}$ avec $h \not\equiv 0 \pmod{q^\beta}$. Il existe alors un sous-groupe maximum H_1 de G d'ordre h_1 divisible par q^β, auquel correspond un isomorphe holoédrique et primitif Γ_1 de G de degré $\frac{g}{h_1}$ premier à q et différent de n et de $\frac{g}{h}$.

III.

QUELQUES PROPRIÉTÉS DES GROUPES DÉCOMPOSABLES.

1° Si $A = B \times B'$, et si D contient B et est contenu dans A, on a $A = D \times B'$.

(¹) *Voir*, par exemple, W. DYCK, *Mathematische Annalen*, t. XX et XXII, et notre *Thèse de Doctorat*, p. 12 et 15.

Nous dirons que B et B′ sont des *facteurs complémentaires* de A.

2° Si $A = B \times B' = C \times C'$, C étant contenu dans B, on a $B = C \times D$, D étant le groupe commun à B et C′.

En effet, soient a, b, b', c, c', d les ordres respectifs de A, B, B′, C, C′, D; E le groupe commun à B et B′, d'ordre e; F le groupe commun à C et C′, d'ordre f. On a

$$a = \frac{bb'}{e} = \frac{cc'}{f} = \frac{bc'}{d}.$$

On en conclut

$$b = \frac{cd}{f}.$$

Soit Φ, d'ordre φ, le groupe commun à C et D; B contenant C et D, on a $b \geq \frac{cd}{\varphi}$. D étant contenu dans C′, Φ est contenu dans C et C′, par suite dans F, et $\varphi \leq f$. On en tire

$$\frac{cd}{\varphi} \geq \frac{cd}{f} = b \geq \frac{cd}{\varphi},$$

d'où $\varphi = f$. Donc si γ et δ sont des substitutions de C et D respectivement, on a exactement $\frac{cd}{f}$ substitutions de la forme $\gamma\delta$ et $B = C \times D$.

3° Réciproquement, si $A = B \times C'$, et $B = C \times D$, D étant le groupe commun à B et C′, on a $A = C \times C'$.

En effet, si F est le groupe commun à C et C′, il suffit de montrer que

$$a = \frac{cc'}{f}.$$

Or

$$a = \frac{bc'}{d}, \qquad b = \frac{cd}{\varphi},$$

Φ étant le groupe commun à C et D, d'où

$$a = \frac{c'}{d}\,\frac{cd}{\varphi} = \frac{cc'}{\varphi}.$$

Or F, commun à C et C′, est commun à B et C′ : donc F est contenu dans D, c'est-à-dire commun à D et C, par suite contenu

dans Φ; f divise φ, et $f \leqq \varphi$. Mais $\frac{cc'}{f} \leqq a = \frac{cc'}{\varphi}$, puisque C et C′ sont contenus dans A ; donc $\varphi \leqq f$, d'où $f = \varphi$, $a = \frac{cc'}{f}$.

4° Si A et B sont échangeables à C, (A, B) est échangeable à C.

5° Si A et B sont échangeables, et si C, contenu dans B, est échangeable à A, soit D le groupe commun à A et B : D est échangeable à C.

Soient α, α', ...; β, ...; γ, ...; δ, ... des substitutions de A, B, C, D respectivement. On a

$$\alpha\beta = \beta'\alpha',$$
$$\alpha\gamma = \gamma'\alpha',$$
$$\delta\gamma = \gamma''\alpha'',$$
$$\alpha'' = \gamma''^{-1}\delta\gamma = \beta'' = \delta',$$
$$\delta\gamma = \gamma''\delta'.$$

6° Si $A = CB'$ et si B contient C et est contenu dans A, on a $B = C \times D$, D étant le groupe commun à B et B′.

Il suffit d'appliquer la deuxième propriété en faisant $C' = B'$.

7° Réciproquement si $A = B \times B'$, si D est le groupe commun à B et B′, et si $B = C \times D$, on a $A = CB'$.

On applique la troisième propriété en faisant $C' = B'$.

IV.

AUTRE MANIÈRE DE PRÉSENTER CERTAINES DES IDÉES PRÉCÉDENTES.

Soient G un groupe transitif qui ne soit pas primitif, H_α le groupe qui laisse une lettre α immobile, N le degré de G, g, h_α les ordres de G et H_α; on a $g = N h_\alpha$.

Soient

$$P_1, \quad P_2, \quad \ldots, \quad P_{\frac{N}{p}},$$
$$Q_1, \quad Q_2, \quad \ldots, \quad Q_{\frac{N}{q}}$$

deux répartitions des lettres de G, p à p et q à q admises par le groupe G. Toute substitution S de G qui remplace P_i par $P_{i'}$, et Q_j par $Q_{j'}$, remplace les lettres communes à P_i et Q_j par les lettres communes à $P_{i'}$ et $Q_{j'}$. Si P_i et Q_j ont en commun r

lettres formant un système R_1 ($r > o$), les lettres communes à $P_{i'}$ et $Q_{j'}$ formeront un système R_2 de r lettres ayant toutes ses lettres communes ou n'en ayant aucune avec R_1. G étant transitif, on pourra toujours trouver une substitution S remplaçant une lettre donnée a de R_1 par une lettre arbitraire b, et si S remplace P_i et Q_j par $P_{i''}$ et $Q_{j''}$, on voit que b fera partie d'un système R_k de r lettres formé des lettres communes à $P_{i''}$ et $Q_{j''}$. Les systèmes

$$R_1, \quad R_2, \quad \ldots, \quad R_k, \quad \ldots$$

contiendront toutes les lettres de G, seront toujours communs chacun à deux des systèmes P et Q et à deux seulement, et n'auront deux à deux une lettre commune que s'ils sont identiques. En choisissant convenablement $\frac{N}{r}$, on aura donc une répartition des lettres de G, r à r, en systèmes de non-primitivité.

Si (P_i), (Q_j), (R_k) sont respectivement les groupes de substitutions qui permutent exclusivement entre elles les lettres d'un des systèmes P_i, Q_j, R_k, leurs ordres sont respectivement

$$(p) = p\,h_\alpha, \qquad (q) = q\,h_\alpha, \qquad (r) = r\,h_\alpha.$$

r étant évidemment diviseur commun de p et q, on a

$$p = \varpi r, \qquad q = \chi r,$$

et si R_k est commun à P_i et Q_j, (R_k) est le groupe commun à (P_i) et (Q_j).

Une répartition R_1, R_2, ... dont chaque système est contenu dans un des systèmes de P_1, P_2, ... et de Q_1, Q_2, ... est dite *commune* aux deux répartitions P et Q. Celle que nous avons formée plus haut est *la plus grande répartition commune à* P *et* Q.

S'il existe une répartition S_1, S_2, ..., S_g telle que chacun des systèmes S contienne un nombre exact de systèmes P et de systèmes Q, la répartition S sera dite *multiple de ces deux répartitions*.

Une substitution T de G qui remplace P_i par $P_{i'}$ remplace l'ensemble Σ_i des systèmes Q ayant des lettres communes avec P_i par l'ensemble $\Sigma_{i'}$ des systèmes Q ayant des lettres communes avec $P_{i'}$. Mais il s'en faut de beaucoup que les ensembles Σ_i, $\Sigma_{i'}$, ...

qu'on obtiendrait en raisonnant comme précédemment sur les systèmes R forment toujours une répartition en systèmes de non-primitivité admise par G. Ces systèmes peuvent avoir deux à deux des lettres communes sans les avoir toutes.

Voici un exemple simple :

Le groupe régulier G d'ordre et de degré 60 isomorphe au groupe alterné de cinq éléments admet plusieurs répartitions de ses lettres cinq à cinq, sans quoi il serait composé (¹). Soient $P_1, P_2, \ldots$ et $Q_1, Q_2, \ldots$ les systèmes de deux de ces répartitions : deux des systèmes P et Q auront en commun r lettres, r divisant 5, d'après ce qui précède, avec $r < 5$: donc $r = 1$. L'ensemble Σ_1 des systèmes Q ayant des lettres communes avec P_1 contient 25 lettres et G n'admet pas de répartition de ses lettres 25 à 25.

Plus généralement, si θ^m est la plus haute puissance du nombre premier θ qui divise l'ordre g d'un groupe régulier G, et si G ne contient pas de sous-groupe invariant d'ordre θ^m, G admettra plusieurs répartitions de ses lettres θ^m à θ^m, et si $P_1, P_2, \ldots$ et $Q_1, Q_2, \ldots$ sont deux de ces répartitions, on verra encore que l'ensemble Σ_1 des systèmes Q ayant des lettres communes avec P_1 contient θ^n lettres avec $n \geq m + 1$, et G n'admet pas de répartition de ses lettres θ^n à θ^n.

Il pourra néanmoins se présenter des cas où deux quelconques des ensembles $\Sigma_1, \Sigma_2, \ldots$ n'ont aucune lettre commune s'ils ne les ont pas toutes. Alors $\Sigma_1, \Sigma_2, \ldots$ donnera une répartition des lettres de G, s à s. Σ_1 comprendra exactement ϖ systèmes Q et χ systèmes P. On voit, en effet, sans peine, que Σ_1 est formé de l'ensemble des systèmes P ayant des lettres communes avec Q_1. Chacun des systèmes $Q_1, Q_2, \ldots$ ayant des lettres communes avec P_1, en aura le même nombre r, et

$$\varpi = \frac{p}{r}, \qquad \chi = \frac{q}{r}, \qquad s = \frac{pq}{r}.$$

L'ordre (s_k) du groupe des substitutions de G laissant invariable le système Σ_k est

$$(s_k) = sh_\alpha = \frac{pq}{r} h_\alpha.$$

(¹) *Voir* notre *Thèse de Doctorat*, p. 10.

(Σ_1) contient (P_1) et (Q_1). (P_1) et (Q_1) n'ayant que rh_α substitutions communes, le groupe $[(P_1), (Q_1)]$ dérivé de (P_1), (Q_1) est d'ordre $\geq \frac{pq}{r} h_\alpha = (s_1)$. Donc (P_1) et (Q_1) sont échangeables et leur produit est (Σ_1).

Réciproquement, si l'on considère les deux systèmes P_1 et Q_1 ayant r lettres communes exactement, et si (P_1) et (Q_1) sont échangeables, l'ensemble Σ_1 des systèmes Q ayant des lettres communes avec P_1 donnera une répartition en systèmes Σ de $\frac{pq}{r}$ lettres admise par G. Il suffit, en effet, de considérer le groupe $(P_1) \times (Q_1)$ d'ordre $\frac{pq}{r} h_\alpha$ et la répartition correspondante admise par G.

Ceci posé, nous dirons par extension que *les deux répartitions* P *et* Q *sont échangeables* si les deux groupes (P_1) et (Q_1) le sont. Nous pouvons donc énoncer le théorème suivant :

THÉORÈME I. — *Étant donné un groupe* G *transitif qui admet les deux répartitions en systèmes*

$$P_1, \quad P_2, \quad \ldots,$$
$$Q_1, \quad Q_2, \quad \ldots,$$

la condition nécessaire et suffisante pour que l'ensemble des systèmes Q *ayant des lettres communes avec un même système* P_1 *forme un système d'une répartition en systèmes de non-primitivité admise par* G, *c'est-à-dire pour que les deux répartitions* P, Q *soient échangeables, est que le groupe* (P_1) *soit échangeable à un des groupes* (Q_j), (P_i), (Q_j) *étant formés respectivement des substitutions qui laissent immobiles* P_i *et* Q_j.

Nous nous proposons de considérer en particulier les groupes dont tous les sous-groupes sont deux à deux échangeables : soit G un pareil groupe d'ordre $g = p_1^{\alpha_1} \ldots p_i^{\alpha_i} (p_1, \ldots, p_i$ nombres premiers différents). G renferme un groupe H_1 d'ordre $p_1^{\alpha_1}$: si H_1 n'est pas invariant dans G, G renferme au moins deux sous-groupes distincts d'ordre $p_1^{\alpha_1}$ échangeables : le groupe dérivé serait d'ordre $p_1^{\beta_1}$ avec $\beta_1 > \alpha_1$, ce qui est absurde.

On en conclut que deux sous-groupes d'ordre $p_k^{\alpha_k}$, $p_j^{\alpha_j}$ $(k \neq j)$

de G sont tels que chacun est permutable aux substitutions de l'autre. Donc (1) chacun a ses substitutions échangeables à celles de l'autre, et l'on a ce théorème :

THÉORÈME II. — *Un groupe* G *d'ordre* $p_1^{\alpha_1}\dots p_i^{\alpha_i}(p_1, \dots, p_i$ *nombres premiers distincts*) *et dont tous les sous-groupes sont échangeables est tel que toute substitution d'ordre* p_k^m *y est échangeable à toute substitution de* G *d'ordre premier à* p_k.

Ces groupes sont résolubles.

Remarque. — Les groupes dont toutes les substitutions sont échangeables appartiennent à cette catégorie de groupes (2); mais celle-ci comprend d'autres groupes. C'est le cas du groupe A régulier d'ordre et de degré 27 dérivé des substitutions

$$\begin{cases} S = (123456789)(1'2'\dots9')(1''2''\dots9''), \\ T = (11'1'')(44'4'')(77'7'')(25'8'')(2'5''8)(2''58')(39'6'')(3'9''6)(3''96'), \end{cases}$$

les éléments étant représentés par 1, 2, ..., 9, 1', 2', ..., 9', 1'', 2'', ..., 9''.

On a

$$T^{-1}S\ T = S^4,$$
$$T^{-1}S^3T = S^3.$$

Ce groupe n'est pas formé de substitutions échangeables, et cependant deux quelconques de ses sous-groupes sont échangeables. On voit, en effet, que ST et ST^2 sont d'ordre 9 et que G renferme 18 substitutions d'ordre 9 et 8 d'ordre 3 formant un sous-groupe d'ordre 9 avec l'unité.

Nous verrons plus tard que les propriétés précédentes s'étendent d'une façon plus parfaite aux groupes de Lie.

---

(1) *Voir,* par exemple, *Annales de la Faculté des Sciences de Toulouse*, t. IX, 1895, D.17, théorème V.

(2) Ces groupes comprennent les groupes appelés *hamiltoniens* par MM. Dedekind et Miller (*Comptes rendus,* 16 mai 1898); ils en comprennent d'autres, car A n'est pas hamiltonien.

Un résumé des résultats ci-dessus a été communiqué au Congrès de Boulogne pour l'avancement des Sciences. (Voir *Comptes rendus de l'Association française pour l'avancement des Sciences,* 1899.)