SOPHIE PICCARD

Structure des groupes libres

Annales scientifiques de l'É.N.S. 3e série, tome 76, no 1 (1959), p. 1-58
<http://www.numdam.org/item?id=ASENS_1959_3_76_1_1_0>

ANNALES
SCIENTIFIQUES
DE
L'ÉCOLE NORMALE SUPÉRIEURE

STRUCTURE DES GROUPES LIBRES

PAR M[lle] SOPHIE PICCARD.

Introduction.

Soit G un groupe multiplicatif engendré par un ensemble A d'éléments dont aucun ne peut être obtenu par composition finie des autres. L'ensemble A ne contient donc pas l'élément neutre 1 du groupe G et ne peut contenir qu'un seul de deux éléments x, x^{-1}, quel que soit $x \in G$, Tout élément de G peut être obtenu par composition finie d'éléments de A (¹). Soit $f(a_1, a_2, \ldots, a_k)$ une composition finie quelconque d'éléments $a_1, a_2, \ldots, a_k$ (en nombre fini k) de A, C'est un produit de puissances finies des éléments $a_1, a_2, \ldots, a_k$, pris dans un ordre quelconque, un même élément a_i pouvant contribuer à former divers facteurs du produit. On dit que la composition f est *réduite* si l'on y a remplacé partout le produit de deux facteurs consécutifs (s'il y en avait) du type $a_i^m a_i^n$, où i est un nombre quelconque de la suite $1, 2, \ldots, k$ et m et n sont deux entiers quelconques, par a_i^{m+n}, dans le cas où $m+n \neq 0$, ou par 1, lorsque $m+n=0$, et si l'on a laissé tomber tous les facteurs égaux à 1, pour autant que la composition envisagée entière ne se réduit pas identiquement à 1, auquel cas on dira que 1 est sa forme réduite. D'après cette définition, toute composition finie réduite $f(a_1, a_2, \ldots, a_k)$ des éléments $a_1, a_2, \ldots, a_k$ de A, pour autant qu'elle n'est pas identiquement égale à 1 (l'élément neutre de G), est de la forme $a_{i_1}^{j_1} a_{i_2}^{j_2} \ldots a_{i_r}^{j_r}$, où $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$ sont des éléments (pas nécessairement distincts) de l'ensemble $\{a_1, a_2, \ldots, a_k\}$ tels que $a_{i_t} \neq a_{i_{t+1}}$ $(t=1, 2, \ldots, k-1)$

(¹) Et de leurs inverses, sous-entendu.

et $j_1, j_2, \ldots, j_r$ sont des entiers non nuls quelconques (positifs ou négatifs). Soient $a_{i_1}^{j_1} a_{i_2}^{j_2} \ldots a_{i_r}^{j_r}$ et $a_{k_1}^{l_1} a_{k_2}^{l_2} \ldots a_{k_s}^{l_s}$ deux compositions finies réduites d'éléments de A qui ne se réduisent pas identiquement à 1. Ces compositions sont distinctes si $s \neq r$ ou si $s = r$ mais si, soit $a_{i_t} \neq a_{k_t}$, pour une valeur au moins de l'indice $t = 1, 2, \ldots, r$, soit $a_{i_t} = a_{k_t} (t = 1, 2, \ldots, r)$ mais $j_t \neq l_t$ pour une valeur au moins de l'indice $t = 1, 2, \ldots, r$.

Si le groupe G n'est pas libre, les éléments de tout système générateur A sont liés par un certain nombre de relations non triviales (qui ne découlent pas des axiomes de groupe) de la forme $f(a_1, a_2, \ldots, a_k) = 1$ où $f(a_1, a_2, \ldots, a_k)$ est une composition finie réduite d'éléments de A qui ne se réduit pas identiquement à 1. Toute relation de cette nature implique l'égalité entre deux compositions finies réduites distinctes d'éléments de A.

Si le groupe G est libre, il possède des systèmes d'éléments générateurs qui ne sont liés par aucune relation non triviale et si A est un tel système d'éléments générateurs du groupe libre G, chaque élément de G peut se mettre de façon unique sous la forme d'une composition finie réduite d'éléments de A. Les éléments d'un système générateur A d'un groupe libre qui ne sont liés par aucune relation non triviale sont appelés des *éléments libres* du groupe G. Tous les éléments de G ne sont pas libres. Ainsi, par exemple, 1 n'est pas libre. Tout groupe libre possède aussi bien des éléments libres que des éléments non libres et il est, comme on sait, le produit libre des groupes cycliques engendrés par les éléments d'un quelconque de ses systèmes générateurs formé d'éléments libres.

Soit c un élément $\neq 1$ quelconque d'un groupe libre engendré par un ensemble A d'éléments libres et soit

$$a_{i_1}^{j_1} a_{i_2}^{j_2} \ldots a_{i_r}^{j_r} \tag{$\uparrow$}$$

la composition finie réduite d'éléments de A qui le représente. Soient $a_1, a_2, \ldots, a_k$ les divers éléments de A (en nombre fini) qui figurent dans cette composition et soit n_i le degré de ($\uparrow$) par rapport à $a_i (i = 1, 2, \ldots, k)$. Nous dirons que n_i est *le degré* de l'élément c par rapport à l'élément a_i de l'ensemble A $(i = 1, 2, \ldots, k)$ et nous dirons que c est de degré nul par rapport à tout élément de l'ensemble $A - \{a_1, a_2, \ldots, a_k\}$. Comme ($\uparrow$) est l'unique composition finie réduite d'éléments de A qui représente l'élément c de G, on voit que quel que soit l'ensemble A d'éléments générateurs libres d'un groupe libre G, tout élément de G possède un degré bien défini par rapport à tout élément de l'ensemble A.

Il est à noter que les groupes libres ne sont pas les seuls à jouir de cette propriété. Tout groupe G défini par un système A d'éléments générateurs liés par un ensemble de relations fondamentales non triviales dont chacune est de degré zéro par rapport à chacun des éléments de A jouit de cette propriété que bien que deux compositions réduites distinctes peuvent représenter un même élément de G, deux telles compositions sont toujours du même degré par rapport à chaque élément de A.

Loi de composition des éléments d'un groupe libre.

Soit G un groupe libre engendré par un ensemble A d'éléments générateurs libres, soient a et b deux éléments quelconques de G. Chacun des éléments a, b possède une expression unique par une composition finie réduite d'éléments de A. Soit

$$a = a_{i_1}^{j_1} a_{i_2}^{j_1} \dots a_{i_r}^{j_r} \qquad \text{et} \qquad b = a_{k_1}^{l_1} a_{k_2}^{l_2} \dots a_{k_s}^{l_s}$$

ces expressions et soit $\{a_1, a_2, \dots, a_k\}$ l'ensemble (fini) d'éléments de A qui figurent dans les expressions de a et de b. Soit m_i le degré de a et n_i le degré de b par rapport à $a_i (i = 1, 2, \dots, k)$; a aussi bien que b est de degré nul par rapport à tout élément de l'ensemble $A - \{a_1, a_2, \dots, a_k\}$. Le produit ab peut à son tour, être exprimé de façon unique par une composition finie réduite des éléments $a_1, a_2, \dots. a_k$. Cette expression est la suivante.

Si $i_r \neq k_1$,

$$ab = a_{i_1}^{j_1} a_{i_2}^{j_2} \dots a_{i_r}^{j_r} a_{k_1}^{l_1} a_{k_2}^{l_2} \dots a_{k_s}^{l_s}.$$

Et si $i_r = k_1$, soit h le plus grand entier $\geqq 0$, tel que $a_{i_{r-h}} = a_{k_{1+h}}$ et que $a_{i_{r-t}}^{j_{r-t}} = a_{k_{1+t}}^{-l_{1+t}} (t = 0, 1, \dots, h-1)$ si $h > 0$.

Alors si $j_{r-h} \neq -l_{1+h}$, on a

$$ab = a_{i_1}^{j_1} a_{i_2}^{j_2} \dots a_{i_{r-h-1}}^{j_{r-h-1}} a_{i_{r-h}}^{j_{r-h}+l_{1+h}} a_{k_{2+h}}^{l_{2+h}} \dots a_{k_s}^{l_s}.$$

Et si $j_{r-h} = -l_{1+h}$, on a

$$ab = a_{i_1}^{j_1} a_{i_2}^{j_2} \dots a_{i_{r-h-1}}^{j_{r-h-1}} a_{k_{2+h}}^{l_{2+h}} \dots a_{k_s}^{l_s}.$$

Il s'ensuit que ab est de degré $m_i + n_i$ par rapport à $a_i (i = 1, 2, \dots, k)$ et que ab est de degré nul par rapport à tout élément de l'ensemble $A - \{a_1, a_2 \dots, a_k\}$. Par conséquent, le degré du produit de deux éléments quelconques a et b de G par rapport à un élément quelconque d'un système A de générateurs libres est égal à la somme des degrés de a et de b par rapport au même élément de A.

Soit G un groupe libre engendré par un ensemble A d'éléments libres. Nous allons répartir les éléments de G d'une infinité de façons en classes d'équivalence dont chacune contient, avec tout élément a de G la classe entière des éléments de G conjugués à a, nous donnerons une loi commutative de composition de ces classes qui permet d'associer à tout groupe libre une infinité de groupes abéliens $\Gamma^{(n)}$ dont les éléments sont des classes d'équivalence d'éléments de G. Nous montrerons que quel que soit le sous-groupe γ d'un groupe $\Gamma^{(n)}$, la réunion des classes d'équivalence d'éléments de G qui constituent les éléments de ce groupe γ est un sous-groupe invariant de G. Nous utiliserons les groupes $\Gamma^{(n)}$

pour étudier la structure des groupes libres. Ces considérations permettent d'établir l'existence d'une infinité de sous-groupes invariants dans tout groupe libre, elles facilitent la recherche des éléments libres des groupes libres, elles permettent d'établir de nombreux théorèmes relatifs à la structure des groupes libres, quelle que soit la puissance de l'ensemble A des générateurs libres. Les classes d'équivalence en lesquelles on répartit, d'une infinité de façons, les éléments de tout groupe libre ont un caractère intrinsèque, indépendant du système générateur A qui sert à les définir. Quel que soit le sous-groupe g du groupe libre G, deux classes d'équivalences quelconques d'éléments de G qui contiennent des éléments de g ont en commun avec g des ensembles d'égale puissance.

Appelons *base* d'un groupe libre G tout système générateur de G formé d'éléments libres. Un groupe cyclique libre, composé des puissances entières d'un élément libre a ne possède, comme on sait, que deux bases : a et a^{-1} qui sont ses seuls éléments libres. Tout groupe libre non cyclique possède, comme on sait, une infinité de bases. Pour s'en convaincre, il suffit d'observer que quelle que soit la base A d'un tel groupe G et quels que soient deux éléments distincts a_1 et a_2 de A, on déduit de A une nouvelle base en remplaçant a_2 par $a_1^m a_2 a_1^n$, quels que soient les entiers m et n. Si le groupe G est engendré par un ensemble infini A de puissance $\mathfrak{m}$ d'éléments générateurs libres, il possède un ensemble de puissance supérieure à $\mathfrak{m}$ de bases. En effet, quel que soit le sous-ensemble non vide $A^\star$ de A, remplaçons dans A chaque élément de $A^\star$ par son inverse. Le système obtenu est, comme on sait, une base de G et à deux sous-ensembles distincts $A^\star$ et $A^{\star\star}$ de A correspondent deux bases différentes. Et comme l'ensemble de tous les sous-ensembles de A est de puissance $2^{\mathfrak{m}} > \mathfrak{m}$, G possède bien un ensemble de puissance $> \mathfrak{m}$ (donc en tout cas indénombrable) de systèmes générateurs dont tous les éléments sont libres.

Tout élément $\neq 1$ d'un groupe libre est, comme on sait, d'ordre infini.

Si un groupe libre est engendré par un système fini de k éléments libres, le groupe G ne saurait, comme on sait, être engendré par moins de k éléments et tout système comprenant k éléments, générateur de G, est formé d'éléments libres. Le nombre k est alors appelé le *rang* du groupe libre G.

Systèmes irréductibles d'éléments générateurs d'un groupe.

Définition. — *Soit G un groupe engendré par un ensemble A (fini ou infini) d'éléments générateurs. Nous disons que l'ensemble de générateurs A est* irréductible *si, quel que soit le sous-ensemble fini* $\mathrm{A}^\star$ *de* A, *il n'existe aucun sous-ensemble fini B de G formé d'un nombre d'éléments inférieur à celui de* $\mathrm{A}^\star$ *et tel que tout élément de* $\mathrm{A}^\star$ *puisse être obtenu par composition finie d'éléments de B.*

Toute base d'un groupe libre est irréductible. — En effet, soit G un groupe libre et soit A l'une quelconque de ses bases. Supposons qu'elle soit réductible et soit $A^\star$ un sous-ensemble fini formé de k éléments de G pour lequel il existe un ensemble B formé de $k' < k$ éléments de G et tel que tout élément de $A^\star$ puisse être obtenu par composition finie d'éléments de B. Soit $G^\star$ le groupe libre engendré par les k éléments de l'ensemble $A^\star$ qui en forment une base. Comme tout élément de $A^\star$ s'obtient par composition finie d'éléments de B, B est à son tour un système générateur de $G^\star$, ce qui est impossible, d'après les propriétés connues des groupes libres, puisque $k' < k$. On voit donc bien que la base A est irréductible.

Nous allons d'abord traiter le cas où l'ensemble A est fini, puis nous passerons au cas où l'ensemble A est infini, de puissance quelconque, et enfin nous signalerons diverses généralisations des méthodes exposées qui se prêtent également à l'étude de la structure des groupes libres.

Les groupes libres de rang fini.

I. Soit G un groupe multiplicatif libre engendré par un nombre fini k d'éléments générateurs $a_1, a_2, \ldots, a_k$ qui ne sont liés par aucune relation non triviale. Les seules relations satisfaites par ces éléments générateurs sont des relations triviales qui dérivent des axiomes de groupes, telles que les relations

$$a_i a_i^{-1} = 1 \qquad (i = 1, 2, \ldots, k),$$

ainsi que les relations identiques de la forme

$$f(a_1, a_2, \ldots, a_k) = f(a_1, a_2, \ldots, a_k),$$

où f est une composition finie quelconque des éléments de l'ensemble

$$A = \{a_1, a_2, \ldots, a_k\}.$$

Les classes $M^{(n)}$. — Soit n un entier quelconque $\geqq 2$. Répartissons les éléments de G en n^k classes $M^{(n)}$ comme suit. Soit a un élément quelconque de G. Il peut être obtenu par composition finie des éléments de A. Soit $a = f(a_1, a_2, \ldots, a_k)$, où f est une composition finie réduite des éléments de A. Comme G est un groupe libre dont l'ensemble A est une base, la composition réduite des éléments de cette base qui représente l'élément a est *unique*. Soit u_i le degré de f par rapport à a_i $(i = 1, 2, \ldots, k)$; u_i est aussi le degré de l'élément a de G par rapport à l'élément a_i de la base A. Soit λ_i le nombre de la suite $0, 1, \ldots, n-1$, tel que $u_i \equiv \lambda_i \pmod{n}$ $(i = 1, 2, \ldots, k)$. Nous disons que l'élément a fait partie de la classe $M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k}$. Quels que soient les k nombres (distincts ou non, peu importe) $\lambda_1, \lambda_2, \ldots, \lambda_k$ de la suite $0, 1, \ldots, n-1$, la classe $M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k}$ n'est pas vide. Elle contient, entre autres, les éléments $a_1^{\lambda_1 + t_1 n} a_2^{\lambda_2 + t_2 n} \ldots a_k^{\lambda_k + t_k n}$ de G, quels que soient les entiers $t_1, t_2, \ldots, t_k$, et elle contient avec tout élément $a = f(a_1, a_2, \ldots, a_k)$ de G la classe entière des éléments de G conjugués à a.

En effet, quel que soit l'élément b de G, b peut être obtenu par composition finie d'éléments de A. Soit $b = g(a_1, a_2, \ldots, a_k)$. D'après la loi de composition des éléments d'un groupe libre, les deux éléments a et bab^{-1} sont de même degré par rapport à a_i, quel que soit $i = 1, 2, \ldots k$, Tout élément de G appartient à une classe $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ et à une seule puisque tout élément de G peut se mettre de façon unique sous la forme d'une composition finie réduite d'éléments de A et le groupe G est la réunion de toutes les classes $M^{(n)}_{\lambda_1\lambda_1\ldots\lambda_k}$ qui sont disjointes deux à deux.

Loi de composition des classes $M^{(n)}$. — Soient $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ et $M^{(n)}_{\mu_1\mu_2\ldots\mu_k}$ deux classes $M^{(n)}$ quelconques. Nous appelons *produit* de ces classes et nous désignons par le symbole $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}M^{(n)}_{\mu_1\mu_2\ldots\mu_k}$ l'ensemble des éléments de G de la forme ab,

$$a \in M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}, \qquad b \in M^{(n)}_{\mu_1\mu_2\ldots\mu_k}.$$

Proposition 1. — *Quelles que soient les deux classes* $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ *et* $M^{(n)}_{\mu_1\mu_2\ldots\mu_k}$, *on a*

$$M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}M^{(n)}_{\mu_1\mu_2\ldots\mu_k} = M^{(n)}_{\nu_1\nu_2\ldots\nu_k}$$

où ν_i *est le nombre de la suite* $0, 1, \ldots, n-1$ *qui satisfait la congruence*

$$\nu_i \equiv \lambda_i + \mu_i \pmod{n} \qquad (i = 1, 2, \ldots, k)$$

Démonstration. — Soit a un élément quelconque de la classe $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ et soit b un élément quelconque de la classe $M^{(n)}_{\mu_1\mu_2\ldots\mu_k}$. Soit u_i le degré de a par rapport à a_i et soit v_i celui de b par rapport à $a_i (i = 1, 2, \ldots, k)$. D'après la loi de composition des éléments d'un groupe libre, ab est de degré $u_i + v_i$ par rapport à a_i, quel que soit $i = 1, 2, \ldots, k$. Soit ν_i le nombre de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence $\nu_i \equiv u_i + v_i \pmod{n}$. Comme $a \in M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$, on a

$$u_i \equiv \lambda_i \pmod{n} \qquad (i = 1, 2, \ldots, k)$$

et comme $b \in M^{(n)}_{\mu_1\mu_2\ldots\mu_k}$, on a

$$v_i \equiv \mu_i \pmod{n} \qquad (i = 1, 2, \ldots, k).$$

Donc

$$\nu_i = \lambda_i + \mu_i \pmod{n}$$

et, d'après ce qui précède,

$$ab \in M^{(n)}_{\nu_1\nu_2\ldots\nu_k}.$$

Cela étant, quels que soient les éléments a de $M^{(n)}_{\lambda_1\lambda_1\ldots\lambda_k}$ et b de $M^{(n)}_{\mu_1\mu_2\ldots\mu_k}$, on a l'inclusion

$$(+) \qquad M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}M^{(n)}_{\mu_1\mu_2\ldots\mu_k} \subset M^{(n)}_{\nu_1\nu_2\ldots\nu_k}.$$

Montrons qu'on a aussi l'inclusion inverse. A cet effet, nous prouverons que pour tout élément fixe a de la classe $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ et pour tout élément c de la classe $M^{(n)}_{\nu_1\nu_2\ldots\nu_k}$ il existe un élément b de la classe $M^{(n)}_{\mu_1\mu_2\ldots\mu_k}$, tel que $ab = c$. En effet, comme G est un groupe dont a et c sont deux éléments, l'équation $ax = c$ admet une solution en G, notamment l'élément $b = a^{-1}c$. Soit $u_i(w_i)$ le degré de l'élément $a(c)$ par rapport à $a_i (i = 1, 2, \ldots, k)$. On a

$$u_i \equiv \lambda_i \pmod{n} \qquad \text{et} \qquad w_i \equiv \nu_i \pmod{n}.$$

L'élément a^{-1} de G est de degré $-u_i$ par rapport à $a_i (i = 1, 2, \ldots, k)$ et, par suite, il fait partie de la classe $M^{(n)}_{n-\lambda_1, n-\lambda_2, \ldots, n-\lambda_k}$, donc, d'après la première partie de la démonstration, $b \in M^{(n)}_{\mu_1 \mu_2 \ldots \mu_k}$. On a donc aussi l'inclusion

$$(++) \qquad M^{(n)}_{\nu_1 \nu_2 \ldots \nu_k} \subset M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k} M^{(n)}_{\mu_1 \mu_2 \ldots \mu_k}.$$

Des deux inclusions $(+)$ et $(++)$ découle l'égalité à démontrer.

Proposition 2. — *Deux classes* $M^{(n)}$ *quelconques sont des ensembles d'égale puissance.*

Démonstration. — Soient $M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k}$ et $M^{(n)}_{\mu_1 \mu_2 \ldots \mu_k}$ deux classes $M^{(n)}$ quelconques. Soit ν_i le nombre de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence

$$\nu_i \equiv \mu_i - \lambda_i \pmod{n} \qquad (i = 1, 2, \ldots k),$$

et soit c un élément quelconque de la classe $M^{(n)}_{\nu_1 \nu_2 \ldots \nu_k}$ et d un élément quelconque de la classe $M^{(n)}_{n-\nu_1, n-\nu_2, \ldots, n-\nu_k}$. Quels que soient l'ensemble E d'éléments de G et l'élément x de G, désignons par le symbole Ex l'ensemble des éléments yx de G, $y \in E$. Il ressort de la démonstration de la proposition 1 qu'on a les deux inclusions

$$M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k} c \subset M^{(n)}_{\mu_1 \mu_2 \ldots \mu_k} \qquad \text{et} \qquad M^{(n)}_{\mu_1 \mu_2 \ldots \mu_k} d \subset M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k},$$

inclusions qui démontrent que les deux ensembles $M^{(n)}_{\lambda_1 \lambda_1 \ldots \lambda_k}$ et $M^{(n)}_{\mu_1 \mu_1 \ldots \mu_k}$ sont bien d'égale puissance. Donc toutes les classes $M^{(n)}$ sont des ensembles d'égale puissance. C. Q. F. D.

Les groupes abéliens $\Gamma^{(n)}$ associés au groupe libre G (²). — Avec la loi de composition indiquée plus haut, loi qui est commutative et associative, les classes $M^{(n)}$ forment *un groupe abélien* $\Gamma^{(n)}$ *associé au groupe* G. La classe $M^{(n)}_{00 \ldots 0}$ constitue l'élément neutre de ce groupe et l'inverse d'une classe $M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k}$ est la classe $M^{(n)}_{n-\lambda_1, n-\lambda_2, \ldots, n-\lambda_k}$.

Proposition 3. — *Quels que soient les nombres* $\lambda_1, \lambda_2, \ldots, \lambda_k$ *de la suite* $0, 1, \ldots, n-1$ *la classse* $M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k}$ *envisagée comme élément du groupe* $\Gamma^{(n)}$ *est d'ordre* $\frac{n}{d}$, *où* d *est le p. g. c. d. des nombres* $n, \lambda_1, \lambda_2, \ldots, \lambda_k$. *En effet, soit* m

(²) On peut associer de la même façon un groupe abélien $\Gamma^{(n)}$ $(n = 2, 3, \ldots)$ à tout groupe non libre G engendré par un ensemble fini $A = \{a_1, a_2, \ldots, a_k\}$ d'éléments générateurs et dont chaque élément possède un degré fixe par rapport à tout élément de A et les propriétés de $\Gamma^{(n)}$ que nous établissons pour les groupes libres subsistent pour de tels groupes non libres.

l'ordre de cette classe et soit ν_i *le nombre de la suite* $0, 1, \ldots, n-1$ *qui satisfait la congruence*

$$\nu_i \equiv \frac{n}{d}\lambda_i \pmod{n} \qquad (i = 1, 2, \ldots, k)$$

D'après la loi de composition des classes $M^{(n)}$, on a

$$\left(M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}\right)^{\frac{n}{d}} = M^{(n)}_{\nu_1\nu_2\ldots\nu_k}.$$

Et comme $\frac{n}{d}\lambda_i \equiv 0 \pmod{n}$, il s'ensuit que

$$\nu_i \equiv 0 \pmod{n} \qquad (i = 1, 2, \ldots, k).$$

Donc $\left(M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}\right)^{\frac{n}{d}} \equiv M^{(n)}_{00\ldots0}$ et par suite, $\frac{n}{d}$ est un multiple de m. Montrons que $m = \frac{n}{d}$. En effet, supposons que $m < \frac{n}{d}$ et soit $\frac{n}{d} = n'm\,(n' > 1)$. Comme m est l'ordre de $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$, on doit avoir $m\lambda_i \equiv 0 \pmod{n}$, quel que soit $i = 1, 2, \ldots, k$ et, par suite, λ_i doit être un multiple de $\frac{n}{m}$ $(i = 1, 2, \ldots, k)$. Or $\frac{n}{m} = n'd$ et, par conséquent, le p. g. c. d. des nombres $n, \lambda_1, \lambda_2, \ldots, \lambda_k$ serait $\geqq n'd > d$ ce qui est contradictoire, Donc $m = \frac{n}{d}$. C. Q. F. D.

PROPOSITION 4. — *Le nombre minimum d'éléments générateurs du groupe* $\Gamma^{(n)}$ *est égal à* k.

Démonstration. — En effet, l'ordre de toute classe $M^{(n)}$ est un diviseur de n, il n'est donc pas supérieur à n. Et comme $\Gamma^{(n)}$ est un groupe abélien d'ordre n^k, le groupe $\Gamma^{(n)}$ ne saurait être engendré par moins de k éléments. D'autre part, il possède des systèmes de k éléments générateurs. Tel est, par exemple, le système formé des k classes $M_{10\ldots0}$, $M_{010\ldots0}$, $M_{00\ldots01}$. Le nombre minimum d'éléments générateurs du groupe $\Gamma^{(n)}$ est donc bien égal à k.

C. Q. F. D.

CLASSES $M^{(n)}$ INDÉPENDANTES ET DÉPENDANTES. — Soient $M^{(n)}_{\lambda_1^i\lambda_2^i\ldots\lambda_k^i}$ $(i = 1, 2, \ldots, t)$ $t \geqq 1$ classes $M^{(n)}$. Nous disons que ces classes sont indépendantes si l'égalité

$$\text{(I)} \qquad \left[M^{(n)}_{\lambda_1^1\lambda_2^1\ldots\lambda_k^1}\right]^{\alpha_1}\left[M^{(n)}_{\lambda_1^2\lambda_2^2\ldots\lambda_k^2}\right]^{\alpha_2}\cdots\left[M^{(n)}_{\lambda_1^t\lambda_2^t\ldots\lambda_k^t}\right]^{\alpha_t} = M^{(n)}_{00\ldots0},$$

où $\alpha_1, \alpha_2, \ldots, \alpha_t$ sont des entiers, implique que $\alpha_i \equiv 0 \pmod{n}$ quel que soit $i = 1, 2, \ldots, t$, et nous disons que les classes $M^{(n)}$ envisagées sont dépendantes ou liées s'il existe un système d'entiers $\alpha_1, \alpha_2, \ldots, \alpha_t$ dont l'un au moins n'est pas congru à 0 modulo n et pour lequel l'égalité (I) a lieu.

PROPOSITION 5. — *Soient* $M^{(n)}_{\lambda_1^i\lambda_2^i\ldots\lambda_k^i}$ $(i = 1, 2, \ldots, t, \ 1 \leqq t \leqq k)$ *t classes* $M^{(n)}$.

Si ces classes sont indépendantes, le rang de la matrice

$$\lambda = \begin{pmatrix} \lambda_1^1 & \lambda_1^2 & \dots & \lambda_1^t \\ \lambda_2^1 & \lambda_2^2 & \dots & \lambda_2^t \\ \dots & \dots & \dots & \dots \\ \lambda_k^1 & \lambda_k^2 & \dots & \lambda_k^t \end{pmatrix}$$

est égal à t.

Démonstration. — Si les t classes considérées sont indépendantes, l'égalité (I), où $\alpha_1, \alpha_2, \dots, \alpha_t$ désignent des entiers, implique que $\alpha_i \equiv 0 \pmod{n}$, quel que soit $i = 1, 2, \dots, t$. Or, d'après la loi de composition des classes $M^{(n)}$ et d'après l'égalité (I), $\alpha_1, \alpha_2, \dots, \alpha_t$ doivent satisfaire le système d'équations linéaires

$$(1) \qquad \begin{cases} \alpha_1 \lambda_1^1 + \alpha_2 \lambda_1^2 + \dots + \alpha_t \lambda_1^t = \tau_1 n, \\ \alpha_1 \lambda_2^1 + \alpha_2 \lambda_2^2 + \dots + \alpha_t \lambda_2^t = \tau_2 n, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_1 \lambda_k^1 + \alpha_2 \lambda_k^2 + \dots + \alpha_t \lambda_k^t = \tau_k n, \end{cases}$$

où $\tau_1, \tau_2, \dots, \tau_k$ sont des entiers.

C'est un système de k équations à $t \leqq k$ inconnues $\alpha_1, \alpha_2, \dots, \alpha_t$ et comme ce système n'admet que des solutions dans lesquelles toutes les inconnues sont des multiples de n, il s'ensuit que le rang du système (1) est nécessairement égal à t.

En effet, supposons le contraire et soit $r < t$ le rang du système considéré. Supposons pour fixer les idées que le déterminant principal de ce système est

$$\delta = \begin{vmatrix} \lambda_1^1 & \lambda_1^2 & \dots & \lambda_1^r \\ \lambda_2^1 & \lambda_2^2 & \dots & \lambda_2^r \\ \dots & \dots & \dots & \dots \\ \lambda_r^1 & \lambda_r^2 & \dots & \lambda_r^r \end{vmatrix}.$$

Il y a alors des inconnues et des équations non principales

Posons

$$\tau_1 = \tau_2 = \dots = \tau_k = 0.$$

Le système (1) est alors homogène, il est possible et admet une infinité de solutions. On peut attribuer à $\alpha_{r+1}, \dots, \alpha_t$ des valeurs arbitraires. Montrons qu'il existe des valeurs entières de $\alpha_1, \alpha_2, \dots, \alpha_t$ qui ne sont pas toutes $\equiv 0 \pmod{n}$, et qui constituent une solution du système envisagé. En effet, résolvons le système des équations principales par la règle de Cramer par rapport aux inconnues principales $\alpha_1, \alpha_2, \dots, \alpha_r$. Désignons par δ_{r+s}^j le déterminant qui se déduit de δ en y remplaçant la colonne de rang j $(j = 1, 2, \dots, r)$ par

$$\begin{cases} \lambda_1^{r+s} \\ \lambda_2^{r+s} \\ \dots \\ \lambda_r^{r+s} \end{cases} \qquad (s = 1, 2, \dots, t - r).$$

Il vient

$$\alpha_j = -\frac{\alpha_{r+1}\delta^j_{r+1} + \alpha_{r+2}\delta^j_{r+2} + \ldots + \alpha_t\delta^j_t}{\delta} \qquad (j = 1, 2, \ldots, r).$$

Si $\delta \not\equiv 0 \pmod{n}$ posons

$$\alpha_{r+1} = \ldots = \alpha_t = \delta.$$

On aura des valeurs entières de $\alpha_1, \alpha_2, \ldots, \alpha_t$ qui ne sont pas toutes $\equiv 0 \pmod{n}$.

Et si $\delta \equiv 0 \pmod{n}$, soit n^m la plus grande puissance de n qui est diviseur de δ. Si tous les déterminants δ^j_{r+s} sont des multiples de n^m et si

$$\delta = n^m\delta', \qquad \delta' \not\equiv 0 \pmod{n},$$

posons

$$\alpha_{r+1} = \ldots = \alpha_t = \delta'.$$

On aura de nouveau une solution $\alpha_1, \alpha_2, \ldots, \alpha_t$ du système considéré dans laquelle toutes les inconnues prennent des valeurs entières dont l'une au moins n'est pas $\equiv 0 \pmod{n}$.

Et si $\delta \equiv 0 \pmod{n}$ et $\delta = n^m\delta'$, où $\delta' \not\equiv 0 \pmod{n}$, mais si l'un au moins des déterminants δ^j_{r+s} n'est pas $\equiv 0 \pmod{n^m}$, soit $n^{m'}\delta''$ $[m' < m, \delta'' \not\equiv 0 \pmod{n}]$ le p. g. c. d. de δ et de tous les déterminants δ^j_{r+s} et soit $\delta^j_{r+s'} \not\equiv 0 \pmod{n^{m'+1}}$. Posons, dans ce cas

$$\alpha_{r+s'} = n^{m-m'}\frac{\delta'}{\delta''}, \qquad \alpha_{r+s} = 0 \qquad (s \neq s').$$

On obtiendra ainsi une solution entière en $\alpha_1, \ldots, \alpha_t$ du système d'équations considéré, solution dans laquelle l'un au moins des nombres $\alpha_1, \alpha_2, \ldots, \alpha_r$ n'est pas $\equiv 0 \pmod{n}$.

Donc, dans tous les cas, on est conduit à une contradiction.

Le raisonnement est tout à fait analogue et la conclusion subsiste quelles que soient les lignes et les colonnes de la matrice λ qui contribuent à former le déterminant principal δ d'ordre r du système considéré.

La condition énoncée est donc bien nécessaire.

C. Q. F. D.

Proposition 6. — *La condition nécessaire et suffisante pour que k classes $M^{(n)}_{\lambda^i_1\lambda^i_2\ldots\lambda^i_k}$ $(i = 1, 2, \ldots, k)$ soient indépendantes, c'est que le p. c. g. d. de n et du déterminant $|\lambda^i_j|$ soit égal à 1.*

Démonstration. — *La condition est nécessaire.* — En effet, supposons que les k classes $M^{(n)}_{\lambda^i_1\lambda^i_2\ldots\lambda^i_k}$ sont indépendantes. Alors, d'après la proposition 5, le déterminant d'ordre k : $\delta = |\lambda^i_j|$ est $\neq 0$.

Si donc $\alpha_1, \alpha_2, \ldots, \alpha_k$ sont des entiers tels que

$$(2) \qquad [M^{(n)}_{\lambda^1_1\lambda^1_2\ldots\lambda^1_k}]^{\alpha_1}[M^{(n)}_{\lambda^2_1\lambda^2_2\ldots\lambda^2_k}]^{\alpha_2}\ldots[M^{(n)}_{\lambda^k_1\lambda^k_2\ldots\lambda^k_k}]^{\alpha_k} = M^{(n)}_{00\ldots0},$$

chacun des nombres $\alpha_1, \alpha_2, \ldots, \alpha_k$ est $\equiv 0 \pmod{n}$ et, d'après la loi de composition des classes $M^{(n)}$ et l'égalité (2), $\alpha_1, \alpha_2, \ldots, \alpha_k$ sont racines du système d'équations linéaires

$$(3) \qquad \begin{cases} \alpha_1\lambda_1^1 + \alpha_2\lambda_1^2 + \ldots + \alpha_k\lambda_1^k = \tau_1 n, \\ \alpha_1\lambda_2^1 + \alpha_2\lambda_2^2 + \ldots + \alpha_k\lambda_2^k = \tau_2 n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_1\lambda_k^1 + \alpha_2\lambda_k^2 + \ldots + \alpha_k\lambda_k^k = \tau_k n, \end{cases}$$

où $\tau_1, \tau_2, \ldots, \tau_k$ désignent des entiers.

Comme le rang de ce système est égal à k, c'est un système régulier qui peut être résolu par la règle de Cramer. Désignons par δ_i le déterminant qui se déduit de δ en remplaçant sa $i^{\text{ième}}$ colonne par $\begin{cases} \tau_1 \\ \tau_2 \\ \ldots \\ \tau_k \end{cases}$. On a

$$\alpha_i = n\frac{\delta_i}{\delta} \qquad (i = 1, 2, \ldots, k).$$

Soit d le p. g. c. d. de n et de δ et soit Λ_j^i le coefficient de λ_j^i dans le développement du déterminant δ.

Deux cas peuvent se présenter :

a. Il existe un coefficient Λ_j^i (au moins) qui n'est pas un multiple de d. Posons alors

$$\tau_j = \frac{\delta}{d}, \qquad \tau_{j'} = 0$$

quel que soit l'indice $j' \neq j$ de la suite 1, 2, ..., k. On obtient pour $\alpha_1, \alpha_2, \ldots, \alpha_k$ les valeurs

$$\alpha_1 = \frac{n}{d}\Lambda_j^1, \qquad \alpha_2 = \frac{n}{d}\Lambda_j^2, \qquad \ldots \qquad \alpha_k = \frac{n}{d}\Lambda_j^k$$

et comme Λ_j^i n'est pas un multiple de d, $\alpha_i \not\equiv 0 \pmod{n}$, ce qui est contradictoire, les classes $M^{(n)}$ considérées, étant, par hypothèse, indépendantes.

b. Tous les coefficients Λ_j^i sont des multiples de d. Soit p le plus petit diviseur premier de d. Il est alors aussi diviseur de tous les Λ_j^i. Soit p^m la plus grande puissance de p commune à tous les Λ_j^i ($m \geqq 1$). Il existe donc un coefficient (au moins) Λ_j^i qui n'est pas divisible par p^{m+1}. Considérons le déterminant $\Delta = |\Lambda_j^i|$ adjoint de δ. Comme chaque élément de Δ est divisible par p^m, le déterminant Δ qui est d'ordre k est divisible par p^{mk}. Or Δ est lié à son adjoint δ par l'égalité $\Delta = \delta^{k-1}$. Donc δ^{k-1} est à son tour divisible par p^{mk}. Et comme les nombres k et $k-1$ sont premiers entre eux et que p est un nombre premier $\geqq 2$, il s'ensuit que $m \equiv 0 \pmod{k-1}$. Soit $m = m'(k-1)$, ($m' \geqq 1$). Le déterminant δ est donc divisible par $p^{m'k} = p^{m+m'}$.

Posons dans ce cas

$$\tau_j = \frac{\delta}{p^{m+1}}, \qquad \tau_{j'} = 0,\ j' = 1, 2, \ldots, k, \text{ mais } j' \neq j.$$

Il vient

$$\alpha_1 = \frac{n}{p}\frac{\Lambda_j^1}{p^m}, \quad \ldots \quad \alpha_i = \frac{n}{p}\frac{\Lambda_j^i}{p^m}, \quad \ldots \quad \alpha_k = \frac{n}{p}\frac{\Lambda_j^k}{p^m},$$

ce qui fournit un système de valeurs entières de $\alpha_1, \alpha_2, \ldots, \alpha_k$ dont l'une au moins $\alpha_i \not\equiv 0 \pmod{n}$ et qui satisfont la relation (2), ce qui est contradictoire. On ne saurait donc avoir $d > 1$ et la condition énoncée est bien nécessaire.

La condition est suffisante. — En effet, supposons que le p. g. c. d. de n et du déterminant $\delta = |\lambda_j^i|$ est égal à 1. Montrons que les classes $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$ sont alors indépendantes. En effet, comme $D(n, \delta) = 1$, on a $\delta \neq 0$ et par suite, le système (3) d'équations linéaires en $\alpha_1, \alpha_2, \ldots, \alpha_k$, où $\tau_1, \tau_2, \ldots, \tau_k$ désignent des entiers, est un système régulier dont la solution est donnée par la règle de Cramer. On a notamment

$$\alpha_i = n\,\frac{\tau_1\Lambda_1^i + \tau_2\Lambda_2^i + \ldots + \tau_k\Lambda_k^i}{\delta} \qquad (i = 1, 2, \ldots, k). \tag{4}$$

Soit a le plus grand commun diviseur de δ et de tous les coefficients Λ_j^i. Pour avoir une solution entière en α_i du système d'équations (3) il convient de choisir les nombres $\tau_1, \tau_2, \ldots, \tau_k$ de façon que

$$\tau_1\Lambda_1^i + \tau_2\Lambda_2^i + \ldots + \tau_k\Lambda_k^i \equiv 0 \pmod{\delta} \qquad (i = 1, 2, \ldots, k). \tag{5}$$

On obtient, par exemple, une telle solution en posant

$$\tau_j = \frac{\delta}{a} \qquad (j = 1, 2, \ldots, k).$$

Mais comme n et δ sont premiers entre eux, il découle des formules (4) que toute solution entière en α_i du système (3) fournit pour toutes les inconnues du système des valeurs $\equiv 0 \pmod{n}$, donc les classes $M^{(n)}$ sont indépendantes et la condition énoncée est bien suffisante.

C. Q. F. D.

Remarque 1. — On démontre sans peine que la condition nécessaire et suffisante pour que t classes $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$ $(i = 1, 2, \ldots, t,\ 1 \leqq t \leqq k)$ soient dépendantes, c'est que le p. g. c. d. de n et de tous les déterminants d'ordre t qu'on peut former à partir de la matrice

$$\begin{pmatrix} \lambda_1^1 & \lambda_1^2 & \ldots & \lambda_1^t \\ \lambda_2^1 & \lambda_2^2 & \ldots & \lambda_2^t \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_k^1 & \lambda_k^2 & \ldots & \lambda_k^t \end{pmatrix},$$

en prenant les éléments communs à ses t colonnes et à t lignes quelconques, soit > 1. La démonstration de cette proposition est tout à fait analogue à celle de la proposition 7 de notre Note (*Un problème de structure des groupes d'ardre fini*) ([3]).

([3]) *J. Math. pures et appl.*, t. 35, 1956, p. 149 à 155.

Proposition 7. — *Quel que soit l'entier $t > k$, t classes $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$ $(i = 1, 2, \ldots, t)$ sont toujours dépendantes.*

Démonstration. — Soit $\mathfrak{M}$ l'ensemble des classes $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$ $(i = 1, 2, \ldots, t)$. Pour établir la proposition 7, nous montrerons qu'il existe t entiers $\alpha_1, \alpha_2, \ldots, \alpha_t$, dont l'un au moins n'est pas un multiple de n, et tels qu'on a l'égalité

$$\text{(I)} \qquad [M^{(n)}_{\lambda_1^1 \lambda_2^1 \ldots \lambda_k^1}]^{\alpha_1} [M^{(n)}_{\lambda_1^2 \lambda_2^2 \ldots \lambda_k^2}]^{\alpha_2} \ldots [M^{(n)}_{\lambda_1^t \lambda_2^t \ldots \lambda_k^t}]^{\alpha_t} = M^{(n)}_{00\ldots 0}.$$

Soient $\alpha_1, \alpha_2, \ldots, \alpha_t$, t entiers, qui vérifient l'égalité (I). Cette égalité implique le système de k équations à t inconnues (1), où $\tau_1, \tau_2, \ldots, \tau_k$ désignent des entiers (*voir* proposition 5).

Soit

$$\Lambda = \begin{pmatrix} \lambda_1^1 & \lambda_1^2 & \ldots & \lambda_1^t \\ \lambda_2^1 & \lambda_2^2 & \ldots & \lambda_2^t \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_k^1 & \lambda_k^2 & \ldots & \lambda_k^t \end{pmatrix}$$

la matrice des coefficients des inconnues de ce système. Comme $t > k$, le rang r de cette matrice est $\leqq k$ et, par suite, ses t colonnes sont liées linéairement. Il existe donc des nombres $\alpha_1, \alpha_2, \ldots, \alpha_t$ non tous nuls tels que

$$(6) \qquad \alpha_1 \lambda_i^1 + \alpha_2 \lambda_i^2 + \ldots + \alpha_t \lambda_i^t = 0 \qquad (i = 1, 2, \ldots, k).$$

Envisageons tous les déterminants d'ordre r qu'on peut former avec les éléments communs à r lignes et à r colonnes quelconques de la matrice Λ. Si l'un au moins de ces déterminants n'est pas congru à o modulo n, prenons un tel déterminant Δ pour déterminant principal du système (6). Supposons, pour fixer les idées, que

$$\Delta = \begin{vmatrix} \lambda_1^1 & \lambda_1^2 & \ldots & \lambda_1^r \\ \lambda_2^1 & \lambda_2^2 & \ldots & \lambda_2^r \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_r^1 & \lambda_r^2 & \ldots & \lambda_r^r \end{vmatrix}.$$

Les inconnues $\alpha_1, \alpha_2, \ldots, \alpha_r$ sont alors principales ; on peut attribuer à $\alpha_{r+1}, \ldots, \alpha_t$ des valeurs arbitraires, les r premières équations du système (6) sont principales et l'on obtient la solution du système (6) en résolvant le système formé par les équations principales. Posons dans les équations principales du système (6)

$$\alpha_{r+1} = \ldots = \alpha_t = \Delta$$

et résolvons le système obtenu par rapport à $\alpha_1, \alpha_2, \ldots, \alpha_r$ par la règle de Cramer. On obtient ainsi des valeurs entières de ces r inconnues et les t nombres $\alpha_1, \alpha_2, \ldots, \alpha_t$ dont les $t - r$ derniers ne sont pas $\equiv 0 \pmod{n}$ satisfont à l'égalité (I). Donc, dans ce cas, les classes de l'ensemble $\mathfrak{M}$ sont bien liées.

Supposons maintenant que tous les déterminants d'ordre r qu'on peut déduire de la matrice Λ sont $\equiv 0 \pmod{n}$. L'un au moins de ces déterminants est $\not\equiv 0$, puisque r est le rang du système (1). Envisageons r lignes de la matrice Λ dont les éléments contribuent à former un déterminant d'ordre r non nul. Supposons, pour fixer les idées, que ce sont les r premières lignes de la matrice Λ. Soient $i_1, i_2, \ldots, i_r$ r nombres distincts de la suite $1, 2, \ldots, t$ et soit $\Delta_{i_1 i_2 \ldots, i_t}$ le déterminant formé des éléments communs aux r premières lignes et aux colonnes de rangs $i_1, i_2, \ldots, i_r$ de Λ. Si $\Delta_{i_1 i_2 \ldots i_r} \not\equiv 0$, soit

$$\Delta_{i_1 i_2 \ldots i_r} = \beta_{i_1 i_2 \ldots i_r} n^{\gamma_{i_1 i_2 \ldots i_r}},$$

où l'entier $\beta_{i_1 i_2 \ldots i_r} \not\equiv 0 \pmod{n}$ et $\gamma_{i_1 i_2 \ldots i_r}$ est un entier $\geqq 1$. Prenons alors pour déterminant principal du système (6) un déterminant $\Delta_{i_1 i_2 \ldots i_r}$ pour lequel le nombre $\gamma_{i_1 i_2 \ldots i_r}$ est minimum. Soit Δ ce déterminant principal et soit, pour fixer les idées,

$$\Delta = \begin{vmatrix} \lambda_1^1 & \ldots & \lambda_r^1 \\ \ldots & \ldots & \ldots \\ \lambda_1^r & \ldots & \lambda_r^r \end{vmatrix};$$

$\alpha_1, \alpha_2, \ldots, \alpha_r$ seront donc de nouveau les inconnues principales et l'on peut attribuer à $\alpha_{r+1}, \ldots, \alpha_t$ des valeurs arbitraires. Posons, dans le système (7) des équations principales

$$\alpha_{r+1} = \ldots = \alpha_t = \beta_{i_1 i_2 \ldots i_r}.$$

(7) est alors un système régulier qui possède une solution unique en $\alpha_1, \ldots, \alpha_r$ donnée par la règle de Cramer et l'on voit sans peine que cette solution est entière. Les nombres $\alpha_1, \alpha_2, \ldots, \alpha_t$ vérifient l'égalité (I) et les nombres $\alpha_{r+1}, \ldots, \alpha_t$ ne sont pas congrus à 0 modulo n. Donc, dans ce cas aussi, les classes de l'ensemble $\mathfrak{M}$ sont dépendantes.

Le raisonnement est tout à fait analogue et la conclusion subsiste quelles que soient les rangées de la matrice Λ qui contribuent à former le déterminant principal du système (6). La proposition 7 est donc démontrée.

Remarque 2. — Si dans un système de classes $M^{(n)}$ figure la classe nulle, les classes sont dépendantes. En effet, soit $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$ $(i = 1, 2, \ldots, t)$ un ensemble de classes $M^{(n)}$ parmi lesquelles figure la classe nulle $M^{(n)}_{\lambda_1^1 \lambda_2^1 \ldots \lambda_k^1} = M^{(n)}_{00 \ldots 0}$. Alors les t classes envisagées sont dépendantes. En effet, posons

$$\alpha_1 = 1 \qquad \alpha_i = 0, \qquad (i = 2, \ldots, t).$$

On a la relation

$$\text{(I)} \qquad [M^{(n)}_{\lambda_1^1 \lambda_2^1 \ldots \lambda_k^1}]^{\alpha_1} [M^{(n)}_{\lambda_1^2 \lambda_2^2 \ldots \lambda_k^2}]^{\alpha_2} \ldots [M^{(n)}_{\lambda_1^t \lambda_2^t \ldots \lambda_k^t}]^{\alpha_t} = M^{(n)}_{00 \ldots 0}.$$

avec les exposants qui ne sont pas tous $\equiv 0 \pmod{n}$, ce qui démontre que les classes $M^{(n)}$ considérées sont bien liées.

D'autre part, si t classes $M^{(n)}$ sont dépendantes, en leur ajoutant une ou un nombre fini quelconque de classes $M^{(n)}$ quelconques, on obtient de nouveau un système de classes dépendantes. Pour s'en convaincre, il suffit d'ajouter aux nombres $\alpha_1, \alpha_2, \ldots, \alpha_t$ dont l'un au moins n'est pas $\equiv 0 \pmod{n}$ et pour lesquels on a l'égalité (I), les nombres $\alpha_{t+1} = \ldots = 0$. On aura

$$\text{(II)} \qquad \left[\mathrm{M}^{(n)}_{\lambda^1_1\lambda^1_2\ldots\lambda^1_k}\right]^{\alpha_1}\ldots\left[\mathrm{M}^{(n)}_{\lambda^t_1\lambda^t_2\ldots\lambda^t_k}\right]^{\alpha_t}\left[\mathrm{M}^{(n)}_{\lambda^{t+1}_1\lambda^{t+1}_2\ldots\lambda^{t+1}_k}\right]^{\alpha_{t+1}}\ldots = \mathrm{M}^{(n)}_{00\ldots 0},$$

ce qui démontre que l'ensemble des classes $\mathrm{M}^{(n)}_{\lambda^i_1\lambda^i_2\ldots\lambda^i_k} (i = 1, 2, \ldots, t, t+1, \ldots)$ sont liées.

Proposition 8. — *La condition nécessaire et suffisante pour que k classes $\mathrm{M}^{(n)}_{\lambda^i_1\lambda^i_2\ldots\lambda^i_k} (i = 1, 2, \ldots, k)$ constituent une base du groupe $\Gamma^{(n)}$, c'est que ces k classes soient indépendantes.*

Démonstration. — La condition est nécessaire. — En effet, si les classes considérées constituent une base de $\Gamma^{(n)}$ en composant ces k classes on obtient les n^k classes $\mathrm{M}^{(n)}$ qui forment la totalité des éléments de $\Gamma^{(n)}$. Or, d'après la loi de composition des classes $\mathrm{M}^{(n)}$ qui est commutative et du fait que toute classe $\mathrm{M}^{(n)}$ envisagée comme élément de $\Gamma^{(n)}$ est d'ordre $\leqq n$, il s'ensuit qu'elles ne peuvent être génératrices du groupe $\Gamma^{(n)}$ que si elles sont indépendantes, ce qui implique, entre autres, que chacune de ces classes est d'ordre n. La condition énoncée est donc bien nécessaire.

La condition est suffisante. — En effet, supposons que les k classes données sont indépendantes. Chacune de ces classes considérée comme élément de $\Gamma^{(n)}$ est donc d'ordre n et les classes

$$\left[\mathrm{M}^{(n)}_{\lambda^1_1\lambda^1_2\ldots\lambda^1_k}\right]^{\alpha_1}\left[\mathrm{M}^{(n)}_{\lambda^2_1\lambda^2_2\ldots\lambda^2_k}\right]^{\alpha_2}\ldots\left[\mathrm{M}^{(n)}_{\lambda^k_1\lambda^k_2\ldots\lambda^k_k}\right]^{\alpha_k},$$

où chacun des entiers $\alpha_1, \alpha_2, \ldots, \alpha_k$ parcourt la suite des valeurs $0, 1, \ldots, n-1$, sont toutes distinctes. Ces classes sont au nombre de n^k et, par suite, les k classes données forment bien une base de $\Gamma^{(n)}$ et la condition énoncée est aussi suffisante.

C. Q. F. D.

Proposition 9. — *Si le groupe G (4) possède un système fini $A = \{a_1\ a_2, \ldots, a_k\}$ d'éléments générateurs, tel que tout élément du groupe G possède un degré fixe par rapport à chacun des éléments $a_i = (i = 1, 2, \ldots, k)$ le nombre k d'éléments qui constituent le système générateur A est minimum et tout élément de G possède un degré fixe par rapport à chaque élément de tout autre système générateur de G : $B = \{b_1, b_2, \ldots, b_k\}$ formé lui aussi de k éléments.*

Démonstration. — Soit A un système générateur du groupe G et supposons que chaque élément de G a un degré fixe par rapport à tout élément de A. Soit c un élément quelconque de G et soit u_i son degré fixe par rapport à

(4) Pas nécessairement libre. *Voir* Note (2) en bas de la page 7.

$a_i (i=1, 2, \ldots, k)$. Un système générateur de G ne saurait être formé de moins de k éléments. En effet, tout élément de G appartient comme nous savons à une classe $M^{(n)}$ et à une seule. Quel que soit le système générateur de G, on doit pouvoir, par composition finie de ses éléments, obtenir des éléments de toute classe $M^{(n)}$. Or le groupe $\Gamma^{(n)}$ est à base minimum d'ordre k et, par suite, aucun système générateur du groupe G ne saurait être formé de moins de k éléments.

Soit à présent $B=\{b_1, b_2, \ldots, b_k\}$ un second système générateur de G, formé lui aussi de k éléments. Soit encore c un élément quelconque de G. Soit u_i son degré (fixe) par rapport à $a_i (i=1, 2, \ldots, k)$. Comme B est un système générateur de G, c peut être obtenu par composition finie des éléments de B. Soit

$$(+) \qquad c=f(b_1, b_2, \ldots, b_k)$$

une telle composition et soit v_i le degré de f par rapport à $b_i (i=1, 2, \ldots, b_k)$. Chacun des éléments b_i en tant qu'élément de G possède un degré fixe par rapport à tout élément de A et comme A est un système générateur de G, chacun des éléments b_i peut être obtenu par composition finie des éléments de A. Soit

$$(++) \qquad b_i=f_i(a_1, a_2, \ldots, a_k)$$

et soit w_j^i le degré (fixe) de b_i par rapport à $a_j (i, j=1, 2, \ldots, k)$. Remplaçons dans l'expression $(+)$ chacun des b_i par son expression $(++)$. Il vient

$$c=f[f_1(a_1, a_2, \ldots, a_k), f_2(a_1, a_2, \ldots, a_k), \ldots, f_k(a_1, a_2, \ldots, a_k)].$$

Le second membre de cette égalité est de degré $v_1 w_j^1+v_2 w_j^2+\ldots+v_k w_j^k$ par rapport à $a_j (j=1, 2, \ldots, k)$. Et comme c possède un degré fixe u_j par rapport à a_j, quel que soit $j=1, 2, \ldots, k$. les nombres $v_1, v_2, \ldots, v_k$ vérifient le système d'équations linéaires

$$(+++) \qquad v_1 w_j^1+v_2 w_j^2+\ldots+v_k w_j^k=u_j \qquad (j=1, 2, \ldots, k).$$

Les éléments $b_1, b_2, \ldots, b_k$ en tant qu'éléments générateurs de G font partie de k classes $M^{(n)}$. Soit $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$ la classe $M^{(n)}$ qui contient l'élément $b_i (i=1, 2, \ldots, k)$. Comme ces classes sont indépendantes, le p. g. c. d. de n et du déterminant $|\lambda_j^i|$ est égal à 1, donc le déterminant $|\lambda_j^i|$ est $\neq 0$ et il n'est pas congru à 0 modulo n. Or

$$|w_j^i| \equiv |\lambda_j^i| \pmod{n}, \qquad \text{donc} \quad |w_j^i| \neq 0.$$

Le système d'équations $(+++)$ est donc régulier et il possède une solution unique en $v_1, v_2, \ldots, v_k$. On voit donc bien que quel que soit le système B générateur de G, formé de k éléments, tout élément de G a un degré fixe par rapport à chaque élément de B. La proposition 9 est donc démontrée.

Soit à présent G un groupe libre qui possède des systèmes finis d'éléments générateurs, soit k le nombre minimum d'éléments générateurs de G. Nous savons que tout élément de G possède un degré fixe par rapport à tout élément d'un système générateur minimum.

PROPOSITION 10. — *Quels que soient les deux systèmes générateurs minima*

$$A=\{a_1, a_2, \ldots, a_k\} \quad \text{et} \quad B=\{b_1, b_2, \ldots, b_k\}$$

du groupe G, on a

$$b_i=f_i(a_1, a_2, \ldots, a_k) \qquad (i=1, 2, \ldots, k),$$

où f_i est une composition finie réduite des éléments $a_1, a_2, \ldots, a_k$, de degré fixe w^i_j par rapport à $a_j (j=1, 2, \ldots, k)$ et le déterminant $|w^i_j|$ est toujours égal à $+1$ ou à -1. D'autre part, quel que soit l'entier $n \geqq 2$, si l'on répartit les éléments de G en classes $\mathrm{M}^{(n)}$ relatives à ce nombre n, les éléments b_i font partie de k classes $\mathrm{M}^{(n)}$ indépendantes et si $b_i \in \mathrm{M}^{(n)}_{\lambda^i_1\lambda^i_2\ldots\lambda^i_k}$ $(i=1, 2, \ldots, k)$, le déterminant $|\lambda^i_j|$, d'ordre k, est congru à $+1$ ou à -1 modulo n.

Démonstration. — Pour établir la première partie de cette proposition, reprenons la démonstration de la proposition 9. Un élément quelconque c de G est de degré fixe u_i par rapport à a_i et de degré fixe v_i par rapport à $b_i (i=1, 2, \ldots, k)$. Soit w^i_j le degré fixe de b_i par rapport à $a_j (i, j=1, 2, \ldots, k)$. Nous avons vu que les nombres $v_1, v_2, \ldots, v_k$ doivent satisfaire le système d'équations (+++) qui est un système de Cramer. La résolution du système (+++) par la règle de Cramer donne

$$(++++) \qquad v_i=\frac{u_1 \mathrm{W}^i_1+u_2 \mathrm{W}^i_2+\ldots+u_k \mathrm{W}^i_k}{|w^i_j|} \qquad (i=1, 2, \ldots, k),$$

où W^i_j est le coefficient de w^i_j dans le développement du déterminant $|w^i_j|$. La formule (++++) doit donner des valeurs entières pour $v_1, v_2, \ldots, v_k$, condition qui est imposée par la nature des nombres v_i, et cela quels que soient les entiers $u_1, u_2, \ldots, u_k$. Or G étant un groupe libre, les degrés d'un élément quelconque c de G par rapport aux éléments de A peuvent être des entiers quelconques. Donc pour que (++++) donne pour v_i des valeurs entières quels que soient $u_1, u_2, \ldots, u_k$ (qui sont des entiers), chacun des coefficients W^i_j doit être un multiple de $|w^i_j|$. Mais alors le déterminant $|\mathrm{W}^i_j|$, adjoint de $|w^i_j|$, doit être un multiple de $|w^i_j|^k$, puisque c'est un déterminant d'ordre k dont chaque rangée est un multiple de $|w^i_j|$. Or $\mathrm{W}^i_j=|w^i_j|^{k-1}$. Donc $|w^i_j|^{k-1}$ qui est un entier doit être un multiple de $|w^i_j|^k$, ce qui n'est possible que si $|w^i_j|$ est égal à $+1$ ou à -1.

Soit à présent n un entier quelconque $\geqq 2$. Répartissons les éléments de G en classes $\mathrm{M}^{(n)}$ relatives à ce nombre n. Soit $\mathrm{M}^{(n)}_{\lambda^i_1\lambda^i_2\ldots\lambda^i_k}$ celle de ces classes qui contient l'élément b_i de $B (i=1, 2, \ldots, k)$. Comme B est un système générateur minimum de G, les classes $\mathrm{M}^{(n)}_{\lambda^i_1\lambda^i_2\ldots\lambda^i_k}$ sont indépendantes et, d'après ce qu'on a vu dans la démonstration de la proposition 9, $|\lambda_j^i| \equiv |w_j^i|$ (mod n). Et comme $|w_j^i| = +1$ ou -1, on a bien

$$|\lambda_j^i| \equiv \varepsilon \pmod{n}, \qquad \text{où} \quad \varepsilon = +1 \quad \text{ou} \quad -1.$$

C. Q. F. D.

Remarque 3. — Bien que le déterminant $|\lambda_j^i|$ soit toujours $\equiv \varepsilon \pmod{n}$, $\varepsilon = +1$ ou -1, la valeur numérique de ce déterminant peut varier avec n et, en général, elle n'est pas égale à ε. En voici un exemple. Soit G un groupe libre à base du second ordre engendré par les deux éléments libres a_1 et a_2. Soit b_1, b_2 une seconde base de G définie par les formules

$$b_1 = [(a_1 a_2)^3 a_1 (a_1 a_2)^4]^7 a_1 a_2 [(a_1 a_2)^3 a_1 (a_1 a_2)^4]^{10}, \qquad b_2 = (a_1 a_2)^3 a_1 (a_1 a_2)^4.$$

Pour vérifier que b_1, b_2 est bien une base de G, il suffit de montrer que a_1 et a_2 peuvent être obtenus par composition finie de b_1 et de b_2. En effet, on a successivement

$$b_2^{-7} b_1 b_2^{-10} = a_1 a_2, \qquad (a_1 a_2)^{-3} b_2 (a_1 a_2)^{-4} = a_1, \qquad a_1^{-1}(a_1 a_2) = a_2.$$

Donc b_1, b_2 est bien une base de G. b_1 est de degré 137 par rapport à a_1 et de degré 120 par rapport à a_2, b_2 est de degré 8 par rapport à a_1 et de degré 7 par rapport à a_2.

Le déterminant

$$|w_j^i| = \begin{vmatrix} 137 & 120 \\ 8 & 7 \end{vmatrix} = -1.$$

Prenons $n = 5$. On a

$$|\lambda_j^i| = \begin{vmatrix} 2 & 0 \\ 3 & 2 \end{vmatrix} = 4,$$

il est $\equiv -1 \pmod{5}$.

Prenons maintenant $n = 21$. Alors

$$|\lambda_j^i| = \begin{vmatrix} 11 & 15 \\ 8 & 7 \end{vmatrix} = -43 \equiv -1 \pmod{21}.$$

Remarque 4. — Il ressort de la proposition 10 que quels que soient les systèmes générateurs minima

$$A = \{a_1, a_2, \ldots, a_k\} \qquad \text{et} \qquad B = \{b_1, b_2, \ldots, b_k\}$$

d'un groupe libre G ayant un nombre fini d'éléments générateurs, si b_i est de degré w_j^i par rapport à a_j, quels que soient i et j de la suite $1, 2, \ldots, k$, le déterminant $|w_j^i|$ est égal à $+1$ ou à -1. On peut le démontrer de la façon suivante. Soit n un entier ≥ 2 quelconque. Soit $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$ la classe $M^{(n)}$ qui contient $b_i (i = 1, 2, \ldots, k)$.

On a

$$(+) \qquad |w_j^i| \equiv |\lambda_j^i| \pmod{n}.$$

Comme B est une base de G, les n classes $M^{(n)}_{\lambda_1^i\lambda_2^i\ldots\lambda_k^i}$ sont indépendantes. Donc, d'après la proposition 6, le p. g. c. d. de n et de $|\lambda_j^i|$ est égal à 1 et, par conséquent, $|\lambda_j^i| \neq 0$ et $|\lambda_j^i| \not\equiv 0 \pmod{n}$. Il s'ensuit, d'après (+), que $|\omega_j^i| \neq 0$, $\omega_j^i \not\equiv 0 \pmod{n}$ et que le p. g. c. d. de $|\omega_j^i|$ et de n est aussi égal à 1. Cela étant, quel que soit l'entier $n = 2, 3, \ldots, |\omega_j^i|$ qui est un entier non nul ne peut être égal qu'à $+1$ ou à -1.

C. Q. F. D.

Remarque 5. — Quel que soit l'entier $n \geqq 2$, aucune base du groupe libre G ne saurait contenir un élément de la classe nulle $M^{(n)}_{00\ldots0}$. En effet, soit $A = \{a_1, a_2, \ldots, a_k\}$ une base de G. D'après ce qui précède, les éléments de A doivent faire partie de k classes indépendantes $M^{(n)}_{\lambda_1^i\lambda_2^i\ldots\lambda_k^i}$ $(i = 1, 2, \ldots, k)$. Or un ensemble de classes $M^{(n)}$ qui contient la classe $M^{(n)}_{00\ldots0}$ est dépendant, d'après la remarque 2.

D'autre part, aucun vrai sous-ensemble de A ne saurait être composé d'éléments de G qui font partie de classes $M^{(n)}$ dépendantes, puisque les classes $M^{(n)}_{\lambda_1^i\lambda_2^i\ldots\lambda_k^i}$ comprenant, chacune, un élément et un seul de A sont indépendantes et que tout ensemble de k classes $M^{(n)}$ dont $k' < k$ sont dépendantes est lui-même dépendant, d'après la remarque 2. Donc, d'après la proposition 5, quelles que soient les $k' < k$ classes $M^{(n)}_{\lambda_1^i\lambda_2^i\ldots\lambda_k^i}$ $(i = i_1, i_2, \ldots, i_{k'})$, le rang de la matrice

$$\begin{pmatrix} \lambda_1^{i_1} & \lambda_1^{i_2} & \ldots & \lambda_1^{i_{k'}} \\ \lambda_2^{i_1} & \lambda_2^{i_2} & \ldots & \lambda_2^{i_{k'}} \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_k^{i_1} & \lambda_k^{i_2} & \ldots & \lambda_k^{i_{k'}} \end{pmatrix}$$

est égal à k'.

Remarque 6. — Soit G un groupe libre engendré par un ensemble fini A d'éléments générateurs libres, soit n un entier $\geqq 2$ et soit $B = \{b_1, b_2, \ldots, b_k\}$ une seconde base quelconque de G. Répartissons les éléments de G en classes d'équivalence $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ en partant de la base A. Les éléments de B font alors partie de k classes $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ indépendantes. En effet, comme B est une base de G, tous les éléments de chaque classe $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ s'obtiennent par composition finie d'éléments de B et, par conséquent, les classes $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ qui contiennent les éléments de B sont génératrices du groupe $\Gamma^{(n)}$. Or pour cela il faut et il suffit, d'après la proposition 8, que ces k classes soient indépendantes.

PROPOSITION 11. — *Soit G un groupe libre engendré par un ensemble $A = \{a_1, a_2, \ldots, a_k\}$ d'éléments générateurs libres. Soit n un entier $\geqq 2$ et soit $\Gamma^{(n)}$ le groupe abélien d'ordre n^k associé à G. Quel que soit le sous-groupe γ du groupe $\Gamma^{(n)}$, la réunion des éléments de G contenus dans les classes $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ qui sont les éléments de $\Gamma^{(n)}$ est un sous-groupe invariant de G.*

Démonstration. — Soit γ un sous-groupe quelconque du groupe $\Gamma^{(n)}$, soit t

l'ordre de γ et soient $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$ ($i = 1, 2, \ldots, t$), les éléments de ce groupe. Soit

$$g = \bigcup_{i=1}^{t} M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_1^i}.$$

C'est un sous-ensemble de G. Montrons que G est un groupe. En effet, soient a et b deux éléments quelconques de g, ils font donc partie de classes $M^{(n)}$-éléments de γ. Soit

$$a \in M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i} \qquad \text{et} \qquad b \in M^{(n)}_{\lambda_1^j \lambda_2^j \ldots \lambda_k^j}.$$

Comme γ est un groupe, le produit des deux classes $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$, $M^{(n)}_{\lambda_1^j \lambda_2^j \ldots \lambda_k^j}$ est aussi un élément de γ et ce produit contient l'élément ab. Donc $ab \in g$. D'autre part, quel que soit l'élément a de g, il est contenu dans une classe $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$ de γ et comme γ est un groupe, il contient, avec la classe $M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}$, la classe inverse $M^{(n)}_{n-\lambda_1^i, n-\lambda_2^i, \ldots, n-\lambda_k^i}$, classe qui contient l'élément a^{-1}. Donc $a^{-1} \in g$. Il s'ensuit que g est un groupe, sous-groupe de G. Et ce sous-groupe est invariant. En effet, quel que soit l'élément c de G, on a

$$cgc^{-1} = c\left[\bigcup_{i=1}^{t} M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}\right]c^{-1} = \bigcup_{i=1}^{t} cM^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i}c^{-1} = \bigcup_{i=1}^{t} M^{(n)}_{\lambda_1^i \lambda_2^i \ldots \lambda_k^i} = g,$$

puisque chaque classe $M^{(n)}$ contient, avec tout élément d de G, la classe entière des éléments de G conjugués à d. On voit donc bien que G est un sous-groupe invariant de G.

C. Q. F. D.

Corollaire 1. — *Quel que soit l'entier $n \geqq 2$, la classe nulle $M^{(n)}_{00\ldots 0}$ est un sous-groupe invariant de G.*

Démonstration. — La classe nulle $M^{(n)}_{00\ldots 0}$ en temps qu'élément neutre du groupe $\Gamma^{(n)}$ constitue, à elle seule, un sous-groupe de $\Gamma^{(n)}$ et, par suite, d'après la proposition 11, l'ensemble des éléments de G qui forment la classe $M^{(n)}_{00\ldots 0}$ est un sous-groupe invariant de G.

Proposition 12. — *Quel que soit l'entier $n \geqq 2$, les classes $M^{(n)}$ en lesquelles se répartissent les éléments d'un groupe libre G engendré par une base A, ont un caractère intrinsèque, elles sont indépendantes de la base $A = \{a_1, a_2, \ldots, a_k\}$ de G à partir de laquelle elles ont été déterminées.*

Démonstration. — Soit G un groupe libre engendré par la base

$$A = \{a_1, a_2, \ldots, a_k\}.$$

Envisageons l'ensemble des classes $M^{(n)}$ définies à partir de cette base A. Soit, d'autre part, $B = \{b_1, b_2, \ldots, b_k\}$ une seconde base quelconque du groupe G, soient $M'^{(n)}$ les classes M définies, pour le même entier n, à partir de cette seconde base. Les classes $M^{(n)}$ aussi bien que les classes $M'^{(n)}$ sont au nombre de n^k et tout élément de G fait partie d'une classe $M^{(n)}$ ainsi que d'une classe $M'^{(n)}$ et d'une seule.

Montrons que si une classe $M^{(n)}$ a un élément commun avec une classe $M'^{(n)}$, ces deux classes sont confondues. En effet, supposons que les deux classes $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ et $M'^{(n)}_{\mu_1\mu_2\ldots\mu_k}$ ont en commun un élément c de G. c a un degré fixe par rapport à chaque élément de toute base de G. Soit u_i le degré de c par rapport à a_i et soit v_i le degré de c par rapport à $b_i (i=1, 2, \ldots, k)$. On a

$$u_i \equiv \lambda_i \pmod{n} \qquad \text{et} \qquad v_i = \mu_i \pmod{n} \qquad (i=1, 2, \ldots, k).$$

Chacun des éléments de la base $B(A)$ en tant qu'élément de G a à son tour un degré fixe par rapport à tout élément de la base $A(B)$. Soit $w^i_j (w'^i_j)$ le degré de $b_i(a_i)$ par rapport à $a_j (b_j)$ $(i, j=1, 2, \ldots, k)$. Soit

$$c = f(a_1, a_2, \ldots, a_k) = f'(b_1, b_2, \ldots, b_k),$$

où $f(f')$ désigne la composition finie réduite des éléments de la base $A(B)$ qui représente c. Cette composition, comme nous savons, est unique. Soit

$$a_i = f_i(b_1, b_2, \ldots, b_k), \qquad b_i = f'_i(a_1, a_2, \ldots, a_k),$$

où f_i est la composition finie réduite des éléments de B qui représente l'élément a_i et f'_i la composition réduite des éléments de A qui représente l'élément $b_i (i=1, 2, \ldots, k)$. On a

$$c = f'[f'_1(a_1, a_2, \ldots, a_k), f'_2(a_1, a_2, \ldots, a_k), \ldots, f'_k(a_1, a_2, \ldots, a_k)].$$

Le second membre de cette composition des éléments de A est de degré

$$v_1 w'_i + v_2 w^2_i + \ldots + v_k w^k_i$$

par rapport à a_i, quel que soit $i=1. 2, \ldots, k$. Et comme c est de degré fixe u_i par rapport à a_i, on a

$$u_i = v_1 w^1_i + v_2 w^2_i + \ldots + v_k w^k_i,$$

égalité qui implique la congruence

$$\lambda_i \equiv \mu_1 w^1_i + \mu_2 w^2_i + \ldots + \mu_k w^k_i \pmod{n} \qquad \text{quel que soit} \quad i=1, 2, \ldots, k.$$

Soit à présent d un élément quelconque de la classe $M'^{(n)}_{\mu_1\mu_2\ldots\mu_k}$ et soit $d = h'(b_1, b_2, \ldots, b_k)$, où le second membre est la composition finie réduite des éléments de B qui représente d. d est de degré fixe par rapport à tout élément de chaque base de G. Le degré v'_i de h par rapport à b_i satisfait la congruence

$$v'_i \equiv \mu_i \pmod{n} \qquad (i=1, 2, \ldots, k).$$

Si l'on remplace dans h les éléments b_i par leurs expressions au moyen des éléments de A, on trouve

$$d = h'[f'_1(a_1, a_2, \ldots, a_k), f'_2(a_1, a_2, \ldots, a_k), \ldots, f'_k(a_1, a_2, \ldots, a_k)]$$

et le second membre de cette expression est de degré

$$v'_1 w_i^1 + v'_2 w_i^2 + \ldots + v'_k w_i^k \equiv \mu_1 w_i^1 + \mu_2 w_i^2 + \ldots + \mu_k w_i^k \equiv \lambda_i \pmod{n}$$
$$\text{quel que soit} \quad i = 1, 2, \ldots, k.$$

Donc $d \in M^{(n)}_{\lambda_1 \lambda_2, \ldots \lambda_k}$. Cela étant quel que soit l'élément d de la classe $M'^{(n)}_{\mu_1 \mu_2, \ldots, \mu_k}$, on a l'inclusion

$$(+) \qquad M'^{(n)}_{\mu_1 \mu_2 \ldots \mu_k} \subset M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k}.$$

Soit maintenant d' un élément quelconque de la classe $M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k}$. Soit $d' = h(a_1, a_2, \ldots, a_k)$, h est de degré $u'_i \equiv \lambda_i \pmod{n}$ par rapport à a_i $(i = 1, 2, \ldots, k)$. Remplaçons dans h les a_i par leurs expressions au moyen des éléments de la base B. Il vient

$$d' = h[f_1(b_1, b_2, \ldots, b_k), f_2(b_1, b_2, \ldots, b_k), \ldots, f_k(b_1, b_2, \ldots, b_k)]$$

et le second membre de cette égalité est de degré

$$u'_1 w_i'^1 + u'_2 w_i'^2 + \ldots + u'_k w_i'^k \equiv \lambda_1 w_i'^1 + \ldots + \lambda_k w_i'^k \pmod{n}$$

par rapport à b_i, quel que soit $i = 1, 2, \ldots, k$; et comme

$$c = f(a_1, \ldots, a_k) = f[f_1(b_1, b_2, \ldots, b_k), f_2(b_1, b_2, \ldots, b_k), \ldots, f_k(b_1, b_2, \ldots, b_k)]$$

et que c fait partie de la classe $M'^{(n)}_{\mu_1 \mu_2 \ldots \mu_k}$, on a

$$\mu_i \equiv \lambda_1 w_i'^1 + \lambda_2 w_i'^2 + \ldots + \lambda_k w_i'^k \pmod{n} \qquad (i = 1, 2, \ldots, k).$$

On voit donc que $d' \in M'^{(n)}_{\mu_1 \mu_2 \ldots \mu_k}$.

Cela étant, quel que soit l'élément d' de $M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k}$ on a l'inclusion

$$(++) \qquad M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k} \subset M'^{(n)}_{\mu_1 \mu_2 \ldots \mu_k}$$

et des deux inclusions $(+)$ et $(++)$ résulte l'égalité

$$M^{(n)}_{\lambda_1 \lambda_2 \ldots \lambda_k} = M'^{(n)}_{\mu_1 \mu_2 \ldots \mu_k}.$$

Et comme tout élément de G appartient à une classe $M^{(n)}$ et à une seule ainsi qu'à une classe $M'^{(n)}$ et à une seule, il s'ensuit qu'il existe entre les classes $M^{(n)}$ et $M'^{(n)}$ une correspondance biunivoque et qu'à toute classe $M^{(n)}$ correspond une classe $M'^{(n)}$ confondue avec la première. Les classes M ont donc bien un caractère intrinsèque et ne dépendent pas de la base A de G à partir de laquelle elles sont formées.

C. Q. F. D.

Remarque 7. — Comme l'élément identique de G est commun aux classes $M^{(n)}_{00\ldots0}$ et $M'^{(n)}_{00\ldots0}$, les deux classes $M^{(n)}_{00\ldots0}$ et $M'^{(n)}_{00\ldots0}$ sont confondues, mais en général, l'égalité

$$M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k} = M^{(n)}_{\mu_1\mu_2\ldots\mu_k}$$

n'implique pas que $\lambda_i = \mu_i$ ($i = 1, 2, \ldots, k$).

Exemple. — Supposons que le groupe G est à base du second ordre. Considérons deux de ses bases a_1, a_2 et b_1, b_2, où $b_1 = a_1^3 a_2$ et $b_2 = a_1$. Soit $n = 5$.

Envisageons les classes $M^{(5)}_{22}$ et $M'^{(5)}_{21}$. L'élément $a_1 a_2 a_1 a_2$ de G fait partie de la première de ces classes et comme $a_1 a_2 a_1 a_2 = b_2^{-2} b_1 b_2^{-2} b_1$, l'élément considéré fait également partie de la classe $M'^{(5)}_{21}$. Donc, d'après ce qui précède, $M^{(5)}_{22} = M'^{(5)}_{21}$.

Quelle que soit la base B de G, à partir de laquelle on détermine les classes $M^{(n)}$, la classe nulle est toujours la même alors que les classes non nulles peuvent être permutées entre elles quand on passe d'une base à l'autre, mais l'ensemble d'éléments de G qui constitue chacune de ces classes est toujours le même, il est indépendant de B.

Remarque 8. — Quel que soit l'entier $n \geqq 2$, comme on l'a vu, aucun élément de la classe $M^{(n)}_{00\ldots0}$ ne saurait faire partie d'une base de G. D'après le corollaire 1, la classe $M^{(n)}_{00\ldots0}$ est un sous-groupe invariant du groupe G. Et comme la classe $M^{(n)}_{00\ldots0}$ varie avec n et qu'à deux valeurs distinctes de l'entier $n \geqq 2$ correspondent, comme nous le verrons, deux classes M nulles différentes, il s'ensuit que tout groupe libre de rang fini possède une infinité de sous-groupes invariants dont aucun élément ne fait partie d'une base de G. Nous prouverons que la réunion des classes $M^{(n)}_{00\ldots0}$ ($n = 2, 3, \ldots$) engendre le groupe G tout entier.

Les classes *M* nulles. — Soit G un groupe libre à base d'ordre fini k. Soit $A = \{a_1, a_2, \ldots, a_k\}$ une base de G et soit n un entier $\geqq 2$ quelconque. La classe nulle $M^{(n)}_{00\ldots0}$ comprend tous les éléments de G de degré $\equiv 0 \pmod{n}$ par rapport à chacun des éléments de la base A. Tous les éléments de G qui sont de degré 0 par rapport à chaque élément d'une première base A jouissent de la même propriété par rapport à n'importe quelle autre base B de G. On peut donc dire que *la classe* $M^{(n)}_{00\ldots0}$ *se compose de tous les éléments de G qui sont de degré* $\equiv 0 \pmod{n}$ *par rapport à chaque élément de n'importe quelle base de G.*

Montrons que *les classes* $M^{(n)}_{00\ldots0}$ ($n = 2, 3, \ldots$) *sont distinctes*, tout en ayant deux à deux une infinité d'éléments communs. En effet, soient n et n' deux entiers $\geqq 2$ et soit $n' > n$. Si n est un diviseur de n', la classe $M^{(n)}_{00\ldots0}$ contient la classe $M^{(n')}_{00\ldots0}$. En effet, soit a un élément quelconque de G qui est de degré $\equiv 0 \pmod{n}$ par rapport à chaque élément de la base A. Comme n' est un multiple de n, tout élément de G qui est de degré $\equiv 0 \pmod{n'}$ est aussi de degré $\equiv 0 \pmod{n}$ par rapport à chaque élément de la base A et, par suite,

$$M^{(n)}_{00\ldots0} \supset M^{(n')}_{00\ldots0}.$$

Mais ces deux classes ne sauraient être confondues puisque la première de ces classes contient, par exemple, les éléments a_i^n $(i=1, 2, \ldots, k)$ qui ne font pas partie de la seconde classe.

Si $D(n, n')=d>1$, mais si $d<n$ les deux classes $M_{00\ldots0}^{(n)}$ et $M_{00\ldots0}^{(n')}$ sont, d'après ce qui précède, contenues dans la classe $M_{00\ldots0}^{(d)}$. Soit m le p. p. c. m. des deux nombres n et n'. Tout élément de G qui est de degré $\equiv 0 \pmod{m}$ par rapport à chaque élément de A est commun aux deux classes nulles considérées, On a

$$M_{00\ldots0}^{(n)} \cap M_{00\ldots0}^{(n')} = M_{00\ldots0}^{(m)},$$

car tout élément commun à nos deux classes nulles est de degré $\equiv 0 \pmod{m}$ [puisqu'il est de degré $\equiv 0 \pmod{n}$ et $\equiv 0 \pmod{n'}$] et que tout élément de $M_{00\ldots0}^{(m)}$ fait évidemment partie de chacune des deux classes nulles considérées. Mais les deux classes $M_{00\ldots0}^{(n)}$ et $M_{00\ldots0}^{(n')}$ sont distinctes. En effet, par hypothèse, $n<n'$. Les éléments $a_i^n (i=1, 2, \ldots, k)$ font partie de la classe $M_{00\ldots0}^{(n)}$, mais non de la classe $M_{00\ldots0}^{(n')}$ quel que soit $i=1, 2, \ldots, k$. Donc $M_{00\ldots0}^{(n)} \neq M_{00\ldots0}^{(n')}$.

Si $D(n, n')=1$, le p. p. c. m. de n et de n' est $m=nn'$. Dans ce cas aussi, comme on le voit sans peine,

$$M_{00\ldots0}^{(n)} \cap M_{00\ldots0}^{(n')} = M_{00\ldots0}^{(m)}$$

ei les deux classses nulles considérées sont distinctes. La première contient les éléments a_i^n et la seconde les éléments $a_i^{n'} (i=1, 2, \ldots, k)$, éléments de G dont aucun n'est commun aux deux classes envisagées.

On voit donc bien que quels que soient les entiers $n \geqq 2$ et $n'>n$, les deux classes $M_{00\ldots0}^{(n)}$ et $M_{00\ldots0}^{(n')}$ ont en commun une infinité d'éléments de G, mais qu'elles sont distinctes. Si n' est un multiple de n, la classe $M_{00\ldots0}^{(n)}$ contient la classe $M_{00\ldots0}^{(n')}$.

Chaque classe $M_{00\ldots0}^{(n)}$ est un sous-groupe invariant de G. Envisageons l'ensemble

$$M = \bigcup_{n=2}^{\infty} M_{00\ldots0}^{(n)},$$

réunion de toutes les classes nulles, *M est un ensemble d'éléments de G qui engendre le groupe G*. En effet, supposons d'abord que A se compose d'un seul élément a, donc que le groupe G est cyclique. Alors toute classe $M_0^{(n)}$ se compose des éléments a^{tn}, où t est un entier quelconque. Considérons deux éléments quelconques a^{tn} et $a^{t'n'}$ de l'ensemble M. Leur produit $a^{tn+t'n'}$ appartient à G. Par suite, M — qui contient avec tout élément de G aussi, son inverse — engendre le groupe G puisqu'il contient les éléments a^{-n} et a^{n+1} $(n \geqq 2)$ et que $a^{-n}a^{n+1}=a$.

Supposons maintenant que A contient au moins deux éléments et soient n et n' deux entiers quelconques $\geqq 2$ et premiers entre eux. L'élément $a_1^n \in M_{00\ldots0}^{(n)}$, l'élément $a_2^{n'} \in M_{00\ldots0}^{(n')}$, ces deux éléments font donc partie de M, mais leur produit ne fait pas partie de M, il n'est contenu dans aucune classe M nulle et, par suite, M n'est pas un groupe. Mais il engendre le groupe G tout entier.

En effet, quel que soit l'élément a_i de la base A, l'élément a_i^3 appartient à la classe $M^{(3)}_{00\ldots0}$, l'élément a_i^{-2} appartient à la classe $M^{(2)}_{00\ldots0}$, donc $a_i = a_i^3 a_i^{-2}$ fait partie du groupe engendré par les éléments de M. Cela étant quel que soit $i = 1, 2, \ldots, k$, il s'ensuit que tout élément de A, donc aussi tout élément de G, fait partie du groupe engendré par l'ensemble M. Donc l'ensemble M est générateur du groupe G.

Ceci montre que *tout élément libre d'un groupe libre peut être obtenu par composition finie d'éléments non libres de ce groupe.*

On appelle libres les éléments d'une base quelconque de G. Tous les éléments de G (libres et non libres) s'obtiennent par composition finie des éléments de n'importe quelle base de ce groupe. Donc tout élément non libre s'obtient à son tour par composition finie d'éléments libres.

Les p-classes. — Soit G un groupe libre engendré par un ensemble $A = \{a_1, a_2, \ldots, a_k\}$ d'éléments libres, soit p un nombre premier $\geqq 2$ et soit n un entier multiple de p et supérieur à p, $n = mp$, $m > 1$. Répartissons les éléments de G en classes $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$. Nous dirons qu'une classe $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ est une p-classe si chacun des nombres $\lambda_1, \lambda_2, \ldots, \lambda_k$ est un multiple de p. Il ressort aussitôt de la loi de composition des classes $M^{(n)}$ que le produit de deux p-classes est une p-classe et que l'inverse d'une p-classe est aussi une p-classe. Donc l'ensemble des p-classes est un sous-groupe du groupe $\Gamma^{(n)}$ et la réunion des éléments de G qui font partie de toutes les p-classes est un sous-groupe invariant de G. Ce sous groupe G_p est formé de tous les éléments de G qui sont de degré $\equiv 0 \pmod p$ par rapport à tout élément de A. Soit $B = \{b_1, b_2, \ldots, b_k\}$ un système quelconque de générateurs libres du groupe G. Tout élément c de G_p est aussi de degré $\equiv 0 \pmod p$ par rapport à tout élément de B. En effet, partons de la composition finie réduite d'éléments de A qui représente c. Cette composition $f(a_1, a_2, \ldots, a_k)$ est de degré $\equiv 0 \pmod p$ par rapport à tout élément de A. Comme B est une base de G, tout élément de A peut être obtenu par composition finie d'éléments de B. Soit

$$a_i = f_i(b_1, b_2, \ldots, b_k) \qquad (i = 1, 2, \ldots, k).$$

On obtient l'expression réduite de c au moyen d'éléments de B en remplaçant dans f l'élément a_i par $f_i(b_1, b_2, \ldots, b_k)(i = 1, 2, \ldots, k)$ et en opérant la réduction par rapport aux éléments de B. Comme tous ces éléments sont libres et que f est de degré $\equiv 0 \pmod p$ par rapport à chacun des éléments a_i, c est aussi de degré $\equiv 0 \pmod p$ par rapport à chaque élément de B. Donc les classes $M^{(n)}$ qui sont des p-classes relativement à la base A sont aussi des p-classes relatives à n'importe quelle autre base B de G.

Proposition 13. — *Aucun élément du groupe G_p (donc aussi aucun élément d'une p-classe) n'est libre.*

Démonstration. — Soit G un groupe libre engendré par l'ensemble

$$A=\{a_1, a_2, \ldots, a_k\}$$

d'éléments libres, soit p un nombre premier quelconque $\geqq 2$ et soit $n=mp$, où m est un entier >1.

Répartissons les éléments de G en classes $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ relatives à la base A. Soit

$$B=\{b_1, b_2, \ldots, b_k\}$$

un ensemble quelconque d'éléments générateurs libres de G. D'après la remarque 6, les éléments $b_1, b_2, \ldots, b_k$ font partie de k classes $M^{(n)}$ indépenpendantes. Soit

$$b_i \in M^{(n)}_{\lambda_1^i\lambda_2^i\ldots\lambda_k^i} \qquad (i=1, 2, \ldots, k).$$

Donc, d'après la proposition 6, le p. g. c. d, de n et du déterminant $|\lambda_j^i|$ est égal à 1. Mais alors aucun des éléments b_i de B ne saurait faire partie d'une p-classe. En effet, si un élément b_i de B faisait partie d'une p-classe, tous les éléments de la $i^{\text{ième}}$ ligne de $|\lambda_j^i|$ seraient des multiples de p et, par suite, le p. g. c. d. de n et de $|\lambda_j^i|$ serait $\geqq p>1$, ce qui est contradictoire. On voit donc bien qu'aucun élément de la base B ne saurait faire partie d'une p-classe et, par suite, qu'aucun élément du groupe G_p n'est libre.

C. Q. F. D.

Remarque 9. — Toute p-classe est formée d'éléments de la classe $M^{(p)}_{00\ldots0}$.

LES CLASSES $M^{(n)}$ ET LES ÉLÉMENTS LIBRES DU GROUPE G. — Soit G un groupe libre engendré par un ensemble fini $A=\{a_1, a_2, \ldots, a_k\}$ d'éléments générateurs libres et soit n un entier >2. Répartissons les éléments de G en classes $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ à partir de la base A et proposons-nous de rechercher s'il existe parmi les classes $M^{(n)}$ qui ne sont pas des p-classes des classes dépourvues d'éléments libres et si de telles classes peuvent faire partie d'un système irréductible d'éléments générateurs du groupe $\Gamma^{(n)}$.

Soit d'abord $k=1$. — Soit p un nombre premier $\geqq 5$. Alors des $p-1$ classes non nulles $M_1^{(p)}, M_2^{(p)}, \ldots, M_{p-1}^{(p)}$, seules la première et la dernière contiennent chacune un seul élément libre, alors que les classes $M_2^{(p)}, \ldots, M_{p-2}^{(p)}$ ne renferment que des éléments non libres. Toutefois, chacune des classes $M_i^{(p)} (i=1, 2, \ldots, p-1)$ est génératrice du groupe $\Gamma^{(n)}$ qui est un groupe cyclique d'ordre p.

Soit à présent $k=2$. — Soit $M^{(n)}_{\lambda_1\lambda_2}$ un élément du groupe $\Gamma^{(n)}$ qui n'est pas une p-classe.

Supposons d'abord que l'un des nombres λ_1, λ_2 est nul. λ_1 et λ_2 ne sauraient être nuls tous les deux, car la classe considérée n'est pas nulle. Le raisonnement étant tout à fait analogue quel que soit celui des deux nombres λ_1, λ_2 qui est nul, bornons-nous à considérer le cas où $\lambda_2=0$. Dans ce cas, le p. g. c. d. des deux nombres n et λ_1 est $=1$, puisque la classe $M^{(n)}_{\lambda_1 0}$ envisagée n'est pas une p-classe et, par suite, il existe un entier t, tel que $tn \equiv 1 \pmod{\lambda_1}$, d'après le petit théorème de Fermat. Soit $tn = 1 + u\lambda_1$, où u désigne un entier. L'élément $(a_1 a_2^u)^{\lambda_1} a_2$ est un élément de la classe $M^{(n)}_{\lambda_1 0}$ et cet élément est libre puisqu'en lui ajoutant l'élément $a_1 a_2^n$, on obtient un système de deux éléments générateurs de G. Or, un tel système est formé d'éléments libres.

On voit, de même, que si $\lambda_1 = 0$ et si $\lambda_2 > 0$, la classe $M^{(n)}_{0\lambda_2}$ contient des éléments libres. Supposons à présent qu'aucun des deux nombres λ_1, λ_2 n'est nul. Comme la classe $M^{(n)}_{\lambda_1\lambda_2}$ envisagée n'est pas une p-classe, le p. g. c. d. des trois nombres n, λ_1, λ_2 est égal à 1.

Si $\lambda_1 = 1$, $a_1 a_2^{\lambda_2}$ est un élément libre de la classe $M^{(n)}_{1\lambda_2}$.

Si $\lambda_1 = n - 1$, $a_1^{-1} a_2^{\lambda_2}$ est un élément libre de la classe $M^{(n)}_{1\lambda_2}$.

De même si $\lambda_2 = 1$ ou $n - 1$, la classe $M^{(n)}_{\lambda_1\lambda_2}$ contient des éléments libres.

Supposons que $1 < \lambda_1 < n - 1$ et que $1 < \lambda_2 < n - 1$.

S'il existe un entier x, tel qu'on a l'une au moins des congruences

$$(\text{♀}) \qquad xn + \lambda_1 \equiv \pm 1 \pmod{\lambda_2}, \qquad xn + \lambda_2 \equiv \pm 1 \pmod{\lambda_1},$$

la classe $M^{(n)}_{\lambda_1\lambda_2}$ contient des éléments libres. En effet, si

$$xn + \lambda_1 = \pm 1 + u\lambda_2,$$

où u désigne un entier, posons

$$c = a_1^{\pm 1} (a_1^u a_2)^{\lambda_2}$$

et si

$$xn + \lambda_2 = \pm 1 + v\lambda_1,$$

où v désigne un entier, posons

$$d = (a_1 a_2^v)^{\lambda_1} a_2^{\mp 1}.$$

Si l'on a la première des congruences (♀), c est un élément de la classe $M^{(n)}_{\lambda_1\lambda_2}$ et cet élément est libre. En effet, les deux éléments c et $a_1^u a_2$ sont générateurs du groupe G puisque, par composition finie de ces deux éléments, on obtient sans peine les deux éléments a_1 et a_2. Or tout système de deux éléments générateurs de G est composé d'éléments libres. Et si l'on a la seconde des congruences (♀), d est un élément libre de la classe $M^{(n)}_{\lambda_1\lambda_2}$.

Mais il n'existe pas toujours un entier x qui satisfasse l'une au moins des congruences (♀). Tel est, par exemple, le cas pour $n = 63$, $\lambda_1 = 9$ et $\lambda_2 = 14$.

Mais la classe $M^{(63)}_{9,14}$ contient néanmoins des éléments libres. Tel est, par exemple, l'élément

$$b_1 = [(a_1 a_2)^5 a_1 (a_1 a_2)^5]^{50} a_1 a_2 [(a_1 a_2)^5 a_1 (a_1 a_2)^5]^8$$

qui appartient à cette classe et qui est libre puisqu'il forme avec l'élément

$$b_2 = (a_1 a_2)^5 a_1 (a_1 a_2)^5$$

un système générateur du groupe G. Or tout système générateur d'un groupe libre de rang 2 est formé, comme on sait, d'éléments libres.

Si le nombre $\lambda_1 - \lambda_2$ est premier avec n, la classe $M^{(n)}_{\lambda_1\lambda_2}$ contient également des éléments libres. En effet, envisageons le système des deux congruences

$$(+) \qquad xy + y + 1 \equiv \lambda_1 \pmod{n}, \qquad xy + 1 \equiv \lambda_2 \pmod{n}.$$

Montrons qu'il existe des valeurs entières de x et de y qui satisfont ces deux congruences. En effet, il résulte de $(+)$ que $y \equiv \lambda_1 - \lambda_2 \pmod{n}$ et il suffit de poser $y = \lambda_1 - \lambda_2$ pour satisfaire à cette congruence. Remplaçons y par cette valeur dans la seconde congruence $(+)$. Il vient

$$x(\lambda_1 - \lambda_2) \equiv \lambda_2 - 1 \pmod{n}$$

et il existe des valeurs entières de x qui satisfont cette congruence, puisque $\lambda_1 - \lambda_2$ et n, sont premiers entre eux. Envisageons un couple de valeurs de x et y qui satisfont les congruences $(+)$ et soient m_1, n_1, m_2, n_2 quatre entiers tels que

$$m_1 + n_1 = x, \qquad m_2 + n_2 = y.$$

Il existe une infinité de tels entiers. Posons

$$b_1 = [(a_1 a_2)^{m_1} a_1 (a_1 a_2)^{n_1}]^{m_2} a_1 a_2 [(a_1 a_2)^{m_1} a_1 (a_1 a_2)^{n_1}]^{n_2}.$$

On vérifie sans peine que cet élément b_1 appartient à la classe $M^{(n)}_{\lambda_1\lambda_2}$ et c'est un élément libre de G, car si on lui ajoute l'élément

$$b_2 = (a_1 a_2)^{m_1} a_1 (a_1 a_2)^{n_1},$$

on obtient un système générateur du groupe G et un tel système est formé d'éléments libres, puisque G est de rang 2.

Soit à présent k un entier quelconque $\geqq 2$ et soit $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ une classe de $\Gamma^{(n)}$, telle que le p. g. c. d. des nombres $n, \lambda_1, \lambda_2, \ldots, \lambda_k$ est égal à 1.

Si un seul des nombres $\lambda_1, \lambda_2, \ldots, \lambda_k$, soit λ_i, est $\neq 0$, la classe $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ contient des éléments libres. En effet, si $\lambda_i = 1$ ou $n - 1$, l'élément a_i ou a_i^{-1} est un élément libre de la classe envisagée. Soit $\lambda_i \neq 1$, $n - 1$ et soit $j \neq i$ un nombre de la suite $1, 2, \ldots, n - 1$. Comme le p. g. c. d. de n et de λ_i est $= 1$, il existe donc un entier t, tel que $tn \equiv 1 \pmod{\lambda_i}$. Soit $tn = 1 + u\lambda_i$, où u est entier, et soit $b = (a_i a_j^u)^{\lambda_i} a_j$. C'est un élément de la classe considérée et cet élément est libre, car si on lui associe les $k - 2$ éléments de l'ensemble

$$A = \{a_1, a_2, \ldots, a_k\} - \{a_i, a_j\}$$

ainsi que l'élément $a_i a_j^u$, on obtient un système générateur de G qui est de rang k et, par suite, les k derniers éléments générateurs de G sont tous libres.

Si deux nombres au moins de la suite $\lambda_1, \lambda_2, \ldots, \lambda_k$ sont $\neq 0$ et si tous les nombres non nuls de cette suite sont égaux, leur valeur commune étant λ, la classe $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ contient des éléments libres. En effet, comme la classe envisagée n'est pas une p-classe, le p. g. c. d. de n et de λ est $=1$. Il existe donc un entier t, tel que $tn \equiv 1 \pmod{\lambda}$. Soit $tn = 1 + u\lambda$, u entier. Soient $i_1, i_2, \ldots, i_r$ $(1 \leqq i_1 < i_2 < \ldots < i_r \leqq k)$ tous les indices de la suite $1, 2, \ldots, k$, tels que $\lambda_{i_l} = \lambda\,(l = 1, 2, \ldots, r)$. L'élément $(a_{i_1}a_{i_2}\ldots a_{i_{r-1}}a_{i_r}^{u+1})^{\lambda}a_{i_r}$ est un élément de la classe envisagée et cet élément est libre puisqu'en lui ajoutant les $k-2$ éléments de l'ensemble $\{a_1, a_2, \ldots, a_k\} - \{a_{i_{r-1}}, a_{i_r}\}$ ainsi que l'élément $a_{i_1}a_{i_2}\ldots a_{i_{r-1}}a_{i_r}^{u+1}$ on obtient un système de k éléments générateurs de G, dont, par conséquent, tous les éléments sont libres.

Quel que soit l'entier $k \geqq 2$, si l'un au moins des nombres $\lambda_1, \lambda_2, \ldots, \lambda_k$ est premier avec n, la classe $\mathrm{M}^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ contient des éléments libres. En effet, supposons que λ_i est premier avec n. Soit j un indice $\neq i$ quelconque de la suite $1, 2, \ldots, k$. Puisque n et λ_i sont premiers entre eux, il existe un entier t, tel que $tn \equiv 1 - \lambda_j \pmod{\lambda_i}$. Soit $tn = 1 - \lambda_j + u\lambda_i$, où u désigne un entier, et soit $i_1, i_2, \ldots, i_{k-2}$ une suite comprenant tous les éléments de l'ensemble $\{1, 2, \ldots, k\} - \{i, j\}$. Alors l'élément $a_{i_1}^{\lambda_{i_1}}a_{i_2}^{\lambda_{i_2}}\ldots a_{i_{k-2}}^{\lambda_{i_{k-2}}}(a_ia_j^u)^{\lambda_i}a_j$ est un élément de la classe considérée et cet élément est libre puisqu'en lui ajoutant les $k-1$ éléments $a_{i_1}, a_{i_2}, \ldots, a_{i_{k-2}}$ et $a_ia_j^u$, on obtient un système générateur du groupe G qui est de rang k et dont tout système minimum d'éléments générateurs est formé d'éléments libres.

Supposons maintenant que $\lambda_i > 0\,(i = 1, 2, \ldots, k)$ et que ces nombres ne sont pas tous égaux. Rangeons les k nombres $\lambda_1, \lambda_2, \ldots, \lambda_k$ par ordre de grandeur croissante et soit $\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_k}$ la suite ainsi obtenue. S'il existe dans cette suite deux nombres consécutifs dont la différence est égale à 1, la classe envisagée contient des éléments libres.

En effet, supposons que $\lambda_{i_{j+1}} - \lambda_{i_j} = 1$. Posons

$$\begin{aligned} c = {} & (a_{i_1}a_{i_2}\ldots a_{i_k})^{\lambda_{i_1}}(a_{i_2}a_{i_3}\ldots a_{i_k})^{\lambda_{i_2}-\lambda_{i_1}}\ldots \\ & \times (a_{i_{j+1}}a_{i_{j+2}}\ldots a_{i_k})(a_{i_{j+2}}a_{i_{j+0}}\ldots a_{i_k})^{\lambda_{i_{j+2}}-\lambda_{i_{j+1}}}\ldots \\ & \times (a_{i_{k-1}}a_{i_k})^{\lambda_{i_{k-1}}-\lambda_{i_{k-2}}}(a_i)^{\lambda_{i_k}-\lambda_{i_{k-2}}} \quad (^5). \end{aligned}$$

On voit sans peine que c'est un élément de la classe considérée. Et cet élément est libre, puisqu'en lui ajoutant $k-1$ éléments, notamment $a_{i_1}a_{i_2}\ldots a_{i_k}$, $a_{i_2}a_{i_3}\ldots a_{i_k}$, $\ldots$, $a_{i_j}a_{i_{j+1}}\ldots a_{i_k}$, $a_{i_{j+2}}\ldots a_{i_k}$, $\ldots$, a_{i_k}, si aucun des nombres $\lambda_{i_t} - \lambda_{i_{t-1}}\,(t = 2, \ldots, k)$ n'est nul, et en prenant le seul élément a_{i_t} au lieu du produit $a_{i_t}a_{i_{t+1}}\ldots a_{i_k}$, si $\lambda_{i_t} - \lambda_{i_{t-1}} = 0$, on voit sans peine que les k éléments considérés forment un système générateur de G, puisque par composition finie de ces k éléments on obtient les k éléments $a_1, \ldots, a_k$. Et comme c fait partie d'un système de k éléments générateurs de G, il est bien libre.

On voit donc que si deux nombres au moins de la suite $\lambda_1, \lambda_2, \ldots, \lambda_k$ diffèrent d'une unité, la classe $\mathrm{M}^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ contient des éléments libres.

---

(5) Où il faut supprimer tout facteur $(a_{i_l}a_{i_{l+1}}\ldots a_{i_k})^{\lambda_{i_l}-\lambda_{i_{l-1}}}$ pour lequel $\lambda_{i_l} - \lambda_{i_{l-1}} = 0$.

D'autre part, s'il existe un entier t, tel que $tn+\lambda_i \equiv \pm 1 \pmod{\lambda_j}$ pour un couple au moins d'indices $\lambda_i, \lambda_j (i, j = 1, 2, \ldots, k)$, la classe $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ contient des éléments libres. En effet, soit $tn+\lambda_i = \pm 1 + u\lambda_j$, où u désigne un entier. Posons

$$c = \left(\prod_{t=1,\, t\neq i,j}^{n} a_t^{\lambda_t} \right) (a_j a_i^u)^{\lambda_j} a_i^{\pm 1}.$$

C'est un élément de la classe considérée et cet élément est libre puisque si on lui ajoute les $k-2$ éléments $a_t (1 \leqq t \leqq k,\ t\neq i,\ t\neq j)$ et $a_j a_i^u$ on obtient un système de k éléments générateurs de G et par suite, c est bien libre.

On peut démontrer que toute classe $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ qui n'est pas une p-classe contient des éléments libres, si $k \geqq 2$.

Proposition 14. — *Soit G un groupe libre engendré par un ensemble fini $A = \{a_1, a_2, \ldots, a_k\}$ d'éléments libres. Quel que soit l'entier $n \geqq 2$ et quel que soit le sous-groupe g de G qui n'est pas contenu tout entier dans la classe $M^{(n)}_{00\ldots 0}$ (avec laquelle il a en tout cas en commun son élément neutre), les différentes classes $M^{(n)}$ qui contiennent des éléments de g ont en commun avec g des ensembles d'égale puissance.*

Démonstration. — Soient $M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}$ et $M^{(n)}_{\mu_1\mu_2\ldots\mu_k}$ deux classes $M^{(n)}$ quelconques qui contiennent des éléments de g et soit

$$g_1 = g \cap M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}, \qquad g_2 = g \cap M^{(n)}_{\mu_1\mu_2\ldots\mu_k}.$$

Soit ν_i le nombre de la suite $0, 1, \ldots, n-1$ qui vérifie la congruence

$$\nu_i \equiv \mu_i - \lambda_i \pmod{n} \qquad (i = 1, 2, \ldots, k)$$

et soient c_1 un élément fixe quelconque de g_1 et c_2 un élément de g_2. Comme g est un groupe, il existe un élément c de g, tel que $c_1 c = c_2$. Et comme

$$c_1 \in M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k} \qquad \text{et} \qquad c_2 \in M^{(n)}_{\mu_1\mu_1\ldots\mu_k},$$

l'élément c fait partie de la classe $M^{(n)}_{\nu_1\nu_2\ldots\nu_k}$, d'après la loi de composition des classes $M^{(n)}$. Et comme

$$M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k} M^{(n)}_{\nu_1\nu_2\ldots\nu_k} = M^{(n)}_{\mu_1\mu_2\ldots\mu_k},$$

on a

$$g_1 c \subset M^{(n)}_{\mu_1\mu_2\ldots\mu_k}.$$

Or $g_1 c \subset g$, puisque g est un groupe, et comme

$$g_2 = g \cap M^{(n)}_{\mu_1\mu_2\ldots\mu_k},$$

on a

$$(+) \qquad g_1 c \subset g_2$$

Or les ensembles g_1 et $g_1 c$ sont d'égale puissance et l'inclusion (+) montre que la puissance de l'ensemble g_1 n'est pas supérieure à celle de g_2.

D'autre part, $c_1 = c_2 c^{-1}$, $c^{-1} \in M^{(n)}_{n-\nu_1, n-\nu_2, \ldots, n-\nu_k}$ et comme

$$M^{(n)}_{\mu_1\mu_2\ldots\mu_k} M^{(n)}_{n-\nu_1, n-\nu_2, \ldots, n-\nu_k} = M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k},$$

on a

$$g_2 c^{-1} \subset M^{(n)}_{\lambda_1\lambda_2\ldots\lambda_k}.$$

Or $g_2 c^{-1} \subset g$ et, par conséquent, $g_2 c^{-1} \subset g_1$. Il s'ensuit que la puissance de g_2 n'est pas supérieure à celle de g_1. Et comme elle ne lui est également pas inférieure d'après l'inclusion (+), les deux ensembles g_1 et g_2 sont bien d'égale puissance. C. Q. F. D.

« Longueur » d'un élément d'un groupe libre dans une base donnée. — Soit G un groupe libre engendré par une base $A = \{a_1, a_2, \ldots, a_k\}$, soit c un élément quelconque de G et soit $a_{i_1}^{j_1} a_{i_2}^{j_2} \ldots a_{i_r}^{j_r}$ la composition finie réduite d'éléments de A qui représente c. Le nombre $j_1 + j_2 + \ldots + j_r$ est appelé la « longueur » de l'élément c dans la base A. C'est le degré de c par rapport à l'ensemble des éléments de A.

Toute base de G est formée de k éléments libres. La base A — appelée base primitive — est formée d'éléments libres dont chacun est de longueur 1.

Nous allons montrer que, quel que soit l'entier N, il existe des bases de G dont chaque élément est de longueur $>$ N dans la base A et qu'on peut former des nouvelles bases dont les éléments sont de plus en plus « longs » à partir de n'importe quelle base de G.

Proposition 15. — *Soit G un groupe libre à base d'ordre fini k. Alors quelle que soit la base $B = \{b_1, b_2, \ldots, b_k\}$ de G, il existe une suite infinie $c_1, c_2, \ldots$ d'éléments de G dont les k premiers sont les éléments de la base B, telle que k éléments consécutifs quelconques de cette suite constituent une base de G.*

Démonstration. — Soit $A = \{a_1, a_2, \ldots, a_k\}$ la base primitive de G, celle qui sert à définir ce groupe libre. Soit $B = \{b_1, \ldots, b_k\}$ une base connue quelconque du groupe G. Chaque élément de cette dernière base s'obtient par composition finie des éléments de la base primitive. Soit, par exemple,

$$b_1 = a_1, \qquad b_2 = a_2 a_1, \qquad \ldots, \qquad b_k = a_k a_{k-1} \ldots a_1,$$

Soit $b_{i_1}, b_{i_2}, \ldots, b_{i_k}$ une permutation quelconque des éléments de la base B et soit $c_j = b_{i_j}$ $(j = 1, 2, \ldots, k)$.

Quel que soit l'entier $m > 1$, désignons par ε_m un nombre qui prend l'une des deux valeurs $+1$ ou -1 et soient u_m et v_m deux entiers quelconques qui ne sont pas nuls simultanément.

Posons

$$c_{k+1} = c_k^{u_{k+1}} c_1^{\varepsilon_1} c_k^{v_{k+1}}, \qquad c_{k+2} = c_{k+1}^{u_{k+2}} c_2^{\varepsilon_2} c_{k+1}^{v_{k+2}}, \qquad \ldots,$$
$$c_{2k} = c_{2k-1}^{u_{2k}} c_k^{\varepsilon_k} c_{2k-1}^{v_{2k}}.$$

Soit à présent n un entier quelconque $\geqq 1$ et supposons que nous ayons déjà défini les éléments $c_1, c_2, \ldots, c_{nk}$. Posons

$$c_{nk+1} = c_{nk}^{u_{nk+1}} c_{(n-1)k+1}^{\varepsilon_{(n-1)k+1}} c_{nk}^{v_{nk+1}}, \qquad c_{nk+2} = c_{nk+1}^{u_{nk+2}} c_{(n-1)k+2}^{\varepsilon_{(n-1)k+2}} c_{nk+1}^{v_{nk+2}}, \qquad \ldots,$$
$$c_{(n+1)k} = c_{nk+k-1}^{u_{(n+1)k}} c_{nk}^{\varepsilon_{nk}} c_{nk+k-1}^{v_{(n+1)k}}.$$

Cela étant quel que soit l'entier $n = 1, 2, 3, \ldots$, nous définissons la suite

$$(\ddagger) \qquad c_1, \quad c_2, \quad \ldots$$

formée d'une infinité d'éléments du groupe G. D'après la loi de composition des éléments d'un groupe libre, tous les éléments de la suite (‡) sont distincts.

Envisageons k éléments consécutifs quelconques de cette suite

$$(\ddagger\ddagger) \qquad c_m, \quad c_{m+1}, \quad \ldots, \quad c_{m+k-1}.$$

Montrons que ces k éléments constituent une base de G. A cet effet, il suffit de montrer que les k éléments de la base B peuvent être obtenus par composition finie des éléments (‡‡).

Si $m = 1$, les éléments (‡‡) forment la base B. Supposons que $m > 1$. Si $m \leqq k$, on a

$$c_k^{-u_{k+1}} c_{k+1} c_k^{-v_{k+1}} = c_1, \qquad c_{k+1}^{-u_{k+2}} c_{k+2} c_{k+1}^{-v_{k+2}} = c_2 \qquad \ldots,$$
$$c_{m+k-2}^{-u_{m+k-1}} c_{m+k-1} c_{m+k-2}^{-v_{m+k-1}} = c_{m-1}$$

et, par suite, (‡‡) est bien une base de G.

Supposons enfin que $m > k$. On a alors

$$c_{m+i}^{-u_{m+i+1}} c_{m+i+1} c_{m+i}^{-v_{m+i+1}} = c_{m+i-k+1} \qquad (i = 0, 1, \ldots, k-2),$$
$$c_{m-1}^{-u_m} c_m c_{m-1}^{-v_m} = c_{m-k}.$$

A partir de $c_{m-k}, c_{m-k+1}, \ldots, c_{m-1}$ on déduit de même $c_{m-2k}, c_{m-2k+1}, \ldots, c_{m-k-1}$, et ainsi de suite, et finalement on est ramené à k éléments consécutifs de la suite $c_1, c_2, \ldots$, dont l'un au moins appartient à l'ensemble $a_1, \ldots, a_k$ et alors, en raisonnant comme dans le cas $m \leqq k$, on en déduit par composition finie les k éléments de la base B. Donc les éléments (‡‡) forment bien une base de G.

C. Q. F. D.

Remarque 10. — Tous les éléments de la suite $c_1, c_2, \ldots$ sont des éléments libres du groupe G. Et comme u_i, v_i sont des entiers arbitraires pourvu qu'ils ne soient pas tous deux nuls et que $\varepsilon_i = \pm 1$ quel que soit $i = 1, 2, \ldots$, on dispose ainsi d'un procédé commode pour déterminer des infinités d'éléments libres du groupe G. On notera que, quel que soit l'entier $\mathcal{N} > 1$, la « longueur » de c_m dans la base A peut être rendue $> \mathcal{N}$ pour m suffisamment grand.

Appliquons l'algorithme trouvé à la base primitive $a_1, a_2, \ldots, a_k$ elle-même. Soit $a_{i_1}, \ldots, a_{i_k}$ une permutation quelconque des éléments de cette base. Posons

$b_{1j} = a_{i_j}$, quel que soit $j = 1, \ldots, k$.

$$b_{21} = b_{1k}^{u_{21}} b_{11} b_{1k}^{v_{21}}, \qquad b_{22} = b_{21}^{u_{22}} b_{12} b_{21}^{v_{22}}, \qquad \ldots, \qquad b_{2k} = b_{2\,k-1}^{u_{2k}} b_{1k} b_{2\,k-1}^{v_{2k}},$$
$$b_{31} = b_{2k}^{u_{31}} b_{21} b_{2k}^{v_{31}}, \qquad b_{32} = b_{31}^{u_{32}} b_{22} b_{31}^{v_{32}}, \qquad \ldots, \qquad b_{3k} = b_{3\,k-1}^{u_{3k}} b_{2k} b_{3\,k-1}^{v_{3k}},$$

et ainsi de suite. Tous les éléments ainsi définis sont libres.

Les groupes libres de rang infini et les groupes libres de rang quelconque.

II. Soit à présent G un groupe libre engendré par un ensemble infini A d'éléments générateurs libres. Soit b un élément quelconque du groupe G. Il existe une composition finie réduite d'éléments de A qui représente b. Soit $b = a_{i_1}^{j_1} a_{i_2}^{j_2} \ldots a_{i_r}^{j_r}$ et soient $a_1, a_2, \ldots, a_k$ les divers éléments de A qui figurent dans cette composition. Soit u_{a_i} le degré de b par rapport à a_i ($i = 1, 2, \ldots, k$). Nous dirons que b est de degré $u_a = 0$ par rapport à tout élément a de l'ensemble $A - \{a_1, a_2, \ldots, a_k\}$.

Les classes $M^{(n)}\binom{a}{\lambda_a}_{a \in A}$. — Soit n un entier $\geqq 2$. Nous allons répartir les éléments du groupe G en classes de la façon suivante. Soit c un élément quelconque de G, a un élément de A et u_a le degré de c par rapport à a. Soit λ_a le nombre de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence

$$u_a \equiv \lambda_a \pmod{n}.$$

Nous dirons que c fait partie de la classe $M^{(n)}\binom{a}{\lambda_a}_{a \in A}$. Il existe pour toute classe $M^{(n)}\binom{a}{\lambda_a}_{a \in A}$ ainsi définie un sous-ensemble fini ou vide $A^\star = \{a_1, a_2, \ldots, a_k\}$ d'éléments de A tels que $\lambda_a \neq 0$, si $a \in A^\star$, et que $\lambda_a = 0$, si $a \in A - A^\star$. Quels que soient les nombres λ_a de la suite $0, 1, \ldots, n-1$, dont un nombre au plus fini sont $\neq 0$, la classe $M^{(n)}\binom{a}{\lambda_a}_{a \in A}$ contient une infinité d'éléments de G. En effet, si $A^\star = \emptyset$, la classe $M^{(n)}\binom{a}{0}_{a \in A}$ — dite *classe nulle* — contient (entre autres) tous les éléments de la forme a^{mn}, où a est un élément quelconque de A et m un entier quelconque, elle est donc infinie. Et si $A^\star \neq \emptyset$, la classe $M^{(n)}\binom{a}{\lambda_a}_{a \in A}$ contient tous les éléments de la forme $a_1^{\lambda_{a_1} + m_1 n} a_2^{\lambda_{a_2} + m_2 n} \ldots a_k^{\lambda_{a_k} + m_k n}$, où $m_1, m_2, \ldots, m_k$ sont des nombres entiers quelconques. Elle est donc également infinie.

On répartit ainsi tous les éléments de G en classes disjointes et l'on voit sans peine que chacune de ces classes contient avec tout élément b de G la classe entière des éléments de G conjugués à b.

Loi de composition des classes $M^{(n)}\binom{a}{\lambda_a}_{a \in A}$. — Nous appelons *produit* de deux classes $\mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}$ et $\mathrm{M}^{(n)}\binom{a}{\mu_a}_{a\in A}$ et nous désignons par le symbole $\mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}\mathrm{M}^{(n)}\binom{a}{\mu_a}_{a\in A}$ l'ensemble des éléments du groupe G qui peuvent se mettre sous la forme d'un produit bc où

$$b\in \mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A} \quad \text{et} \quad c\in \mathrm{M}^{(n)}\binom{a}{\mu_a}_{a\in A}.$$

PROPOSITION 16. — *Quelles que soient les classes* $\mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}$ *et* $\mathrm{M}^{(n)}\binom{a}{\mu_a}_{a\in A}$, *on a l'égalité*

$$(♀) \qquad \mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}\mathrm{M}^{(n)}\binom{a}{\mu_a}_{a\in A} = \mathrm{M}^{(n)}\binom{a}{\nu_a}_{a\in A},$$

où ν_a *désigne le nombre de la suite* $0, 1, \ldots, n-1$ *qui satisfait la congruence*

$$\nu_a \equiv \lambda_a + \mu_a \pmod{n}$$

quel que soit l'élément a *de* A. *Avec cette loi de composition qui est commutative et associative, les classes* $\mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}$ *forment un groupe abélien* $\Gamma^{(n)}$ *dont l'élément neutre est la classe nulle et dont l'inverse d'une classe* $\mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}$ *est la classe* $\mathrm{M}^{(n)}\binom{a}{n-\lambda_a}_{a\in A}$.

Démonstration. — En effet, soit b un élément quelconque de la classe $\mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}$ et soit c un élément de la classe $\mathrm{M}^{(n)}\binom{a}{\mu_a}_{a\in A}$. Soit u_a le degré de b et v_a le degré de c par rapport à un élément quelconque a de A. D'après la loi de composition des éléments d'un groupe libre, bc est de degré u_a+v_a par rapport à a, quel que soit $a\in A$. Soit ν_a le nombre de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence $\nu_a\equiv u_a+v_a \pmod{n}$. Comme

$$u_a\equiv\lambda_a \pmod{n} \quad \text{et que} \quad v_a\equiv\mu_a \pmod{n},$$

on a

$$\nu_a\equiv\lambda_a+\mu_a \pmod{n}.$$

Cela étant quel que soit l'élément a de A, il s'ensuit que

$$bc\in \mathrm{M}^{(n)}\binom{a}{\nu_a}_{a\in A}.$$

On a donc l'inclusion

$$(\dagger) \qquad \mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}\mathrm{M}^{(n)}\binom{a}{\mu_a}_{a\in A} \subset \mathrm{M}^{(n)}\binom{a}{\nu_a}_{a\in A}.$$

Soit maintenant d un élément quelconque de la classe $\mathrm{M}^{(n)}\binom{a}{\nu_a}_{a\in A}$ et soit b un élément fixe d'ailleurs quelconque de la classe $\mathrm{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}$. Soit $c=b^{-1}d$. C'est un élément du groupe G qui fait partie de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A}$ d'après la première partie de la démonstration, car b^{-1} est un élément de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ n-\lambda_a \end{pmatrix}_{a\in A}$. Il existe donc pour tout élément d de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \nu_a \end{pmatrix}_{a\in A}$ un élément c de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A}$ tel que $bc = d$. On a donc aussi l'inclusion

$$(++)\qquad \mathrm{M}^{(n)}\begin{pmatrix} a \\ \nu_a \end{pmatrix}_{a\in A} \subset \mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A} \mathrm{M}^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A}.$$

Et des deux inclusions $(+)$ et $(++)$ résulte l'égalité (♀). Il s'ensuit que la loi de composition des classes $\mathrm{M}^{(n)}$ est associative et commutative, que la classe $\mathrm{M}^{(n)}$ nulle est neutre par rapport à cette loi de composition et que l'inverse d'une classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ est la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ n-\lambda_a \end{pmatrix}_{a\in A}$ et, par conséquent, les classes $\mathrm{M}^{(n)}$, avec cette loi de composition, forment bien un groupe abélien $\Gamma^{(n)}$.

C. Q. F. D.

Définition. — *Nous disons que le groupe abélien $\Gamma^{(n)}$ est* associé *au groupe libre G. En faisant varier n, on peut ainsi associer au groupe libre G une infinité de groupes abéliens.*

Remarque 11. — Il ressort de la définition des classes $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ qu'à tout sous-ensemble fini $A^\star = \{a_1, a_2, \ldots, a_k\}$ de A correspondent n^k classes distinctes telles que $\lambda_a = 0$, $a\in A - A^\star$, et que les classes $\mathrm{M}^{(n)}$ qui correspondent à deux sous-ensembles finis différents de A sont distinctes. Donc l'ensemble des classes $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ a la même puissance que l'ensemble A.

Proposition 17. — *Deux classes $\mathrm{M}^{(n)}$ quelconques sont des ensembles d'égale puissance.*

Démonstration. — En effet, soit $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ et $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A}$ deux éléments quelconques du groupe $\Gamma^{(n)}$. Soit $A^\star$ l'ensemble des éléments de A, tels que l'un au moins des nombres λ_a, μ_a qui correspondent à tout élément a de $A^\star$ est $\neq 0$. Soit ν_a le nombre de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence $\nu_a \equiv \mu_a - \lambda_a \pmod{n}$, quel que soit $a\in A$. La classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \nu_a \end{pmatrix}_{a\in A}$ contient tout élément de la forme cb^{-1},

$$c\in \mathrm{M}^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A}, \qquad b\in \mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A},$$

alors que tout élément de la forme bc^{-1} fait partie de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ n-\nu_a \end{pmatrix}_{a\in A}$. Soit d un élément quelconque de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \nu_a \end{pmatrix}_{a\in A}$ et soit d' un élément de

$M^{(n)}\begin{pmatrix} a \\ n-\nu_a \end{pmatrix}_{a\in A}$. D'après (♀), on a les deux inclusions

$$dM^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A} \subset M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A'} \quad \text{et} \quad d'M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A} \subset M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A'}$$

dont il découle que les classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ et $M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A}$ sont bien des ensembles d'égale puissance. C. Q. F. D.

Proposition 18. — *Quel que soit le sous-groupe γ du groupe $\Gamma^{(n)}$, la réunion des classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ qui constituent les éléments de γ est un sous-groupe invariant de G.*

Démonstration. — Soit γ un sous-groupe quelconque du groupe $\Gamma^{(n)}$ et soit g la réunion des classes $M^{(n)}$ qui sont les éléments de γ. Le produit de tout couple d'éléments de g fait partie de g, puisque le produit des classes $M^{(n)}$ qui les contiennent fait partie du groupe γ. D'autre part, l'inverse de tout élément de g appartient à g puisque l'inverse de la classe $M^{(n)}$ qui contient l'élément envisagé fait partie du groupe γ. Donc l'ensemble g est un groupe. Et ce groupe est un sous-groupe invariant de G puisqu'il est la réunion de classes $M^{(n)}$ dont chacune contient avec tout élément b de G la classe entière des éléments de G conjugués à b. La proposition 18 est donc démontrée.

Corollaire 2. — *Quel que soit l'entier $n \geqq 2$, la classe nulle $M^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$ est un sous-groupe invariant de G.*

Démonstration. — En effet, la classe nulle qui est l'élément neutre du groupe $\Gamma^{(n)}$ forme à elle seule un sous-groupe de $\Gamma^{(n)}$, et par suite, d'après la proposition 18, cette classe nulle est un sous-groupe invariant du groupe G.

Comme la classe $M^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$ varie avec n, on en déduit l'existence d'une infinité de sous-groupes invariants dans tout groupe libre G.

Proposition 19. — *Quelle que soit la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$, l'ordre de cette classe, considérée comme élément du groupe $\Gamma^{(n)}$ est égal à $\frac{n}{d}$ où d est le p. g. c. d. de n et de tous les nombres λ_a (dont un nombre fini seulement sont $\neq 0$).*

Démonstration. — En effet, soit m l'ordre de la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$. On a donc

$$\left[M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}\right]^m = M^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}.$$

D'autre part, d'après (♀), on a

$$\left[M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}\right]^{\frac{n}{d}} = M^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A'}, \qquad \text{puisque} \quad \frac{n}{d}\lambda_a \equiv 0 \pmod{n}$$

quel que soit $a \in A$. Donc $\frac{n}{d}$ est un multiple de m : $\frac{n}{d} = m'm$ et l'entier m' ne saurait être > 1, sinon le p. g. c. d. de n et de tous les nombres λ_a serait $> d$, ce qui contredit la définition de d. On a donc bien $m = \frac{n}{d}$.

C. Q. F. D.

Corollaire 3. — *Tout système irréductible d'éléments générateurs du groupe* $\Gamma^{(n)}$ *a la même puissance que le groupe* $\Gamma^{(n)}$.

Démonstration. — En effet, d'après la proposition 19, tout élément du groupe $\Gamma^{(n)}$ est d'ordre fini $\leqq n$ et comme le groupe $\Gamma^{(n)}$ est abélien d'ordre infini, il ne saurait être engendré par un nombre fini de ses éléments, puisque quel que soit le nombre fini $m \geqq 1$, m éléments commutables d'ordre non supérieur à n chacun engendrent un groupe d'ordre fini $\leqq n^m$. Or, on sait que tout groupe qui ne saurait être engendré par un nombre fini d'éléments possède la même puissance que tout ensemble irréductible de ses éléments générateurs.

Remarque 12. — Considérons l'ensemble $\mathfrak{M}$ des classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ pour chacune desquelles il existe un seul élément a de A, tel que $\lambda_a = 1$, alors que $\lambda_{a'} = 0$ quel que soit $a' \in A - \{a\}$. Comme nous le verrons plus loin, $\mathfrak{M}$ est un système irréductible d'éléments générateurs du groupe $\Gamma^{(n)}$. On notera que les ensembles $\mathfrak{M}$ et A sont d'égale puissance. Donc le groupe $\Gamma^{(n)}$ et chacun de ses systèmes générateurs irréductibles sont des ensembles de même puissance que A.

Remarque 13. — Quel que soit l'ensemble A_1 d'éléments libres générateur du groupe G, l'ensemble $\mathfrak{M}$ des classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ qui comprennent des éléments de A_1 est générateur du groupe $\Gamma^{(n)}$. En effet, nous avons vu que quel que soit le sous-ensemble fini $A^\star$ de A et quels que soient les nombres λ_a de la suite $0, 1, \ldots, n-1$ $(a \in A^\star)$, alors que $\lambda_a = 0$, $a \in A - A^\star$, la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ comprend une infinité d'éléments du groupe G. Or si l'ensemble des classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ qui contiennent des éléments de A_1 n'était pas générateur du groupe $\Gamma^{(n)}$, il existerait des classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ faisant partie de ce groupe et dont aucun élément ne saurait être obtenu par composition finie des éléments de A_1. Donc A_1 ne serait pas générateur du groupe G, ce qui est contraire à notre hypothèse sur A_1. On voit donc bien que l'ensemble $\mathfrak{M}$ est générateur du groupe $\Gamma^{(n)}$.

Proposition 20. — *Soit G un groupe libre engendré par un ensemble infini A d'éléments générateurs libres. Soit n un entier $\geqq 2$. Les classes* $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ *ont un* *caractère intrinsèque, elles ne dépendent pas du système d'éléments générateurs A qui sert à les déterminer.*

Démonstration. — En effet, soit B un second système quelconque générateur de G, formé d'éléments libres. Tout élément de G appartient à une classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in\mathrm{A}}$ et à une seule ainsi qu'à une classe unique $\mathrm{M}^{(n)}\begin{pmatrix} b \\ \mu_b \end{pmatrix}_{b\in\mathrm{B}}$. Nous allons montrer que si les deux classes $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in\mathrm{A}}$ et $\mathrm{M}^{(n)}\begin{pmatrix} b \\ \mu_b \end{pmatrix}_{b\in\mathrm{B}}$ ont un élément commun, elles sont confondues. Montrons d'abord que

$$\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in\mathrm{A}} = \mathrm{M}^{(n)}\begin{pmatrix} b \\ 0 \end{pmatrix}_{b\in\mathrm{B}}.$$

Soit c un élément quelconque de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in\mathrm{A}}$. Comme A est une base de G, c s'obtient par composition finie d'éléments de A. Soient $a_1, a_2, \ldots, a_r$ les éléments de A dont une composition finie réduite $f(a_1, a_2, \ldots, a_r)$ représente c et soit v_i le degré de c par rapport à $a_i (i = 1, 2, \ldots, r)$. Comme B est aussi une base de G, chacun des éléments $a_1, a_2, \ldots, a_r$ peut s'exprimer par une composition finie réduite d'éléments de B. Soient $b_1, b_2, \ldots, b_s$ les éléments de B qui figurent dans les compositions finies réduites d'éléments de B qui représentent les r éléments a_i et soit u_{ij} le degré de a_i par rapport à $b_j (j = 1, 2, \ldots, s; i = 1, 2, \ldots, r)$. Pour avoir l'expression réduite de c par composition d'éléments de B, il suffit de remplacer dans $f(a_1, a_2, \ldots, a_r)$ chacun des éléments a_i par son expression réduite au moyen des éléments b_j et de procéder à des réductions en utilisant, au besoin, des relations triviales. Donc c est de degré

$$u_j \equiv v_1 u_{1j} + v_2 u_{2j} + \ldots + v_r u_{rj} \quad \text{par rapport à } b_j \qquad (j = 1, 2, \ldots, s).$$

Et comme

$$v_i \equiv 0 \pmod{n} \qquad \text{quel que soit} \quad (j = 1, 2, \ldots, r),$$

puisque $c \in \mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in\mathrm{A}}$, on a aussi

$$u_j \equiv 0 \pmod{n} \qquad (j = 1, 2, \ldots, s)$$

et, par suite, $c \in \mathrm{M}^{(n)}\begin{pmatrix} b \\ 0 \end{pmatrix}_{b\in\mathrm{B}}$. Cela étant, quel que soit l'élément c de $\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in\mathrm{A}'}$ on a l'inclusion

$$\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{\mathrm{A}\in\mathrm{A}} \subset \mathrm{M}^{(n)}\begin{pmatrix} b \\ 0 \end{pmatrix}_{b\in\mathrm{B}}.$$

Par un raisonnement tout à fait analogue, on démontre qu'on a aussi l'inclusion inverse et, par suite, on a bien

$$\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in\mathrm{A}} = \mathrm{M}^{(n)}\begin{pmatrix} b \\ 0 \end{pmatrix}_{b\in\mathrm{B}}.$$

Soit maintenant c un élément de G commun aux deux classes non nulles $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ et $M^{(n)}\begin{pmatrix} b \\ \mu_b \end{pmatrix}_{b\in B}$. L'un au moins des nombres λ_a et l'un au moins des nombres μ_b sont $\neq 0$. Par définition des classes $M^{(n)}$, il existe un sous-ensemble fini $A^\star = \{a_1, a_2, \ldots, a_k\}$ de A, tel que $\lambda_{a_i} \neq 0\ (i = 1, 2, \ldots, k)$, alors que $\lambda_a = 0$ pour tout $a \in A - A^\star$. Et comme B est une base de G, il existe un ensemble fini $B^\star = \{b_1, b_2, \ldots, b_l\}$ d'éléments de B, tel que tout élément a_i de $A^\star$ est une composition finie réduite d'éléments de $B^\star$. Soit u_{ij} le degré de a_i par rapport à b_j $(j = 1, 2, \ldots, l;\ i = 1, 2, \ldots, k)$. Dans la composition finie réduite d'éléments de A qui représente l'élément c figurent les k éléments a_i et éventuellement d'autres éléments de A (en nombre fini) par rapport auxquels c est de degré $\equiv 0 \pmod n$ alors que le degré de c par rapport à a_i est $\equiv \lambda_{a_i} \pmod n$ $(i = 1, 2, \ldots, k)$, puisque $c \in M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$. Donc le degré u_j de c par rapport à b_j dans l'expression réduite de c au moyen des éléments de B satisfait la congruence

$$u_j \equiv \lambda_{a_1} u_{1j} + \lambda_{a_2} u_{2j} + \ldots + \lambda_{a_k} u_{kj} \pmod n \qquad (j = 1, 2, \ldots, l),$$

alors que c est de degré $\equiv 0 \pmod n$ par rapport à tout autre élément de B qui figure éventuellement dans son expression réduite au moyen d'éléments de B. Et comme c fait partie de la classe $M^{(n)}\begin{pmatrix} b \\ \mu_b \end{pmatrix}_{b\in B}$ pour laquelle il existe un sous-ensemble fini non vide $B'^\star = \{b'_1, b'_2, \ldots, b'_{l'}\}$ de B, tel que $\mu_{b'_j} \neq 0\ (j = 1, 2, \ldots, l')$, alors que $\mu_b = 0$ quel que soit $b \in B - B'^\star$, il s'ensuit que $B'^\star \subset B^\star$, donc $l \geqq l'$, et si l'on choisit les notations de façon à avoir $b_j = b'_j\ (j = 1, 2, \ldots, l')$ on doit avoir

$$\lambda_{a_1} u_{1j} + \lambda_{a_2} u_{2j} + \ldots + \lambda_{a_k} u_{kj} \equiv \mu_j \pmod n \qquad (j = 1, 2, \ldots, l'),$$

alors que c est de degré $\equiv 0 \pmod n$ par rapport à tout élément de l'ensemble $B - B'^\star$, donc aussi

$$\sum_{i=1}^{n} \lambda_{a_i} u_{ij} \equiv 0 \pmod n \qquad \text{si} \quad j > l'.$$

Soit à présent d un élément quelconque de la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$. La composition finie réduite d'éléments de A qui représente d contient donc nécessairement les k éléments $a_1, a_2, \ldots, a_k$, elle est de degré $\equiv \lambda_{a_i} \pmod n$ par rapport à $a_i\ (i = 1, 2, \ldots, k)$, alors qu'elle est de degré $\equiv 0 \pmod n$ par rapport à tout élément de $A - A^\star$ qu'elle contient. Donc, d'après ce qui précède, la composition finie réduite d'éléments de B qui représente d est de degré $\equiv \mu_j \pmod n$ par rapport à $b_j\ (j = 1, 2, \ldots, l')$ et de degré $\equiv 0 \pmod n$ par rapport à tout élément de $B - B'^\star$ qu'elle renferme. Donc $d \in M^{(n)}\begin{pmatrix} b \\ \mu_b \end{pmatrix}_{b\in B}$. Cela étant, quel que soit l'élément d de $M^{(n)}\binom{a}{\lambda_a}_{a\in A}$, on a donc l'inclusion

$$M^{(n)}\binom{a}{\lambda_a}_{a\in A} \subset M^{(n)}\binom{b}{\mu_b}_{b\in B}.$$

Par un raisonnement tout à fait analogue, on établit l'inclusion inverse, ce qui démontre qu'on a bien

$$M^{(n)}\binom{a}{\lambda_a}_{a\in A} = M^{(n)}\binom{b}{\mu_b}_{b\in B},$$

si ces deux classes ont un élément commun. Et comme tout élément de G est commun à une classe $M^{(n)}\binom{a}{\lambda_a}_{a\in A}$ et à une classe $M^{(n)}\binom{b}{\mu_b}_{b\in B}$, il s'ensuit que l'ensemble des classes $M^{(n)}\binom{a}{\lambda_a}_{a\in A}$ coïncide avec l'ensemble des classes $M^{(n)}\binom{b}{\mu_b}_{b\in B}$ et, par suite, que les classes $M^{(n)}$ ont bien un caractère intrinsèque, elles sont indépendantes de la base de G à partir de laquelle elles sont déterminées.

C. Q. F. D.

Corollaire 4. — *Quel que soit le groupe libre G, la répartition des éléments de G en classes $M^{(n)}$ varie avec $n = 2, 3, \ldots$. On peut donc répartir d'une infinité de façons les éléments d'un groupe libre en classes d'équivalence $M^{(n)}$ qui ont un caractère intrinsèque et caractérisent les propriétés de structure du groupe libre.*

Remarque 14. — Il ressort de la démonstration de la proposition 20, que si A et B sont deux systèmes d'éléments générateurs libres du groupe libre G, quel que soit l'entier $n \geqq 2$, il existe entre les classes $M^{(n)}\binom{a}{\lambda_a}_{a\in A}$ et les classes $M^{(n)}\binom{b}{\mu_b}_{b\in B}$ une correspondance biunivoque, telle que deux classes homologues dans cette correspondance coïncident. On a toujours $M^{(n)}\binom{a}{0}_{a\in A} = M^{(n)}\binom{b}{0}_{b\in B}$. Quel que soit le nombre premier p, diviseur de n, l'ensemble des p-classes relatives à A se confond avec celui des p-classes relatives à B [6].

Remarque 15. — Il ressort du fait que les classes $M^{(n)}\binom{a}{\lambda_a}_{a\in A}$ ont un caractère intrinsèque, indépendant du système d'éléments générateurs libres A qui servent à les déterminer, que la répartition des éléments de G en classes $M^{(n)}$ dépend essentiellement du nombre n ainsi que de la structure du groupe G. Aussi peut-on parler de répartition des éléments de G en classes M relatives à un entier $n \geqq 2$.

Proposition 21. — *Soit G un groupe libre engendré par un ensemble A d'élé-*

---

[6] *Voir* définition des p-classes à la page 48.

ments générateurs libres. Quel que soit l'entier $n \geqq 2$, *aucun élément du groupe* G *qui fait partie de la classe* $\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in A}$ *n'est libre.*

Démonstration. — En effet, il ressort de la définition des classes $\mathrm{M}^{(n)}$ qu'aucun élément de A ne fait partie de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in A}$. Soit à présent B, un autre système quelconque d'éléments générateurs libres du groupe G. Comme $\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in A} = \mathrm{M}^{(n)}\begin{pmatrix} b \\ 0 \end{pmatrix}_{b \in B}$, aucun élément de B ne fait également partie de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in A}$, ce qui démontre la proposition 21.

Corollaire 5. — *Quel que soit l'élément libre* a *de* G *et quel que soit l'entier* n, *l'élément* a^n *n'est pas libre, puisqu'il fait partie de la classe* $\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in A}$, *où* A *est un système d'éléments générateurs libres de* G *comprenant l'élément* a.

D'autre part, quels que soient les éléments $a_1, a_2, \ldots, a_k$, en nombre fini k, de G qui font partie d'un même ensemble A d'éléments générateurs libres de G, et quel que soit l'entier $n \geqq 2$ aucun élément de G qui s'obtient par composition finie de $a_1, a_2, \ldots, a_k$ et qui est de degré $\equiv 0 \pmod{n}$ par rapport à chacun de ces éléments n'est libre. En effet, un tel élément appartient à la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in A}$ qui ne contient aucun élément libre.

Soit par, exemple, $k = 3$, $n = 5$ et soit $c = a_1^2 a_2^5 a_1^3 a_3^2 a_1^4 a_3^3 a_1$. Cet élément du groupe libre G qui est de degré 10 par rapport à a_1 et de degré 5 par rapport à chacun des deux éléments a_2 et a_3 n'est pas libre. Il ne fait partie d'aucune base de G.

Proposition 22. — *Soit* G *un groupe libre engendré par un ensemble* A *d'éléments générateurs libres. Soit* $\mathrm{A}^\star$ *un sous-ensemble propre de* A *et soit* $\mathrm{G}^\star$ *le groupe libre qu'il engendre. Alors tout élément libre de* $\mathrm{G}^\star$ *est aussi un élément libre de* G.

Démonstration. — Le groupe G est le produit libre des groupes cycliques engendrés par les éléments de A et $\mathrm{G}^\star$ est le produit libre des groupes cycliques engendrés par les éléments de $\mathrm{A}^\star$. Soit c un élément libre quelconque de $\mathrm{G}^\star$. Il existe donc un ensemble $\mathrm{B}^\star$ d'éléments libres de $\mathrm{G}^\star$, qui comprend l'élément c et qui est générateur de $\mathrm{G}^\star$. Comme les ensembles $\mathrm{A}^\star$ et $\mathrm{B}^\star$ sont deux systèmes d'éléments libres générateurs du groupe libre $\mathrm{G}^\star$, chacun de ces ensembles est irréductible et si l'on remplace dans A l'ensemble $\mathrm{A}^\star$ par l'ensemble $\mathrm{B}^\star$ on obtient un nouveau système d'éléments générateurs de G. Soit G' le groupe libre engendré par l'ensemble $\mathrm{A} - \mathrm{A}^\star$. G est le produit libre de G' et de $\mathrm{G}^\star$. Comme $\mathrm{B}^\star$ est un système d'éléments générateurs libres de $\mathrm{G}^\star$, $\mathrm{G}^\star$ est le produit libre des groupes cycliques engendrés par les éléments de $\mathrm{B}^\star$. Et si l'on remplace dans l'égalité $G = G' \star G^{\star}$ (7), G' par le produit libre des groupes cycliques engendrés par les éléments de $A - A^{\star}$ et $G^{\star}$ par le produit libre des groupes cycliques engendrés par les éléments de l'ensemble $B^{\star}$, G est, comme on sait, le produit libre de tous les groupes cycliques en question. Mais ceci prouve que l'ensemble $(A - A^{\star}) \cup B^{\star}$ est un système d'éléments générateurs libres de G, système qui comprend l'élément c de $G^{\star}$. Donc c qui, par hypothèse, est un élément libre de $G^{\star}$ est aussi un élément libre de G. C. Q. F. D.

PROPOSITION 23. — *Soit G un groupe libre engendré par un ensemble A d'éléments libres et soit $G^{\star}$ le groupe libre engendré par un sous-ensemble fini $A^{\star} = \{a_1, a_2, \ldots, a_k\}$ de A. Soit b un élément commun à G et à $G^{\star}$. Si b est un élément libre de G, il est aussi un élément libre de $G^{\star}$.*

Démonstration. — Soit B un système d'éléments générateurs libres de G qui contient l'élément b. Comme les éléments du système générateur B sont libres, G est le produit libre des groupes cycliques infinis engendrés par les éléments de B. C'est aussi le produit libre du groupe libre G' engendré par l'ensemble des éléments $B - \{b\}$ et du groupe cyclique G'' engendré par l'élément b. Les groupes G' et G'' ont en commun le seul élément 1. Soit $G^{\star\star} = G' \cap G^{\star}$ Le groupe $G^{\star}$ est le produit libre des deux groupes $G^{\star\star}$ et G''. En effet, on a l'inclusion $G^{\star\star} \star G'' \subset G^{\star}$ puisque le groupe $G^{\star}$ est libre et que G'' et $G^{\star\star}$ sont des sous-groupes de $G^{\star}$ qui ont en commun le seul élément 1. D'autre part, tout élément de $G^{\star}$ peut être obtenu en faisant le produit libre de $G^{\star\star}$ et de G''. En effet, le produit libre de G' et de G'' donne le groupe G tout entier, et comme $G^{\star}$ est un sous-groupe de G, on a $G^{\star} \subset G' \star G''$, Or un élément $\neq 1$ du produit libre $G' \star G''$ est, comme on sait, de la forme (1) $c_1 d_1 c_2 d_2 \ldots e_r$ ou de la forme (2) $c_1 d_1 c_2 d_2 \ldots c_r d_r$, où r est un entier ≥ 1, c_i fait partie de $G'(G'')$, d_i fait partie de $G''(G')$ quel que soit $i = 1, 2, \ldots, r$. Comme G' et G'' ont en commun le seul élément 1 et que $G'' \subset G^{\star}$, un élément de la forme (1) ou (2) ne peut faire partie du groupe $G^{\star}$ que si tous les éléments de chacun des deux ensembles $\{c_1, c_2, \ldots, c_r\}$ $\{d_1, d_2, \ldots, d_r\}$ sont des éléments de $G^{\star}$. Et comme les éléments de l'un de ces deux ensembles sont aussi des éléments de G', ils font partie de $G^{\star\star}$. On a donc bien $G^{\star} = G^{\star\star} \star G''$. Et comme $G^{\star}$ est un groupe libre de rang k (il est engendré par k éléments libres), il s'ensuit que $G^{\star\star}$ qui est à son tour un groupe libre, en tant que sous-groupe du groupe libre $G^{\star}$, est un produit libre de groupes cycliques infinis. Ces groupes cycliques sont en nombre fini (appelons ce nombre k') puisque $G^{\star}$ est le produit libre de ces groupes cycliques et de G'' et que $G^{\star}$ est de rang fini k. Et comme le rang est un invariant du groupe libre, on a $k' + 1 = k$. Soit $B^{\star\star}$ une base quelconque du groupe libre $G^{\star\star}$. Alors l'ensemble $B^{\star} = B^{\star\star} \cup \{b\}$ constitue une base de $G^{\star}$, base qui contient l'élément b. On voit donc bien que b est aussi un élément libre de $G^{\star}$. C. Q. F. D.

(7) Le signe $\star$ sert à désigner le produit libre.

Corollaire 6. — *Quel que soit le groupe libre G engendré par un ensemble (fini ou infini) A d'éléments libres, étant donné un élément quelconque c du groupe G, pour savoir si cet élément est libre, il suffit de considérer le groupe libre* $G^\star$ *engendré par les éléments de A, en nombre fini, figurant dans la composition finie réduite des éléments de A qui représente c et de voir si c qui est un élément de* $G^\star$ *est libre ou non dans* $G^\star$. *S'il est libre dans* $G^\star$ *il est libre aussi dans* G.

Cela simplifie beaucoup la recherche des éléments libres d'un groupe libre. En voici quelques exemples. Soit c un élément de G qui s'obtient par une composition finie de deux éléments a_1, a_2 de A : $c = f(a_1, a_2)$. Pour savoir si c est un élément libre de G ou non il suffit de voir s'il est libre ou non dans le groupe libre $G^\star$ engendré par les deux éléments a_1 et a_2. Pour démontrer que c est libre, il suffit de montrer qu'il existe un second élément d de $G^\star$ qui engendre avec c le groupe $G^\star$ puisque tout couple d'éléments générateurs d'un groupe libre de rang 2 est formé, comme on sait, d'éléments libres. Et pour prouver que deux éléments c et d sont générateurs de $G^\star$, il suffit de prouver que les deux éléments a_1 et a_2 s'obtiennent par composition finie de c et de d. On établit ainsi aisément les critères suivants :

Critère 1. — *Soit* $\varepsilon = \pm 1$ *et soient m et n deux entiers quelconques. Alors l'élément* $c = a_1^m a_2^\varepsilon a_1^n$ *est libre. En effet, il suffit de lui associer l'élément* a_1, *pour obtenir un couple d'éléments générateurs de* $G^\star$.

Critère 2. — *Soit* $\varepsilon_i = \pm 1$ $(i = 1, 2, 3)$ *et soit n un entier quelconque. Alors l'élément* $c = (a_1^{\varepsilon_1} a_2^{\varepsilon_2})^n a_3^{\varepsilon_3}$ *ainsi que l'élément* $d = a_1^{\varepsilon_1} a_2^{\varepsilon_2}$ *sont libres. En effet, on a* $d^{-n} c = a_1^{\varepsilon_3}$ *et les deux éléments* a_1, a_2 *s'obtiennent par composition finie de c et d qui sont donc tous les deux libres. En particulier, l'élément* $a_1 a_2$ *est libre.*

Critère 3. — *Soit* $\varepsilon_i = \pm 1$ $(i = 1, 2)$ *et soit n un entier* $\neq 1, -1$. *L'élément* $c = (a_1^{\varepsilon_1} a_2^{\varepsilon_2})^n$ *n'est pas pas libre. En effet, d'après le critère 2, l'élément* $a_1^{\varepsilon_1} a_2^{\varepsilon_2}$ *est libre et c ne saurait être libre, en tant que puissance* $\neq 1, -1$ *d'un élément libre, car une telle puissance appartient à la classe* $M^{(n)}$ *nulle, dépourvue d'éléments libres.*

Critère 4. — *Soit G un groupe libre engendré par un ensemble A d'éléments générateurs libres. Quel que soit le sous-ensemble fini* $A^\star = \{a_1, a_2, \ldots, a_k\}$ *de A et quels que soient les entiers non nuls* $n_1, n_2, \ldots, n_k$ *dont l'un au moins* n_i *est égal à* $+1$ *ou à* -1, *l'élément* $c = a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k}$ *est libre. En effet, soit* $G^\star$ *le groupe libre engendré par* $A^\star$. *L'ensemble* A_1 *obtenu en remplaçant dans* $A^\star$ *l'élément* a_i *par c est générateur de* $G^\star$ *puisque* a_i *s'obtient aisément par composition finie de c et des autres éléments de* A_1 *et que* $A_1 \supset A^\star - \{a_i\}$. *Donc c est un élément libre de* $G^\star$ *et, par suite, il est aussi un élément libre de G.*

Remarque 16. — Si une classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ contient au moins un élément libre c de G, elle en contient une infinité. En effet, cette classe contient, en même temps que c, la classe entière des éléments de G conjugués à c, classe qui est infinie. Or tous les éléments de cette classe sont libres puisque, quelle que soit la base B de G et quel que soit l'élément d de G, l'ensemble $B^\star$ composé de tous les éléments de la forme dbd^{-1}, $b \in B$, est à son tour une base de G.

Corollaire 7. — *Toute classe* $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$, *où l'un au moins des nombres* λ_a *est égal à* 1, *contient une infinité d'éléments libres.*

Démonstration. — En effet, soit $A^\star = \{a_1, a_2, \ldots, a_k\}$ le sous-ensemble (fini) de A, tel que $\lambda_a > 0$ si $a \in A^\star$ et $\lambda_a = 0$ si $a \in A - A^\star$. Soit $\lambda_i = 1$. L'élément $c = a_1^{\lambda_1} a_2^{\lambda_2} \ldots a_k^{\lambda_k}$ de G fait partie de la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ et, d'après le critère 4, c'est un élément libre de $G^\star$ et de G. Or, d'après la remarque 16, si la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ contient un élément libre, elle en contient une infinité.

Proposition 24. — *Une classe* $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ *ne contient aucun élément libre si le p. g. c. d. de n et de tous les nombres* λ_a *est* > 1.

Démonstration. — Soit $A^\star = \{a_1, a_2, \ldots, a_k\}$ le sous-ensemble fini de A, tel que $\lambda_a > 0$, si $a \in A^\star$ et $\lambda_a = 0$, si $a \in A - A^\star$. Le p. g. c. d. de n et de tous les nombres λ_a est égal à celui de n et des nombres $\lambda_{a_i} (i = 1, 2, \ldots, k)$. Soit $d = D(n, \lambda_{a_1}, \lambda_{a_2}, \ldots, \lambda_{a_k})$. Si $d > 1$, on a l'inclusion

$$M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A} \subset M^{(d)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in A}.$$

Or, aucune classe nulle ne contient, comme nous savons, d'éléments libres. Donc la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ est, elle aussi, dépourvue d'éléments libres.

C. Q. F. D.

Proposition 25. — *Quel que soit le groupe libre G engendré par un ensemble A (fini ou infini) d'éléments générateurs libres et quel que soit l'entier* $n \geq 2$, *toute classe* $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ *contient des éléments non libres.*

Démonstration. — Envisageons une classe quelconque $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$. Soit $A^\star = \{a_1, a_2, \ldots, a_k\}$ le sous-ensemble fini de A, tel que $\lambda_{a_i} > 0 (i = 1, 2, \ldots, k)$, alors que $\lambda_a = 0$ quel que soit $a \in A - A^\star$. Parmi les éléments de la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in A}$ figure l'élément

$$c = (a_1)^{\lambda_{a_1} + m_1 n} (a_2)^{\lambda_{a_2} + m_2 n} \ldots (a_k)^{\lambda_{a_k} + m_k n},$$

où $m_1, m_2, \ldots, m_k$ sont des entiers quelconques. Supposons d'abord que

$n > 2$, et soit $n' = n - 1$. Montrons qu'on peut choisir les nombres $m_1, m_2, \ldots, m_k$ de façon que $c \in M^{(n')}\binom{a}{0}_{a\in A}$. En effet, il suffit de poser

$$m_i = n' - \lambda_{a_i} \qquad (i = 1, 2, \ldots, k).$$

Alors

$$\lambda_{a_i} + (n' - \lambda_{a_i})\, n = n'(n - \lambda_{a_i}) \equiv 0 \pmod{n'} \qquad (i = 1, 2, \ldots, k).$$

Donc pour ces valeurs de $m_1, m_2, \ldots, m_k$, l'élément c n'est pas libre.

Soit à présent $n = 2$. Alors $\lambda_{a_i} = 1\,(i = 1, 2, \ldots, k)$. Posons

$$n' = 3 \qquad \text{et} \qquad m_1 = m_2 = \ldots = m_k = 1.$$

Alors

$$\lambda_{a_i} + m_i n = 3 \qquad (i = 1, 2, \ldots, k) \qquad \text{et, par suite,} \quad c \in M^{(3)}\binom{a}{0}_{a\in A}.$$

Donc dans ce cas aussi l'élément c n'est pas libre et la proposition est démontrée.

Corollaire 8. — *Soit $\mathfrak{M}$ un ensemble irréductibles de classes $M^{(n)}$, générateur du groupe $\Gamma^{(n)}$. Choisissons un élément et un seul dans chaque classe $M^{(n)}$ faisant partie de $\mathfrak{M}$ et soit A^* l'ensemble des éléments ainsi choisis. Tout système d'éléments générateurs libres de G peut être obtenu de cette façon, mais l'ensemble A^* n'est pas forcément générateur de G. Il suffit qu'il contienne un seul élément non libre de G (ce qui est possible, puisque d'après la proposition 25 toute classe $M^{(n)}$ contient des éléments non libres de G) pour qu'il engendre un sous-groupe propre de G.*

Proposition 26. — *Quel que soit le groupe libre G engendré par un ensemble A d'éléments générateurs libres et quel que soit l'entier $n \geq 2$, toute classe $M^{(n)}\binom{a}{\lambda_a}_{a\in A}$ contient une infinité d'éléments non libres.*

Démonstration. — En effet d''après la proposition 25, toute classe $M^{(n)}\binom{a}{\lambda_a}_{a\in A}$ contient au moins un élément non libre. Or si elle en contient un, elle en contient une infinité puisque cette classe contient avec tout élément c de G la classe entière des éléments de G conjugués à c. Or cette classe est infinie et si c n'est pas libre, dcd^{-1} n'est également pas libre, quel que soit l'élément d de G. La proposition 26 est donc démontrée.

Remarque 17. — Si $n = 2$, toute classe non nulle $M^{(2)}\binom{a}{\lambda_a}_{a\in A}$ d'éléments d'un groupe libre G engendré par un ensemble A (fini ou infini) d'éléments générateurs libres contient aussi bien des éléments libres que des éléments non libres.

En effet, soit $A^* = \{a_1, a_2, \ldots, a_k\}$ l'ensemble fini (non vide) formé de tous les élements a de A, tels que $\lambda_a > 0$. On a $\lambda_{a_i} = 1$ $(i = 1, 2, \ldots, k)$. L'élément $a_1 a_2 \ldots a_k$ appartient à la classe $M^{(2)}\binom{a}{\lambda_a}_{a\in A}$ envisagée, et comme il est de la forme $a_1 f(a_2, \ldots, a_k)$, il est, comme on sait, un élément libre de G. D'autre part, quel que soit l'entier positif m, l'élément $a_1^{1+2m} a_2^{1+2m} \ldots a_k^{1+2m}$ qui fait partie de la classe $\mathrm{M}^{(2)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in \mathrm{A}}$ n'est pas libre, car il fait partie de la classe nulle $\mathrm{M}^{1+2m}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in \mathrm{A}}$, classe qui est dépourvue d'éléments libres.

Remarque 18. — Soit G un groupe libre engendré par un ensemble A d'éléments générateurs libres. Soit n un entier quelconque $\geqq 3$, soit $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in \mathrm{A}}$ une classe non nulle et soit $\mathrm{A}^\star = \{a_1, a_2, \ldots, a_k\}$ l'ensemble (fini, non vide) formé de tous les éléments a de A, tels que $\lambda_a > 0$. Soit $n' = n - 1$ et soit $m_i = (n' - \lambda_{a_i}) n^{r_i}$ $(i = 1, 2, \ldots, k)$, où r_i désigne un nombre entier quelconque. L'élément

$$c = a_1^{\lambda_{a_1} + m_1 n} a_2^{\lambda_{a_2} + m_2 n} \ldots a_k^{\lambda_{a_k} + m_k n}$$

de G est alors un élément non libre de la classe $\mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in \mathrm{A}}$. En effet, par définition des classes $\mathrm{M}^{(n)}$,

$$c \in \mathrm{M}^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a \in \mathrm{A}}.$$

Or

$$\lambda_{a_i} + m_i n = \lambda_{a_i} + (n' - \lambda_{a_i}) n^{r_i+1} = n' n^{r_i+1} - (n-1)\lambda_{a_i}(n^{r_i} + n^{r_i-1} + \ldots + 1) \equiv 0 \pmod{n'},$$

puisque $n - 1 = n'$. Donc $c \in \mathrm{M}^{n'}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in \mathrm{A}}$ et, par suite, il n'est pas libre.

Proposition 27. — *Soit G un groupe libre engendré par un ensemble A d'éléments générateurs libres. Soit c un élément quelconque de G. Soient $a_1, a_2, \ldots, a_k$ les éléments de A qui figurent dans la composition finie réduite d'éléments de A qui représente c et soit v_i le degré de c par rapport à a_i $(i = 1, 2, \ldots, k)$.*

La condition nécessaire et suffisante pour que c appartienne à une classe $\mathrm{M}^{(n)}$ nulle, c'est que le p. g. c. d. d des nombres $v_1, v_2, \ldots, v_k$ soit > 1. En effet, si cette condition est satisfaite, $c \in \mathrm{M}^{(d)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in \mathrm{A}}$. Donc la condition est suffisante. Elle est aussi nécessaire. En effet, supposons qu'il existe un entier $n \geqq 2$, tel que $c \in \mathrm{M}^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a \in \mathrm{A}}$. Mais alors, par définition de cette dernière classe, $v_i \equiv 0 \pmod{n}$ $(i = 1, 2, \ldots, k)$ et, par suite, $d \geqq n > 1$. La condition est donc aussi nécessaire.

C. Q. F. D.

Proposition 28. — *Tout groupe libre G engendré par un ensemble infini A d'éléments générateurs libres possède une infinité indénombrable de sous-groupes invariants.*

Démonstration. — L'ensemble A est au moins dénombrable. Soit $\mathfrak{m}$ sa puissance. On a $\mathfrak{m} \geqq \aleph_0$. Soit n un entier quelconque $\geqq 2$. Considérons le groupe $\Gamma^{(n)}$ associé au groupe G. Soit $A^\star$ un sous-ensemble quelconque de A et soit $\gamma_{A^\star}$ le sous-ensemble de $\Gamma^{(n)}$ formé de toutes les classes $M^{(n)}\binom{a}{\lambda_a}_{a \in A}$, telles que $\lambda_a = 0$ si $a \in A^\star$, alors que $\lambda_{a'}$ peut prendre l'une quelconque des valeurs $0, 1, \ldots, n-1$, si $a' \in A - A^\star$, D'après (♀), le produit de deux éléments de $\gamma_{A^\star}$ fait partie du même ensemble et l'inverse de tout élément de $\gamma_{A^\star}$ fait également partie de $\gamma_{A^\star}$. Donc l'ensemble $\gamma_{A^\star}$ est un groupe, sous-groupe propre de $\Gamma^{(n)}$ puisqu'il ne contient aucune des classes $M^{(n)}\binom{a}{\lambda_a}_{a \in A}$ pour lesquelles $\lambda_a > 0$ pour un élément au moins a de $A^\star$. Soient $A^\star$ et $A^{\star\star}$ deux sous-ensembles distincts quelconques de A. Les sous-groupes correspondants $\gamma_{A^\star}$ et $\gamma_{A^{\star\star}}$ sont distincts. En effet, comme $A^\star \neq A^{\star\star}$, il existe au moins un élément de l'un de ces deux ensembles qui ne fait pas partie de l'autre. Soit, pour fixer les idées, $a^\star$ un élément de $A^\star$ qui $\notin A^{\star\star}$. Alors le groupe $\gamma_{A^{\star\star}}$ contient la classe $M^{(n)}\binom{a}{\lambda_a}_{a \in A}$, où $\lambda_{a^\star} = 1$ alors que $\lambda_a = 0$ quel que soit $a \in A - \{a^\star\}$, classe qui ne fait pas partie du groupe $\gamma_{A^\star}$. Donc les deux groupes $\gamma_{A^\star}$ et $\gamma_{A^{\star\star}}$ sont bien distincts. Comme l'ensemble A est infini de puissance $\mathfrak{m}$, l'ensemble de tous les sous-ensembles de A est de puissance $2^{\mathfrak{m}} > \mathfrak{m}$. Donc l'ensemble des sous-groupes $\gamma_{A^\star}$ de $\Gamma^{(n)}$ est aussi de puissance supérieure à $\mathfrak{m}$. Or, d'après la proposition 18, la réunion $g_{A^\star}$ des classes $M^{(n)}$ qui constituent les éléments du groupe $\gamma_{A^\star}$ est un sous-groupe invariant du groupe G. Et comme $g_{A^\star} \neq g_{A^{\star\star}}$, si $A^\star$ et $A^{\star\star}$ sont deux sous-ensembles différents de A, on voit bien que G possède une infinité indénombrable de sous-groupes invariants.

C. Q. F. D.

Remarque 19. — Quel que soit le nombre premier $p \geqq 2$, l'ensemble G_p des éléments de G qui sont de degré $u_a \equiv 0 \pmod{p}$ par rapport à tout élément a d'un système A d'éléments générateurs libres de G est un sous-groupe invariant de G. En effet, soient b et c deux éléments quelconques de G_p et soit $u_a(v_a)$ le degré de $b(c)$ par rapport à a quel que soit $a \in A$. On a

$$u_a \equiv 0 \pmod{p} \quad \text{et} \quad v_a \equiv 0 \pmod{p} \quad (a \in A),$$

D'après la loi de composition des éléments d'un groupe libre, bc est de degré $u_a + v_a$ par rapport à a, quel que soit $a \in A$. Or

$$u_a + v_a \equiv 0 \pmod{p}.$$

Donc $bc \in G_p$. D'autre part, quel que soit l'élément b de G_p, de degré $u_a \equiv 0 \pmod{p}$ par rapport à tout $a \in A$, l'élément b^{-1} est de degré $-u_a \equiv 0 \pmod{p}$ par rapport à a et, par suite, $b^{-1} \in G_p$. Donc G_p est un groupe et ce groupe est un sous-groupe invariant de G puisque, quel que soit l'élément b de G_p et quel que soit l'élément c de G, les deux éléments b et cbc^{-1} sont de même degré par rapport à tout élément de A.

Les p-classes. — Soit G un groupe libre engendré par un ensemble infini A d'éléments générateurs libres, soit n un entier $\geqq 2$, soit $\Gamma^{(n)}$ le groupe abélien associé à G et soit p un nombre premier quelconque $\geqq 2$, diviseur de n. Nous disons qu'une classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$, élément de $\Gamma^{(n)}$, est une p-classe si $\lambda_a \equiv (\bmod p)$, quel que soit $a \in A$. Comme $n \equiv 0 \pmod p$, les p-classes forment un sous-groupe du groupe $\Gamma^{(n)}$ et leur réunion forme un sous-groupe invariant de G.

Proposition 29. — *Aucun élément d'une p-classe n'est un élément libre de G.*

Démonstration. — En effet, soit n est un multiple de p. Tout élément d'une p-classe est de degré $\equiv 0 \pmod p$ par rapport à chaque élément d'un ensemble A de générateurs libres de G. Il fait donc partie de la classe $M^{(p)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$ et, par suite, il n'est pas libre.

C. Q. F. D.

Corollaire 9. — *Si n est un nombre composé, il existe une infinité de classes* $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ *qui sont dépourvues d'éléments libres de G. En effet, quel que soit le nombre premier p, diviseur de n, toute p-classe est dépourvue d'éléments libres d'après la proposition 29. Or le nombre de ces classes est infini. En effet, à tout sous-ensemble fini* $A^\star$ *de A correspond la p-classe* $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$, *où*

$$\lambda_a = p \quad \text{si } a \in A^\star \qquad \text{et} \qquad \lambda_a = 0 \quad \text{si } a \in A - A^\star.$$

Les p-classes qui correspondent ainsi à deux sous-ensembles distincts finis de A sont distincts et comme A est infini et possède une infinité de sous-ensembles finis distincts, on voit bien qu'il existe une infinité de p-classes. Et chacune de ces classes est dépourvue d'éléments libres.

C. Q. F. D.

Remarque 20. — Soit G un groupe libre engendré par un ensemble A d'éléments générateurs libres. Considérons tous les groupes abéliens $\Gamma^{(n)}$ ($n = 2, 3, \ldots$) associés à G. Montrons que les éléments neutres de ces groupes sont tous distincts. En effet, soient n et $n' < n$ deux nombres quelconques de la suite $2, 3, \ldots$ et soit d le p. g. c. d. de n et de n'. Si $d = n'$, la classe $M^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$ est un sous-ensemble de $M^{(n')}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$. En effet, la classe $M^{(n')}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$ comprend tous les éléments de G qui sont de degré $\equiv 0 \pmod{n'}$ par rapport à tout élément de A et cet ensemble comprend tous les éléments de G qui sont de degré $\equiv 0 \pmod n$

par rapport à chaque élément de A. Mais l'élément $a^{n'}$ fait partie de $M^{(n')}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$, alors qu'il fait défaut dans la classe $M^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$. Donc les deux classes nulles envisagées sont distinctes. Et si $d < n'$, chacun des éléments a^n, $a^{n'}$ $(a \in A)$ fait partie de l'une des deux classes nulles considérées alors qu'il fait défaut dans l'autre. Les deux classes nulles considérées sont donc bien distinctes.

PROPOSITION 30. — *Soit G un groupe libre engendré par un ensemble infini A d'éléments générateurs, soit n un entier $\geqq 2$ et soit $\Gamma^{(n)}$ le groupe abélien associé au groupe G. Soit $\mathfrak{M}$ l'ensemble comprenant toutes les classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ pour chacune desquelles il existe un seul élément $a^\star$ de l'ensemble A, tel que $\lambda_{a^\star} = 1$, alors que $\lambda_a = 0$ pour tout $a \in A - \{a^\star\}$. L'ensemble $\mathfrak{M}$ est générateur du groupe $\Gamma^{(n)}$.*

Démonstration. — En effet, soit $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ un élément quelconque du groupe $\Gamma^{(n)}$. Soit $A^\star$ le sous-ensemble (fini ou vide) de A, tel que $\lambda_a > 0$, si $a \in A^\star$, alors que $\lambda_a = 0$ pour tout $a \in A - A^\star$. Soit $A^\star = \{a_1, a_2, \ldots, a_k\}$ et soit M_i la classe de l'ensemble $\mathfrak{M}$ pour laquelle $\lambda_{a_i} = 1$ $(i = 1, 2, \ldots, k)$. On a

$$M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A} = (M_1)^{\lambda_{a_1}}(M_2)^{\lambda_{a_2}}\ldots(M_k)^{\lambda_{a_k}}.$$

On voit donc bien que tout élément du groupe $\Gamma^{(n)}$ peut être obtenu par composition finie des éléments de l'ensemble $\mathfrak{M}$ qui est donc bien générateur du groupe $\Gamma^{(n)}$. On voit immédiatement que cet ensemble est irréductible et qu'il a la puissance de l'ensemble A.

PROPOSITION 31. — *Soit G un groupe libre engendré par un ensemble A (fini ou infini) d'éléments générateurs libres. Soit n un entier $\geqq 2$, soit $\Gamma^{(n)}$ le groupe abélien associé à G et soit g un sous-groupe quelconque du groupe G. Alors l'ensemble γ des classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ qui contiennent des éléments de g forment un sous-groupe du groupe $\Gamma^{(n)}$.*

Démonstration. — En effet, soit $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ un élément quelconque de l'ensemble γ. Cette classe contient un élément b du groupe g. Or l'élément b^{-1} de g appartient à la classe $M^{(n)}\begin{pmatrix} a \\ n - \lambda_a \end{pmatrix}_{a\in A}$. Donc l'ensemble γ, contient, avec tout élément de $\Gamma^{(n)}$, son inverse. D'autre part, considérons deux éléments quelconques de l'ensemble γ : $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ et $M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A}$. Soit b un élément de g qui appartient à la première de ces classes et c un élément de g qui fait partie de la seconde. L'élément bc de g appartient à la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A} M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A}$ et, par suite, l'ensemble γ contient avec tout couple d'éléments du groupe $\Gamma^{(n)}$ aussi le produit de ces éléments. L'ensemble γ est donc bien un sous-groupe du groupe $\Gamma^{(n)}$.

C. Q. F. D.

PROPOSITION 32. — *Soit G un groupe libre engendré par un ensemble A d'éléments générateurs libres. Soit B la réunion des classes* $M^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$ $(n = 2, 3, \ldots)$. *L'ensemble B est générateur du groupe G.*

Démonstration. — En effet, quel que soit l'élément a de A et quel que soit l'entier $m > 2$, l'élément a^m fait partie de la classe nulle $M^{(m)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$, alors que l'élément a^{-m+1} appartient à la classe $M^{(m-1)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A}$. Donc le produit $a^{-m+1}a^m = a$ fait partie du groupe engendré par B. Cela étant quel que soit l'élément a de A, l'ensemble B est bien générateur de G.

C. Q. F. D.

PROPOSITION 33. — *Soit G un groupe libre engendré par un ensemble A d'éléments générateurs libres et soit n un entier* ≥ 2. *Aucune classe* $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ *ne saurait contenir plus d'un élément d'un même système d'éléments générateurs libres de G.*

Démonstration. — En effet, tout élément $a^\star$ de A appartient à la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$, où $\lambda_{a^\star} = 1$ et $\lambda_a = 0$, $a \in A - \{a^\star\}$, classe qui ne contient que le seul élément $a^\star$ de A. Il existe d'ailleurs de nombreuses classes $M^{(n)}$, dont la classe nulle, qui ne contiennent aucun élément de A. Soit à présent B un autre système quelconque formé d'éléments libres générateurs de G. Tout élément $b^\star$ de B appartient à la classe $M^{(n)}\begin{pmatrix} b \\ \mu_b \end{pmatrix}_{b\in B}$, telle que $\mu_{b^\star} = 1$, alors que $\mu_b = 0$, quel que soit $b \in B - \{b^\star\}$ et la classe en question ne contient pas d'antre élément de B. Or, les classes $M^{(n)}$ ayant un caractère intrinsèque, indépendant du système d'éléments générateurs libres de G à partir duquel elles ont été définies, la classe $M^{(n)}\begin{pmatrix} b \\ \mu_b \end{pmatrix}_{b\in B}$ se confond avec une classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ et, par suite, aucune des classes $M^{(n)}$ ne contient plus d'un élément de n'importe quel système d'éléments générateurs libres du groupe G.

Il s'ensuit qu'aucun système d'éléments générateurs libres de G ne saurait contenir deux éléments d'une même classe $M^{(n)}$, quel que soit $n = 2, 3, \ldots$.

CLASSES $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ DÉPENDANTES ET INDÉPENDANTES. — Soit G un groupe libre engendré par un ensemble infini A d'éléments générateurs libres, soit n un entier $\geqq 2$ et soit $\Gamma^{(n)}$ le groupe abélien associé à G et comprenant toutes les classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$.

Soit d'abord $\mathfrak{M}_t$ un sous-ensemble fini de $\Gamma^{(n)}$ composé des classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a^i \end{pmatrix}_{a\in A}$ $(i=1, 2, \ldots, t)$. Nous disons que ces t classes sont indépendantes si l'égalité

$$\text{(I)} \qquad \left[M^{(n)}\begin{pmatrix} a \\ \lambda_a^1 \end{pmatrix}_{a\in A}\right]^{\alpha_1}\left[M^{(n)}\begin{pmatrix} a \\ \lambda_a^2 \end{pmatrix}_{a\in A}\right]^{\alpha_2}\cdots\left[M^{(n)}\begin{pmatrix} a \\ \lambda_a^t \end{pmatrix}_{a\in A}\right]^{\alpha_t} = M^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A},$$

où $\alpha_1, \alpha_2, \ldots, \alpha_t$ sont des entiers, implique que $\alpha_i \equiv 0 \pmod{n}$ $(i=1, 2, \ldots, t)$ et nous disons que les t classes considérées sont dépendantes ou liées s'il existe un système d'entiers $\alpha_1, \alpha_2, \ldots, \alpha_t$ dont l'un au moins n'est pas congru à 0 modulo n et qui satisfont l'égalité (I).

Soit $A^\star = \{a_1, a_2, \ldots, a_k\}$ le sous-ensemble fini de A, comprenant tous les éléments a de A, tels que l'un au moins des nombres λ_a^i $(i=1, 2, \ldots, t)$ est >0. Soit $G^\star$ le groupe libre engendré par $A^\star$. Répartissons les éléments de $G^\star$ en classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^\star}$. On a

$$M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^\star} \subset M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}.$$

Il ressort aussitôt de la loi de composition des classes $M^{(n)}$ que la condition nécessaire et suffisante pour que les t classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a^i \end{pmatrix}_{a\in A^\star}$ soient indépendantes est aussi la condition nécessaire et suffisante pour que les t classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a^i \end{pmatrix}_{a\in A}$ soient indépendantes et *vice versa*. Les propositions 5-7 permettent donc de décider si les classes de $\mathfrak{M}_t$ sont indépendantes ou si elles sont liées.

Soit maintenant $\mathfrak{M}$ un sous-ensemble infini de $\Gamma^{(n)}$. Nous dirons que les classes de cet ensemble $\mathfrak{M}$ sont indépendantes si, quel que soit le sous-ensemble fini $\mathfrak{M}_t$ de $\mathfrak{M}$, il est formé de classes indépendantes dans le sens précisé plus haut.

On démontre sans peine que quel que soit l'ensemble B formé d'éléments libres, générateur de G, et quel que soit l'entier $n \geqq 2$, l'ensemble des classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ qui contiennent des éléments de B est formé de classes indépendantes. De même, tout ensemble irréductible de classes $M^{(n)}$, générateur du groupe $\Gamma^{(n)}$ est formé de classes $M^{(n)}$ indépendantes.

Proposition 34. — *Quel que soit le sous-groupe g du groupe libre G engendré par l'ensemble A d'éléments générateurs libres et quelles que soient les classes* $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A}$ *et* $M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A}$ *qui contiennent des éléments de g, les deux ensembles*

$$M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A} \cap g \qquad \text{et} \qquad M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A} \cap g$$

sont d'égale puissance.

Démonstration. — Soit g un sous-groupe quelconque du groupe libre G et soient $\mathbf{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}$ et $\mathbf{M}^{(n)}\binom{a}{\mu_a}_{a\in A}$ deux classes $\mathbf{M}^{(n)}$ qui contiennent l'une et l'autre au moins un élément de g. Montrons que les ensembles

$$g_1 = \mathbf{M}^{(n)}\binom{a}{\lambda_a}_{a\in A} \cap g \qquad \text{et} \qquad g_2 = \mathbf{M}^{(n)}\binom{a}{\mu_a}_{a\in A} \cap g$$

sont d'égale puissance. En effet, soit c un élément quelconque de G qui fait partie de la classe $\mathbf{M}^{(n)}\binom{a}{\nu_a}_{a\in A}$, où ν_a est le nombre de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence

$$\nu_a \equiv \mu_a - \lambda_a \qquad (\bmod n),$$

quel que soit l'élément a de A. Soit d_1 un élément de g qui fait partie de l'ensemble g_1 et d_2 un élément de l'ensemble g_2. Comme g est un groupe, l'élément $d_3 = d_1^{-1} d_2$ fait partie de g. Or cet élément fait partie de la classe $\mathbf{M}^{(n)}\binom{a}{\nu_a}_{a\in A}$. Donc, d'après la loi de composition des classes $\mathbf{M}^{(n)}$,

$$\mathbf{M}^{(n)}\binom{a}{\lambda_a}_{a\in A} \mathbf{M}^{(n)}\binom{a}{\nu_a}_{a\in A} = \mathbf{M}^{(n)}\binom{a}{\mu_a}_{a\in A}.$$

Il s'ensuit que l'ensemble $g_1 d_3$ est contenu dans la classe $\mathbf{M}^{(n)}\binom{a}{\mu_a}_{a\in A}$. Et comme tous les éléments de $g_1 d_3$ font partie de g, puisque g est un groupe qui contient g_1 et d_3, et que la partie commune à $\mathbf{M}^{(n)}\binom{a}{\mu_a}_{a\in A}$ et à g est l'ensemble g_2, on a l'inclusion

$$(+) \qquad g_1 d_3 \subset g_2.$$

Soit $d_4 = d_3^{-1}$. C'est un élément du groupe g qui fait partie de la classe $\mathbf{M}^{(n)}\binom{a}{n-\nu_a}_{a\in A}$ et comme

$$\mathbf{M}^{(n)}\binom{a}{\mu_a}_{a\in A} \mathbf{M}^{(n)}\binom{a}{n-\nu_a}_{a\in A} = \mathbf{M}^{(n)}\binom{a}{\lambda_a}_{a\in A},$$

l'ensemble $g_2 d_4$ est contenu dans la classe $\mathbf{M}^{(n)}\binom{a}{\lambda_a}_{a\in A}$. Et comme il est composé uniquement d'éléments de g, on a aussi l'inclusion

$$(++) \qquad g_2 d_4 \subset g_1.$$

Or les deux inclusions $(+)$ et $(++)$ montrent que les deux ensembles g_1 et g_2 sont d'égale puissance.

C. Q. F. D.

Proposition 35. — *Soit G un groupe libre engendré par un ensemble A de puissance $\mathfrak{m}$ d'éléments générateurs libres. Alors G possède une infinité de puissance supérieure à $\mathfrak{m}$ de sous-groupes qui ne sont ni invariants, ni maxima.*

Démonstration. — En effet, quel que soit le sous-ensemble $A^\star$ de A, il engendre un sous-groupe propre $G^\star$ de G et à deux sous-ensembles distincts $A^\star$ et $A^{\star\star}$ de A correspondent évidemment deux sous-groupes distincts $G^\star$ et $G^{\star\star}$ de G. Le sous-groupe $G^\star$ engendré par un sous-ensemble propre $A^\star$ de A n'est pas invariant. En effet, quel que soit l'élément a de l'ensemble $A - A^\star$, le transmué d'un élément non neutre quelconque de $G^\star$ par a ne fait pas partie de $G^\star$ puisque A est formé d'éléments libres. D'autre part, $G^\star$ n'est pas un sous-groupe maximum de G puisque, quel que soit l'élément a de $A - A^\star$ et quel que soit l'entier $m \neq 0, 1, -1$, l'ensemble $A^\star \cup a^m$ engendre un groupe G_1 qui contient $G^\star$ et qui ne saurait être confondu avec G puisqu'il ne contient pas l'élément a. La proposition est donc démontrée.

Remarque 21. — Soit G un groupe libre engendré par un ensemble A d'éléments libres. Soit n un entier quelconque ≥ 1, mais ne dépassant pas le nombre d'éléments de A, soient $a_1, a_2, \ldots, a_n$ n éléments quelconques de A et soient $m_1, m_2, \ldots, m_n$ n entiers quelconques, $\neq 0, +1$ ou -1. Alors l'élément $a = a_1^{m_1} a_2^{m_2} \ldots a_n^{m_n}$ du groupe G n'est pas libre, il ne fait partie d'aucun système d'éléments générateurs libres de G.

En effet, soit $A^\star = \{a_1, a_2, \ldots, a_n\}$ et soit $G^\star$ le groupe libre engendré par $A^\star$. D'après la proposition 23, pour prouver que l'élément a n'est pas libre dans G, il suffit de prouver que a est un élément non libre du groupe $G^\star$. Or $G^\star$ est un groupe libre à un nombre fini n d'éléments générateurs libres, et l'on sait (*voir*, par exemple, Kurosh, *Théorie des groupes*, 2e édition russe, p. 252 et suiv.) que quel que soit le système $b_1, b_2, \ldots, b_n$ formé de n éléments générateurs de $G^\star$, ces n éléments sont à leur tour libres, et que le groupe $G^\star$ ne saurait être engendré par moins de n éléments. On le démontre en prouvant que si les éléments $b_1, b_2, \ldots, b_n$ sont générateurs de $G^\star$, chacun des éléments $a_1, a_2, \ldots, a_n$ peut être obtenu à partir de l'ensemble $B^\star = \{b_1, b_2, \ldots, b_n\}$ en effectuant un nombre fini d'opérations de deux types. L'opération du premier type consiste à remplacer un élément c dans l'ensemble considéré de générateurs de $G^\star$ par son inverse c^{-1}. L'opération du second type consiste à remplacer un élément quelconque c de l'ensemble considéré par fc ou par cf, f étant une composition finie quelconque d'éléments $\neq c$ du système envisagé de générateurs de $G^\star$. Or il est clair que si un ensemble $B = \{b_1, b_2, \ldots, b_n\}$ formé de n éléments de $G^\star$ comprend parmi ses éléments l'élément a, par application finie des deux procédés que nous venons de décrire, il est impossible d'en déduire au moins un des éléments $a_1, a_2, \ldots, a_n$ et, par suite, l'ensemble B ne saurait être générateur de $G^\star$, ce qui démontre que a ne saurait faire partie d'aucun ensemble formé de n éléments générateurs de $G^\star$ et, par suite, qu'il n'est pas libre. N'étant pas libre dans $G^\star$, il ne saurait également pas être libre dans G.

Remarque 22. — Soit G un groupe libre engendré par un ensemble A d'éléments générateurs libres. Soit $A^\star$ un sous-ensemble propre de A et soit $G^\star$ le groupe libre qu'il engendre. Soit B un second système d'éléments générateurs libres de G. Chaque élément de $A^\star$ peut être obtenu par composition finie d'éléments de B, mais l'ensemble d'éléments de B nécessaire à former, par composition finie, tous les éléments de $A^\star$, peut être de puissance supérieure à celle de A. Il peut même se confondre avec l'ensemble B tout entier. En voici un exemple. Soit G le groupe libre engendré par les cinq éléments libres de l'ensemble $A=\{a_1, a_2, a_3, a_4, a_5\}$, soit $A^\star=\{a_1, a_2, a_3\}$ et soit $B=\{b_1, b_2, b_3, b_4, b_5\}$, où

$$b_1=a_1^6 a_2, \quad b_2=a_1^5 a_4, \quad b_3=a_1^4 a_4, \quad b_4=a_3^6 a_5, \quad b_5=a_3^5 a_5.$$

L'ensemble B ne contient aucun sous-ensemble formé de trois éléments générateurs du groupe $G^\star$ engendré par $A^\star$. On a

$$b_2 b_3^{-1}=a_1, \quad a_1^{-6} b_1=a_2, \quad a_1^{-5} b_2=a_4, \quad b_4 b_5^{-1}=a_3 \quad \text{et} \quad a_3^{-5} b_5=a_5.$$

Pour obtenir par composition finie les trois éléments de $A^\star$ à partir de B, il faut utiliser les cinq éléments de B.

L'élément b_1 fait partie de $G^\star$ et c'est un élément libre de $G^\star$.

Remarque 23. — Soit G un groupe libre engendré par un ensemble A de puissance $\mathfrak{m}$ d'éléments générateurs libres. Alors l'ensemble des automorphismes extérieurs de G est de puissance $\geq 2^{\mathfrak{m}} > \mathfrak{m}$. En effet, soit A_1 un sous-ensemble quelconque de A. Remplaçons dans A chaque élément de A_1 par son inverse. On obtient de nouveau un système $A^\star$ d'éléments générateurs libres de G. Faisons correspondre à tout élément a de A l'élément $a^\star=a^{-1}$ si $a \in A_1$, ou l'élément $a^\star=a$ si $a \in A - A_1$ et faisons correspondre à toute composition finie $f(a_1, a_2, \ldots, a_k)$ d'éléments de G la même composition $f(a_1^\star, a_2^\star, \ldots, a_k^\star)$ des éléments correspondants de $A^\star$. Cette correspondance est un automorphisme extérieur de G et à deux sous-ensembles différents de A correspondent ainsi deux automorphismes distincts de G. L'ensemble des automorphismes extérieurs du groupe G est donc bien de puissance supérieure à $\mathfrak{m}$.

C. Q. F. D.

Remarque 24. — Soit G un groupe libre engendré par un ensemble A d'éléments générateurs libres, de puissance $\mathfrak{m}$. Il existe alors un ensemble de puissance $2^{\mathfrak{m}} > \mathfrak{m}$ de sous-groupes propres de G qui sont holoédriquement isomorphes au groupe G. En effet, soit A_1 un sous-ensemble quelconque de A. Faisons correspondre à tout élément a_1 de A_1 un entier $m_{a_1} \neq 0, +1, -1$, mais à part cela quelconque et remplaçons dans l'ensemble A tout élément a_1 de A_1 par l'élément $a_1^{m_{a_1}}$. Soit $A^\star$ l'ensemble ainsi obtenu à partir de A et soit $G^\star_{A_1}$ le groupe qu'il engendre. G est le produit libre des groupes cycliques engendrés par les éléments de A alors que $G^\star_{A_1}$ est le produit libre des groupes cycliques engendrés par les éléments de $A^\star$. $G^\star_{A_1}$ est un sous-groupe propre de G, puisque aucun élément de l'ensemble A_1 contenu dans G ne fait partie de $G^\star_{A_1}$. Or les groupes G et $G^{\star}_{A_1}$ sont (holoédriquement) isomorphes. Pour établir un isomorphisme entre ces deux groupes libres, il suffit de faire correspondre à tout élément a_1 de A_1 l'élément $a_1^{m_{a_1}}$ de $A^{\star}$, à tout élément a de $A - A_1$ le même élément a de $A^{\star}$, et à toute composition finie d'éléments de A la même composition des éléments correspondants de $A^{\star}$. Et comme à deux sous-ensembles distincts A_1 et A_2 de l'ensemble A correspondent deux sous-groupes propres distincts $G^{\star}_{A_1}$ et $G^{\star}_{A_2}$ de G, notre assertion est démontrée.

Généralisations.

III. Soit G un groupe libre engendré par un ensemble A fini ou infini, d'éléments générateurs libres. Soit $A^{\star}$ un sous-ensemble propre quelconque (fini ou infini) de A et soit n un entier $\geqq 2$. On peut répartir les éléments de G en classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^{\star}}$ comme suit. Soit c un élément quelconque du groupe G, soit u_a son degré par rapport à l'élément a de $A^{\star}$ et soit λ_a le nombre de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence $u_a \equiv \lambda_a \pmod{n}$, quel que soit $a \in A^{\star}$. Nous dirons que c fait partie de la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^{\star}}$. On répartit ainsi tous les éléments de G en classes d'équivalence disjointes deux à deux, dont chacune est infinie et contient avec tout élément c de G la classe entière des éléments de G conjugués à c. Si l'on appelle produit de deux telles classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^{\star}}$ et $M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A^{\star}}$ l'ensemble des éléments de G de la forme bc,

$$b \in M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^{\star}}, \qquad c \in M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A^{\star}},$$

on démontre sans peine que

$$M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^{\star}} M^{(n)}\begin{pmatrix} a \\ \mu_a \end{pmatrix}_{a\in A^{\star}} = M^{(n)}\begin{pmatrix} a \\ \nu_a \end{pmatrix}_{a\in A^{\star}},$$

où ν_a désigne l'élément de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence

$$\nu_a \equiv \lambda_a + \mu_a \pmod{n},$$

quel que soit $a \in A^{\star}$.

Avec cette loi de composition, les classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^{\star}}$ forment un groupe abélien $\Gamma^{(n)\star}$ dont l'élément neutre est la classe nulle $M^{(n)}\begin{pmatrix} a \\ 0 \end{pmatrix}_{a\in A^{\star}}$, l'inverse de la classe $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^{\star}}$ étant la classe $M^{(n)}\begin{pmatrix} a \\ n-\lambda_a \end{pmatrix}_{a\in A^{\star}}$. Les groupes $\Gamma^{(n)\star}$ sont également associés au groupe libre G et permettent de déceler de nombreux sous-groupes invariants de G. La plupart des résultats établis pour les groupes $\Gamma^{(n)}$ subsistent pour les groupes $\Gamma^{(n)\star}$, mais les classes $M^{(n)}\begin{pmatrix} a \\ \lambda_a \end{pmatrix}_{a\in A^{\star}}$ n'ont plus un caractère intrinsèque et la classe nulle $\mathrm{M}^{(n)}\binom{a}{0}_{a\in\mathrm{A}^\star}$ peut contenir des éléments libres de G.

IV. Soit G un groupe libre engendré par un ensemble A (fini ou infini) d'éléments générateurs libres. Faisons correspondre à tout élément a de A un entier $n_a \geqq 2$. Soit c un élément quelconque de G, soit u_a son degré par rapport à l'élément a de A et soit λ_a le nombre de la suite $0, 1, \ldots, n_a - 1$ qui satisfait la congruence $\lambda_a \equiv u_a \pmod{n_a}$ quel que soit $a \in \mathrm{A}$. Nous dirons que l'élément c fait partie de la classe $\mathrm{M}^{\{n_a\}}\binom{a}{\lambda_a}_{a\in\mathrm{A}}$. On répartit ainsi les éléments de G en classes disjointes, dont chacune est infinie et contient avec tout élément c de G la classe entière des éléments de G conjugués à c. Appelons produit de deux classes $\mathrm{M}^{\{n_a\}}\binom{a}{\lambda_a}_{a\in\mathrm{A}}$ et $\mathrm{M}^{\{n_a\}}\binom{a}{\mu_a}_{b\in\mathrm{A}}$ l'ensemble des éléments de G de la forme bc,

$$b \in \mathrm{M}^{\{n_a\}}\binom{a}{\lambda_a}_{a\in\mathrm{A}}, \qquad c \in \mathrm{M}^{\{n_a\}}\binom{a}{\mu_a}_{a\in\mathrm{A}}.$$

On a

$$\mathrm{M}^{\{n_a\}}\binom{a}{\lambda_a}_{a\in\mathrm{A}} \mathrm{M}^{\{n_a\}}\binom{a}{\mu_a}_{a\in\mathrm{A}} = \mathrm{M}^{\{n_a\}}\binom{a}{\nu_a}_{a\in\mathrm{A}},$$

où ν_a est le nombre de la suite $0, 1, \ldots, n_a - 1$ qui satisfait la congruence

$$\nu_a \equiv \lambda_a + \mu_a \pmod{n_a},$$

quel que soit $a \in \mathrm{A}$. Avec cette loi de composition les classes $\mathrm{M}^{\{n_a\}}\binom{a}{\lambda_a}_{a\in\mathrm{A}}$ forment un groupe abélien $\Gamma^{\{n_n\}}$ qui est également associé au groupe libre G, dont l'élément neutre est la classe nulle $\mathrm{M}^{\{n_n\}}\binom{a}{0}_{a\in\mathrm{A}}$, l'inverse d'une classe $\mathrm{M}^{\{n_n\}}\binom{a}{\lambda_a}_{a\in\mathrm{A}}$ étant la classe $\mathrm{M}^{\{n_a\}}\binom{a}{n_a - \lambda_a}_{a\in\mathrm{A}}$. Les groupes $\Gamma^{\{n_a\}}$ possèdent des propriétés analogues à celles des groupes $\Gamma^{(n)}$ et permettent à leur tour de déceler de nombreux sous-groupes invariants du groupe libre G. Mais les classes $\mathrm{M}^{\{n_a\}}\binom{a}{\lambda_a}_{a\in\mathrm{A}}$ n'ont pas un caractère intrinsèque et la classe nulle $\mathrm{M}^{\{n_a\}}\binom{a}{0}_{a\in\mathrm{A}}$ contient des éléments libres de G.

Si, au lieu de A, on considère un sous-ensemble quelconque $\mathrm{A}^\star$ de A et si l'on fait correspondre à tout élément a de $\mathrm{A}^\star$ un entier $n_a \geqq 2$, cet entier pouvant varier d'un élément à l'autre de $\mathrm{A}^\star$, en employant les mêmes notations que ci-dessus, on peut répartir les éléments de G en classes $\mathrm{M}^{\{n_a\}}\binom{a}{\lambda_a}_{a\in\mathrm{A}^\star}$ disjointes deux à deux dont chacune contient avec tout élément c de G la classe entière des éléments de G conjuguée à c et l'on peut définir pour ces classes une loi de composition commutative et associative qui conduit à de nouveaux groupes abéliens associés au groupe G.

V. Soit G un groupe libre non cyclique, engendré par un ensemble A (fini ou infini) d'éléments générateurs libres. Soit n un entier ≥ 2, soit t un entier fixe ≥ 2, mais non supérieur au nombre d'éléments de A, soit c un élément quelconque du groupe G, soit $A_t = \{a_1, a_2, \ldots, a_t\}$ un système quelconque formé de t éléments distincts de A, soit u_{A_t} le degré de c par rapport à l'ensemble des éléments de A_t et soit λ_{A_t} le nombre de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence $\lambda_{A_t} \equiv u_{A_t} \pmod{n}$. Nous dirons que c est de classe $M^{(n)}\begin{pmatrix} A_t \\ \lambda_{A_t} \end{pmatrix}_{A_t \subset A}$. On répartit ainsi à nouveau l'ensemble des éléments de G en classes d'équivalence, disjointes deux à deux, dont chacune est infinie et contient, avec tout élément c de G la classe entière des éléments de G conjugués à c. Appelons produit de deux classes $M^{(n)}\begin{pmatrix} A_t \\ \lambda_{A_t} \end{pmatrix}_{A_t \subset A}$ et $M^{(n)}\begin{pmatrix} A_t \\ \mu_{A_t} \end{pmatrix}_{A_t \subset A}$ l'ensemble des éléments de G de la forme bc,

$$b \in M^{(n)}\begin{pmatrix} A_t \\ \lambda_{A_t} \end{pmatrix}_{A_t \subset A} \qquad \text{et} \qquad c \in M^{(n)}\begin{pmatrix} A_t \\ \mu_{A_t} \end{pmatrix}_{A_t \subset A}.$$

On a

$$M^{(n)}\begin{pmatrix} A_t \\ \lambda_{A_t} \end{pmatrix}_{A_t \subset A} M^{(n)}\begin{pmatrix} A_t \\ \mu_{A_t} \end{pmatrix}_{A_t \subset A} = M^{(n)}\begin{pmatrix} A_t \\ \nu_{A_t} \end{pmatrix}_{A_t \subset A},$$

où ν_{A_t} est le nombre de la suite $0, 1, \ldots, n-1$ qui satisfait la congruence

$$\nu_{A_t} \equiv \lambda_{A_t} + \mu_{A_t} \pmod{n}$$

quel que soit le système A_t formé de t éléments distincts de A. Avec cette loi de composition, les classes $M^{(n)}\begin{pmatrix} A_t \\ \lambda_{A_t} \end{pmatrix}_{A_t \subset A}$ forment à leur tour un groupe abélien $\Gamma_t^{(n)}$ dont l'élément neutre est la classe nulle $M^{(n)}\begin{pmatrix} A_t \\ 0 \end{pmatrix}_{A_t \subset A}$. En faisant varier n et t, on associe ainsi au groupe libre G encore une infinité de groupes abéliens qui permettent de déceler de nombreux sous-groupes invariants de G. Ici encore les classes $M^{(n)}\begin{pmatrix} A_t \\ \lambda_{A_t} \end{pmatrix}_{A_t \subset A}$ n'ont pas un caractère intrinsèque et la classe nulle $M^{(n)}\begin{pmatrix} A_t \\ \lambda_{A_t} \end{pmatrix}_{A_t \subset A}$ peut contenir des éléments libres de G.

En prenant, au lieu de A un sous-ensemble propre quelconque $A^\star$ de A, on peut encore répartir d'une infinité de façons en classes d'équivalences les éléments de G en se donnant un entier fixe quelconque $n \geq 2$ et en considérant le degré de tout élément c de G par rapport aux systèmes de t éléments de $A^\star$. Chacune de ces classes contient, avec tout élément c de G la classe entière des éléments de G conjugués à c et l'on peut définir pour ces nouvelles classes une loi de composition commutative et associative qui conduit à un nouvel ensemble de groupes abéliens associés à G.

Tous ces groupes abéliens sont intimement liés à la structure d'un groupe libre, ils permettent de déceler une infinité indénombrable de sous-groupes invariants dans tout groupe libre engendré par un ensemble infini A d'éléments générateurs libres, ils facilitent la recherche des éléments libres de G et ils permettent d'établir l'existence de classes très étendues d'éléments non libres.