ANNALES SCIENTIFIQUES DE L'É.N.S.

LÉO KALOUJNINE

La structure des p-groupes de Sylow des groupes symétriques finis

Annales scientifiques de l'É.N.S. 3^e série, tome 65 (1948), p. 239-276

<http://www.numdam.org/item?id=ASENS_1948_3_65__239_0>

LA

STRUCTURE DES p-GROUPES DE SYLOW

DES

GROUPES SYMÉTRIQUES FINIS

PAR M. LÉO KALOUJNINE.

INTRODUCTION.

Le présent Mémoire est consacré à l'étude des p-groupes de Sylow des groupes symétriques dont le degré est une puissance p^m d'un nombre premier p. Ces groupes, qui seront désignés par $\mathfrak{P}_m$, jouent, relativement aux p-groupes, un rôle analogue à celui que les groupes symétriques jouent relativement aux groupes finis.

Le fait de considérer seulement des groupes symétriques de degré p^m n'est pas une restriction artificielle. Il est facile de montrer que les p-groupes de Sylow d'un groupe symétrique quelconque sont des produits directs de tels groupes $\mathfrak{P}_m$. De façon précise, si le nombre entier n s'écrit dans le système de numération de base p :

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_m p^m,$$

un p-groupe de Sylow du groupe symétrique de degré n est isomorphe au produit direct

$$\mathfrak{P}_1^{a_1} \times \mathfrak{P}_2^{a_2} \times \ldots \times \mathfrak{P}_m^{a_m}.$$

On peut représenter les groupes $\mathfrak{P}_m$ par des systèmes, que j'appelle tableaux, de m polynomes, à $m-1$ variables, dont les coefficients sont des classes d'entiers, mod p (ou des éléments d'un champ de Galois de p éléments). Entre ces systèmes existe une loi de composition, définie par des opérations

rationnelles relativement simples. On peut ainsi traduire tout problème sur les groupes $\mathfrak{P}_m$ en un problème sur les polynomes, dans un champ de Galois. Il est vrai que, dans la plupart des cas, on aboutit ainsi à des problèmes qui sont loin d'être résolus. Cependant il est des cas pour lesquels on obtient une réponse satisfaisante et quasi définitive. C'est ainsi qu'on peut déterminer tous les sous-groupes caractéristiques d'un groupe $\mathfrak{P}_m$, et les caractériser par des systèmes de m entiers satisfaisant à certaines conditions.

Les résultats obtenus sont formulés dans les Chapitres IV et V, sous forme d'un certain nombre de théorèmes. Les démonstrations en sont basées sur quelques lemmes simples et sur quelques inégalités qui sont établis aux Chapitres II et III; le Chapitre I indiquant le principe de la représentation des groupes par des tableaux de polynomes. Si ces inégalités pouvaient être précisées, elles permettraient sans doute de trouver d'autres propriétés intéressantes des groupes $\mathfrak{P}_m$ et de leurs sous-groupes.

Cependant le problème de la détermination de tous les sous-groupes des groupes $\mathfrak{P}_m$ et de leur description précise semble exiger des moyens qui dépassent de loin nos connaissances actuelles. Il peut néanmoins être traité complètement dans le cas des groupes $\mathfrak{P}_2$. C'est ce que j'ai fait dans le Chapitre VI. Une grande partie des résultats que j'ai ainsi obtenus semble avoir été trouvée déjà par d'autres méthodes. J'ai pensé qu'il y avait quelque intérêt à les reprendre avec l'algorithme du présent travail. On peut voir mieux ainsi le mécanisme du calcul, et il n'est pas impossible de penser que leur étude pourra servir à une étude ultérieure des groupes $\mathfrak{P}_3$.

Dans un autre Mémoire qui sera publié ultérieurement, j'étudie quelques généralisations des idées dont je me suis servi dans le présent travail, en étudiant les groupes $\mathfrak{P}_\infty$ des tableaux formés par une suite infinie dénombrable de polynomes à coefficients dans des champs de Galois.

Le présent Mémoire et sa généralisation ont été présentés à l'Université de Paris comme Thèse de Doctorat. J'exprime toute ma gratitude à MM. É. Cartan, G. Darmois et A. Châtelet, qui ont bien voulu être membres du Jury. Je tiens à remercier plus spécialement M. Châtelet pour le vif intérêt qu'il a pris au présent travail et les conseils qu'il m'a prodigués, pour son développement et pour sa rédaction.

J'adresse encore mes remercîments à M. H. Cartan pour l'intérêt qu'il a pris à mes recherches et pour ses encouragements, et à M. Krasner dont les critiques et les conseils m'ont été précieux et m'ont permis d'améliorer mon exposé.

Je suis également très reconnaissant à MM. É. Cartan et J. Hadamard qui, à plusieurs reprises, ont présenté mes Notes sur ces sujets à l'Académie des Sciences, et plus spécialement à M. Paul Montel, qui n'a pas hésité à accueillir et faire publier une de mes Notes, pendant mon internement par la Gestapo, au camp de Compiègne; en acceptant ce travail dans les *Annales de l'École Normale*

Supérieure, il m'a donné une nouvelle preuve de confiance et d'estime dont je sens profondément tout le prix.

Notations. — Dans tout ce Mémoire, p désigne un *entier premier*, arbitraire, mais fixe, qui sera parfois supposé impair (Chap. V).

On désignera par :

G_p, le *corps des restes* des entiers rationnels, mod p (champ de Galois de p éléments);

E_s l'*espace vectoriel*, de dimension s sur G_p (puissance directe G_p^s);

X_s, de coordonnées $x_1, x_2, \ldots, x_s$ (définies mod p), un *vecteur* de E_s.

Les *groupes* sont toujours désignés par des lettres gothiques majuscules : $\mathfrak{A}$, $\mathfrak{E}$, $\mathfrak{G}$, $\mathfrak{K}$, $\mathfrak{H}$, $\mathfrak{L}$, $\mathfrak{W}$, $\mathfrak{V}$, $\mathfrak{P}$, $\mathfrak{R}$, $\mathfrak{S}$, $\mathfrak{D}$, $\mathfrak{Z}$ éventuellement affectées d'indices.

Des éléments d'un groupe, ou des groupes eux-mêmes, entre accolades, $\{a, b, c\}$, $\{\mathfrak{E}_\alpha \mathfrak{E}_\rho\}$, ... désignent le groupe engendré par ces éléments, ou par les éléments de ces groupes.

On emploie deux sortes de *commutateurs*, notés par des lettres entre parenthèses :

(a, b), commutateur des éléments a, b, égal à $aba^{-1}b^{-1}$;

$(\mathfrak{G}, \mathfrak{L})$, sous-groupe engendré par les commutateurs de tout élément de $\mathfrak{G}$ avec tout élément de $\mathfrak{L}$.

Les groupes abéliens de type $(p, p, \ldots, p)$ sont appelés *élémentaires*.

Le *groupe symétrique*, de degré n (et d'ordre $n!$) est désigné par $\mathfrak{S}_n$.

Le p-groupe de Sylow de $\mathfrak{S}_{p^m}$, défini à un isomorphisme près, est désigné par $\mathfrak{P}_m$.

On utilise les signes ordinaires de la théorie des ensembles :

$\subset$ inclusion stricte; $<$ inégalité stricte;

$\subseteqq$ inclusion large; $\leqq$ inégalité large.

CHAPITRE I.

LES TABLEAUX DE RANG m.

Considérons un ensemble de T de p^m éléments et le groupe des permutations $\mathfrak{S}_{p^m}$ de T; c'est-à-dire le groupe symétrique de degré p^m. La contribution de p dans son ordre $p^m!$ est $p^{p^{m-1}+p^{m-2}+\ldots+1}$; c'est l'ordre commun de ses p-groupes de Sylow, $\mathfrak{P}_m$ (tous isomorphes entre eux).

Étant donné un p-groupe quelconque $\mathfrak{G}$, il existe une représentation fidèle de $\mathfrak{G}$ comme groupe de permutations dont le degré est une puissance p^m. Alors, en raison des théorèmes de Sylow, dans tout $\mathfrak{P}_m$, il existe un sous-

groupe isomorphe à $\mathfrak{G}$. On voit donc combien l'étude des $\mathfrak{P}_m$ est importante pour la théorie générale des p-groupes.

J'ai réussi à construire explicitement, pour tout m, un p-groupe de Sylow $\mathfrak{P}_m$ de $\mathfrak{S}_{p^m}$ sous une forme qui en permet une étude approfondie. Cette construction et cette étude sont l'objet principal de ce travail.

Représentons T par l'ensemble des vecteurs X_m (de coordonnées $x_1, x_2, \ldots, x_m$, du champ de Galois G_p, ou définies mod p) de l'espace E_m puissance directe G_p^m et désignons par $T_{x_1 x_2 \ldots x_s}$ l'ensemble des éléments de T qui, dans E_m, ont pour premières coordonnées $x_1, x_2, \ldots, x_s$. Une transformation ponctuelle biunivoque de l'espace E_m est, en même temps, une permutation des éléments de T, donc, à une similitude près, un élément du groupe $\mathfrak{S}_{p^m}$.

Considérons alors des opérations $\pi(a)$, $\pi\big(a(x_1)\big), \ldots, \pi\big(a(x_1, x_2, \ldots, x_{m-1})\big)$, dans lesquelles $a(x_1, x_2, \ldots, x_s)$ est une fonction dont la valeur est dans G_p et dont la variable est un vecteur X_s (de coordonnées $x_1, x_2, \ldots, x_s$) de l'espace E_s. Elles sont définies comme suit :

1° $\pi(a)$ est une permutation circulaire des ensembles T_{x_1}, qui, à x_1 fait correspondre $x_1 + a$ (sur la figure c'est une rotation du grand cercle T, d'angle $2\pi\frac{a}{p}$).

2° $\pi\big(a(x_1)\big)$ est une permutation circulaire, variable avec x_1, de l'ensemble $T_{x_1 x_2}$ (de première coordonnée x_1), qui, à x_1, x_2 fait correspondre x_1, $x_2 + a(x_1)$. (Sur la figure ce sont p rotations des cercles T_{x_1}, d'angles respectifs $2\pi\frac{a(x_1)}{p}$.)

En général :

$\pi\big(a(x_1, x_2, \ldots, x_{s-1})\big)$ est une permutation circulaire, variable avec X_{s-1}, de l'ensemble $T_{x_1 x_2 \ldots x_s}$ (de premières coordonnées X_{s-1}), qui, à $(x_1, x_2, \ldots, x_{s-1}, x_s)$ fait correspondre

$$\big(x_1, x_2, \ldots, x_{s-1}, x_s + a(x_1, x_2, \ldots, x_{s-1})\big).$$

(Sur la figure ce serait p^{s-1} rotations des cercles $T_{x_1 x_2 \ldots x_{s-1}}$, d'angles respectifs $2\pi\frac{a(x_1, x_2, \ldots, x_{s-1})}{p}$.)

Le produit α des permutations π

$$\pi\big(a(x_1, x_2, \ldots, x_{m-1})\big), \ldots, \pi\big(a(x_1)\big)\pi(a)$$

(dans l'ordre droite gauche) est une transformation ponctuelle de E_m (ou une

permutation de T) qui est représentée par un *tableau* A_m (ou simplement A), dit de *rang m*,

$$A=\begin{pmatrix} a \\ a(x_1) \\ \cdots \\ a(x_1,x_2,\ \ldots,\ x_{m-1}) \end{pmatrix}=[\,a,\,a(x_1),a(x_1,x_2),\ \ldots,(x_1,\ldots,x_{m-1})\,].$$

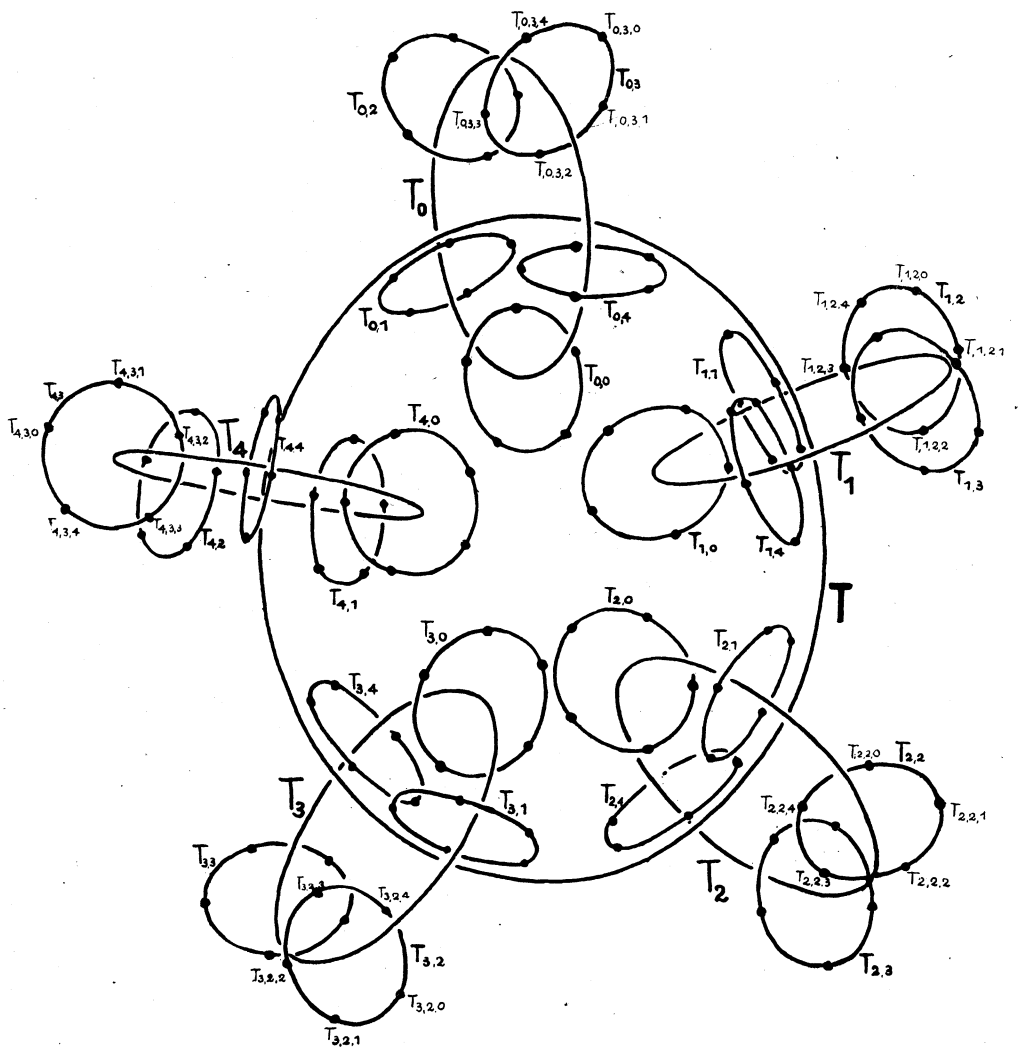

Fig. 1.

Les fonctions $[A]_s=a(x_1, x_2, \ldots, x_{s-1})$ seront appelées les coordonnées de la transformation α, ou du tableau A, et l'on désignera par A_s le tableau de rang s, dont les coordonnées sont égales aux s premières coordonnées de α. Le nombre de fonctions $a(x_1, x_2, \ldots, x_s)$ étant p^{p^s}, le nombre de transformations α est $p^{p^{m-1}+p^{m-2}+\ldots+1}$.

On vérifie immédiatement que la loi de composition de deux tableaux (ou transformations) est :

A. de coordonnées $a(x_1, x_2, \ldots, x_s)$; B. de coordonnées $b(x_1, x_2, \ldots, x_s)$; AB. (B, puis A) a pour coordonnées (s de 0 à $m-1$)

$$(1.1)\quad a(x_1, x_2, \ldots, x_s) + b\big(x_1 - a,\ x_2 - a(x_1),\ \ldots,\ x_s - a(x_1, x_2, \ldots, x_{s-1})\big).$$

La transformation unité est représentée par un tableau de coordonnées toutes nulles. L'inverse du tableau a pour coordonnées

$$(1.2)\quad -a\big(x_1 + a,\ x_2 + a(x_1 + a),\ \ldots,\ x_s + a\,(x_1 + a,\ x_2 + a(x_1 + a),\ \ldots)\big).$$

Il en résulte la propriété :

Théorème 1. — *Les transformations α forment un groupe $\mathfrak{P}_m$, d'ordre $p^{p^{m-1}+p^{m-2}+\ldots+1}$, isomorphe à un sous-groupe de $\mathfrak{S}_{p^m}$, notamment à un p-groupe de Sylow de $\mathfrak{S}_{p^m}$ (puisqu'il a le même ordre).*

Un tableau sera dit *de profondeur r* lorsque

$$[A]_s = 0, \quad \text{pour } s \leq r \quad \text{et} \quad [A]_{r+1} \neq 0.$$

Les tableaux dont la profondeur est au moins égale à r forment un groupe qui est isomorphe au produit direct de p^r groupes isomorphes à $\mathfrak{P}_{m-r}$. Ce groupe, qui est un sous-groupe distingué de $\mathfrak{P}_m$, sera désigné par $\mathfrak{D}_r$.

On peut toujours représenter une fonction $a(x_1, x_2, \ldots, x_s)$ par un polynome en $x_1, x_2, \ldots, x_s$, à coefficients dans G_p et dans lesquels les exposants de chaque x_i ne sont pas supérieurs à $p-1$. Il suffit d'appliquer la formule d'interpolation de Lagrange

$$(1.3)\quad a(x_1, x_2, \ldots, x_s) = \sum_{d_i \in G_p} a(d_1, d_2, \ldots, d_s)\,\frac{x_1 - x_1^p}{x_1 - d_1}\,\frac{x_2 - x_2^p}{x_2 - d_2}\cdots\frac{x_s - x_s^p}{x_s - d_s}$$

$$= \sum_{0 \leq i_\sigma \leq p-1} c_{i_1 i_2 \ldots i_s} x_1^{i_1} x_2^{i_2} \ldots x_s^{i_s}.$$

Dans l'anneau des polynomes en $x_1, x_2, \ldots, x_s$, qu'on note $G_p(x_1, \ldots, x_s)$, deux polynomes représentent la même fonction, lorsqu'ils sont congrus relativement à l'idéal

$$I_s = (x_1^p - x_1,\ x_2^p - x_2,\ \ldots,\ x_s^p - x_s).$$

Donc la fonction représentée par un polynome ne change pas quand on remplace chaque exposant d'une variable par son plus petit reste positif non nul (mod $p-1$). Un polynome où les exposants des variables sont tous ainsi rendus aux plus égaux à $p-1$ sera appelé *réduit* et nous conviendrons, dans la suite, de représenter les coordonnées d'un tableau par des polynomes réduits.

La multiplication se fera suivant la règle indiquée, en mettant les résultats des calculs sous forme réduite.

Il peut être commode d'employer un autre mode d'écriture des lois de composition (1.1) et (1.2), en particulier dans des raisonnements et des démonstrations par récurrence sur m. Considérons un vecteur X_{m-1} de l'espace E_{m-1} et un tableau A_{m-1}, de rang $m-1$, de coordonnées $a(x_1, x_2, \ldots, x_s)$. Nous noterons $X_{m-1}^{A_{m-1}}$ la transformation de l'espace E_{m-1}, associée à A_{m-1}, et définie par les relations

$$x_i^{A_{m-1}} = x_i - a(x_1, x_2, \ldots, x_{i-1}) \qquad (i \text{ de } 1 \text{ à } m-1). \tag{1.4}$$

Un tableau de rang m étant alors représenté par $[A_{m-1}, a(X_{m-1})]$, les lois de composition sont exprimées par

$$[A_{m-1}, a(X_{m-1})]\,[B_{m-1}, b(X_{m-1})] = [A_{m-1}B_{m-1}, a(X_{m-1}) + b(X_{m-1}^{A_{m-1}})], \tag{1.1}$$

$$[A_{m-1}, a(X_{m-1})]^{-1} = [A_{m-1}^{-1}, -a(X_{m-1}^{A_{m-1}^{-1}})]. \tag{1.2}$$

CHAPITRE II.

PROPRIÉTÉS DES POLYNOMES A COEFFICIENTS DANS G_p.

Dans ce Chapitre, je vais exposer quelques propriétés des fonctions, définies sur l'espace E_s, à valeurs dans G_p et représentées, comme il a été dit, par des polynomes réduits, relativement aux transformations $X_s^{A_s}$ de l'espace E_s, définies par les formules (1.4). Ces propriétés, résumées en quelques lemmes, constituent l'outil principal pour l'étude des groupes $\mathfrak{P}_m$.

Dans un polynôme réduit, nous rangerons les monômes (dissemblables), lexicographiquement, ou par *hauteur* : $x_1^{i_1}x_2^{i_2}\ldots x_s^{i_s}$ de hauteur supérieure à $x_1^{i'_1}x_2^{i'_2}\ldots x_s^{i'_s}$ si, dans la suite des différences $i_s - i'_s$, $i_{s-1} - i'_{s-1}$, $\ldots$, $i_1 - i'_1$, la première qui n'est pas nulle est positive. D'une façon plus précise, nous appellerons *hauteur du monome réduit*

$$x_1^{i_1}x_2^{i_2}\ldots x_{s-1}^{i_{s-1}}x_s^{i_s},$$

les i au plus égaux à $p-1$, l'entier

$$h = i_s p^{s-1} + i_{s-1}p^{s-2} + \ldots + i_2 p + i_1 + 1 \leq p^s.$$

La comparaison précédente est équivalente à celle des entiers h, et deux monomes de même hauteur sont nécessairement semblables (ne différant que par leurs coefficients).

Dans un polynome

$$f(x_1, x_2, \ldots, x_s) \quad \text{ou} \quad f(X_s) \quad \text{ou} \quad f(X),$$

réduit, sans termes semblables, et ordonné par hauteur de ses monomes, le terme de plus grand hauteur h, dont le coefficient a_h n'est pas nul, sera appelé le *terme principal* et a_h sera le *coefficient principal* du polynome. La hauteur du terme principal sera appelée la *hauteur du polynome* et désignée par $h[f(X)]$.

LEMME 1. — *Le terme principal* (et, par suite, le coefficient principal et la hauteur) *d'un polynome reste invariant dans toute transformation* $X_s^{A_s}$, *du groupe* $\mathfrak{P}_s$.

Notamment

$$h[f(X^A)] = h[f(X)].$$

COROLLAIRE. — *La hauteur de* $f(X) - f(X^A)$ *est inférieure à celle de* $f(X)$

$$h[f(X) - f(X^A)] < h[f(X)]. \tag{2.1}$$

Démonstration. — Nous poserons, pour abréger et provisoirement,

$$\bar{h}[f(X)] = h[f(X)] - 1;$$

il en résulte les relations

$$\bar{h}[f(X) + f'(X)] \leq \max(\bar{h}[f(X)], \bar{h}[f'(X)]); \tag{1}$$

$$\bar{h}[f(X) \times f'(X)] \leq \bar{h}[f(X)] + \bar{h}[f'(X)]. \tag{2}$$

La première relation, qui est également vraie pour la hauteur $h[f(X)]$, est évidente; elle permet de ne vérifier la seconde que pour des monomes (de coefficients 1)

$$M = x_1^{i_1} x_2^{i_2} \dots x_s^{i_s}, \qquad M' = x_1^{i'_1} x_2^{i'_2} \dots x_s^{i'_s};$$

leur produit est

$$M M' = x_1^{\overline{i_1+i'_1}} x_2^{\overline{i_2+i'_2}} \dots x_s^{\overline{i_s+i'_s}};$$

la surligne indique qu'on a remplacé l'entier surligné par son plus petit reste positif (mod $p-1$). Les nombres à comparer sont alors

$$\bar{h}[M] + \bar{h}[M'] = (i_1+i'_1) + (i_2+i'_2)p + \dots + (i_s+i''_s)p^{s-1};$$

$$\bar{h}[M M'] = (\overline{i_1+i'_1}) + (\overline{i_2+i'_2})p + \dots + (\overline{i_s+i'_s})p^{s-1};$$

l'inégalité est manifeste. En outre, dans la relation (2), il n'y a égalité que si et seulement si, dans les produits des termes principaux, les sommes des exposants de chaque variable x_i ne dépassent pas $p-1$, et, par suite, ne donnent pas lieu à réduction. On dira, dans ce cas, que $f(X)$ et $f'(X)$ *se multiplient sans réduction*. D'après la propriété (1), il est manifeste que si deux polynomes se multiplient sans réduction, le terme principal du produit est égal au produit des termes principaux des facteurs.

Le lemme peut alors se démontrer par récurrence sur la hauteur; il est évident pour une hauteur égale à 1, le polynome étant alors une constante, qui

n'est pas modifiée par la transformation. Supposons-le vrai pour tout polynome de hauteur inférieure à $h^\star$, que je désignerai, d'une façon générale, par $o(X)$, en sorte que

$$h[o(X^A)] = h[o(X)] < h^\star.$$

Un polynome de hauteur $h^\star$ est alors une somme

$$f(X) = c\,M + o(X), \qquad M = x_1^{i_1} x_2^{i_2} \dots x_s^{i_s};$$
$$c \not\equiv 0, \qquad h[M] = h^\star.$$

Dans la transformation, les termes restent de hauteur inférieure à $h^\star$, sauf le premier qui devient

$$(c\,M)^A = c\,(x_1 - a)^{i_1}\big(x_2 - a(x_1)\big)^{i_2} \dots \big(x_s - a(x_1, x_2, \dots, x_{s-1})\big)^{i_s};$$

c'est un produit de facteurs, dont les termes principaux sont, respectivement :

$$c, \quad x_1^{i_1}, \quad x_2^{i_2}, \quad \dots, \quad x_s^{i_s};$$

la multiplication se fait sans réduction, le terme principal en est leur produit, qui est cM, de hauteur $h^\star$. Donc

$$(c\,M)^A = c\,M + o(X), \qquad f(X) = c\,M + o(X);$$

la propriété, vraie pour toute hauteur inférieure à $h^\star$, le reste pour $h^\star$.

LEMME 2. — *Pour tout polynome $f(X)$, de hauteur k, on peut trouver au moins une transformation* $A(\text{de } \mathfrak{P}_s)$, *telle que* $f(X) - f(X^A)$, qui est de hauteur inférieure à k, *soit effectivement de hauteur* $k - 1$.

Considérons d'abord un monome (de coefficient 1) et soit r le plus petit indice, tel que l'exposant i_r ne soit pas nul, de sorte que

$$M = x_r^{i_r} x_{r+1}^{i_{r+1}} \dots x_s^{i_s} \qquad i_r \not\equiv 0.$$

Formons alors le tableau A, (de profondeur $r - 1$), dont toutes les coordonnées sont nulles, sauf celle de rang r qui est égale à

$$[A]_r = x_1^{p-1} x_2^{p-1} \dots x_{r-1}^{p-1}.$$

La transformation qu'il définit vérifie la propriété pour le monome, car

$$M - M^A = x_r^{i_r} x_{r+1}^{i_{r+1}} \dots x_s^{i_s} - (x_r - x_1^{p-1} x_2^{p-1} \dots x_{r-1}^{p-1})^{i_r} x_{r+1}^{i_{r+1}} \dots x_s^{i_s}$$
$$= i_r x_1^{p-1} x_2^{p-1} \dots x_{r-1}^{p-1} x_r^{i_r - 1} x_{r+1}^{i_{r+1}} \dots x_s^{i_s} + \text{termes de haut. inf.};$$

et la hauteur de cette différence est

$$1 + (p-1) + (p-1)p + \dots + (p-1)p^{r-2} + (i_r - 1)p^{r-1} + i_{r+1}p^r + \dots + i_s p^{s-1}$$
$$= (1 + i_r p^{r-1} + \dots + i_s p^{s-1}) - 1 = h[M] - 1.$$

Considérons alors un polynome de hauteur k

$$f(X) = cM + o(X), \qquad h[M] = k, \qquad h[o(X)] \leq k-1.$$

D'après le corollaire,

$$h[o(X) - o(X^A)] < h[o(X)] \leq k-1 = h[M - M^A],$$

de sorte que

$$h[f(X) - f(X^A)] = h[cM - cM^A + o(X) - o(X^A)] = k-1.$$

Remarque. — L'ensemble des polynomes dont la hauteur est au plus égale à un entier t, positif, est évidemment un module, qui sera désigné par $\mathfrak{F}_t$. D'autre part, si un module de polynomes contient au moins un polynome de de hauteur égale à chacun des entiers au plus égaux à t, il est égal à $\mathfrak{F}_t$. Le lemme 2 entraîne alors la conséquence suivante :

COROLLAIRE. — *Si $f(X)$ est un polynome de hauteur t, les polynomes $f(X^A)$, où A est une transformation quelconque de $\mathfrak{P}_s$, engendrent le module $\mathfrak{F}_t$.*

LEMME 3. — *Tout polynome $f(X)$ et tout tableau* A, *de profondeur r, au plus égale à s vérifient l'inégalité*

$$h[f(X) - f(X^A)] \leq p^s - p^r. \tag{2.2}$$

Une application immédiate de l'inégalité (1), dans le cas des hauteurs, donne l'inégalité

$$h\big[\big(f(X)+f'(X)\big) - \big(f(X^A)+f'(X^A)\big)\big] = h\big[\big(f(X)-f(X^A)\big) + \big(f'(X)-f'(X^A)\big)\big],$$
$$\leq \operatorname{Max}\big(h[f(X)-f(X^A)],\ h[f'(X)-f'(X^A)]\big).$$

Elle montre qu'il suffit de démontrer le lemme pour un monome quelconque (de coefficient 1)

$$M = x_1^{i_1} \dots x_s^{i_s}.$$

Effectuons une transformation A, de profondeur r

$$M^A = x_1^{i_1} \dots x_r^{i_r}\big(x_{r+1} - a(x_1, \dots, x_r)\big)^{i_{r+1}} \dots \big(x_s - a(x_1, \dots, x_{s-1})\big)^{i_s},$$

formons la différence, c'est une somme de termes de la forme

$$M_J = C_{j_{r+1}}^{i_{r+1}} \dots C_{j_s}^{i_s} x_1^{i_1} \dots x_r^{i_r} x_{r+1}^{i_{r+1}-j_{r+1}} a(x_1, \dots, x_r)^{j_{r+1}} \dots x_s^{i_s-j_s} a(x_1, \dots, x_{s-1})^{j_s};$$

les premiers facteurs sont les coefficients du binome; les indices $j_{r+1}, \dots, j_s$, constituant l'indice complexe J, sont les divers systèmes de valeurs non toutes nulles, telles que $j_{r+u} \leq i_{r+u}$. Dans un terme M_J, appelons v le plus grand indice tel que j_v ne soit pas nul; le seul facteur qui contient x_v est $x_v^{i_v - j_v}$, dont

l'exposant est au plus égal à $p-2$. La hauteur de M_j ne peut donc pas dépasser celle du monome

$$x_1^{p-1}\dots x_\nu^{p-2}\dots x_s^{p-1},$$

c'est-à-dire que

$$h(M_j)\leq 1+(p-1)+(p-1)p+\dots+(p-1)p^{s-1}$$
$$+\left((p-2)p^{\nu-1}-(p-1)p^{\nu-1}\right)=p^s-p^{\nu-1}\leq p^s-p^r;$$

d'après la propriété (1), cette inégalité subsiste pour la somme des M_j.

L'inégalité ainsi démontrée ne peut pas être améliorée, c'est ce qu'exprime la propriété suivante :

LEMME 4. — *Pour tout tableau* A, *de profondeur* r (*au plus égale à* s), *on peut trouver au moins un polynome* $f(X)$, *tel que*

$$h[f(X)-f(X^A)]=p^s-p^r. \tag{2.3}$$

Étudions d'abord l'effet de la transformation

$$A=[0,\dots,0,a(x_1,\dots,x_r),\dots,a(x_1,\dots,x_{s-1})],\qquad a(x_1,\dots,x_r)\not\equiv 0$$

sur le monome $M_1=x_{r+1}^{p-1}\dots x_s^{p-1}$. Il est manifeste que la différence

$$M_1-M_1^A=x_{r+1}^{p-1}\dots x_s^{p-1}-\left(x_{r+1}-a(x_1,\dots,x_r)\right)^{p-1}\dots\left(x_s-a(x_1,\dots,x_{s-1})\right)^{p-1}$$

contient des termes non nuls de la forme

$$m(x_1,\dots,x_r)x_{r+1}^{p-2}x_{r+2}^{p-1}\dots x_s^{p-1},$$

où les $m(x_1,\dots,x_r)$ sont certains monomes; choisissons celui de hauteur maximum; si ses exposants sont $j_1,\dots,j_r$, le monome

$$M=x_1^{p-1-j_1}\dots x_r^{p-1-j_r}.M_1$$

vérifie la propriété énoncée.

Cherchons maintenant à résoudre l'*équation fonctionnelle*

$$f(X)-f(X^A)=g(X); \tag{2.4}$$

où $f(X)$ est un polynome inconnu, les données étant la transformation A et le polynome second membre $g(X)$. Le nombre de solutions, s'il en existe, est évidemment égal à celui des solutions de l'équation sans second membre

$$f(X)-f(X^A)=0 \qquad \text{ou} \qquad f(X)=f(X^A), \tag{2.5}$$

dont une condition de possibilité est manifestement fournie par la considération des domaines de transitivité de A.

LEMME 5. — *Pour qu'un polynome* $h(X)$ *soit solution de l'équation* (2.5), sans second membre, *il faut et il suffit que* $h(X)$ *soit constant, pour tous les points* X, *d'un domaine de transitivité de* A.

Le nombre de solutions est, par suite, $p^{t(A)}$; $t(A)$ nombre des domaines de transitivité. Dans le cas particulier d'une transformation A, d'ordre p^s, son domaine de transitivité est l'espace E_s lui-même et les solutions de (2.5) sont les fonctions $h(X) = \text{const.}$

Pour étudier l'équation (2.4), avec second membre, définissons d'abord une opération de sommation dans un sous-ensemble R de E_s

$$\mathbf{S}_R[f(X)] = \sum f(X_i), \qquad \text{tous} \quad X_i \in R. \tag{2.6}$$

Il en résulte, pour une sommation étendue à un domaine T(A) de transitivité de A,

$$\mathbf{S}_{T(A)}[f(X^A)] = \mathbf{S}_{T(A)}[f(X)]. \tag{2.7}$$

On peut alors énoncer une condition de possibilité de l'équation (2.4) (avec second membre) :

LEMME 6. — *Pour que l'équation* (2.4) *ait des solutions, il faut et il suffit que*

$$\mathbf{S}_{T(A)}[g(X)] = 0$$

pour tout domaine T(A), *de transitivité de* A.

La condition est *nécessaire*, car, si $f_1(X)$ est une solution de (2.4), pour tout domaine T(A), on a

$$\mathbf{S}_{T(A)}[g(X)] = \mathbf{S}_{T(A)}[f_1(X) - f_1(X^A)] = \mathbf{S}_{T(A)}[f_1(X)] - \mathbf{S}_{T(A)}[f_1(X^A)] = 0.$$

La condition est *suffisante*. Choisissons dans chaque domaine $T_i(A)$ de transitivité de A, un représentant X_i; tout point de E_s est de la forme $X_i^{A^u}$. Nous déterminerons une solution $f_1(X)$ par les conditions

$$f_1(X_i) = 0, \qquad f_1(X_i^{A^u}) = -g(X_i) - g(X_i^A) \ldots - g(X_i^{A^{u-1}});$$

ces conditions sont compatibles, car si k est l'ordre de A,

$$f_1(X_i) = f_1(X_i^{A^k}) = \mathbf{S}_{T(A)}[-g(X)] = 0;$$

en outre, pour chaque u et pour chaque i,

$$f_1(X_i^{A^u}) - f_1\left((X_i^{A^u})^A\right) = g(X^{A^u}).$$

CHAPITRE III.

PROPRIÉTÉS ÉLÉMENTAIRES DES TABLEAUX.

Dans un tableau A, de rang m on représentera la hauteur de la coordonnée de rang u, de A, par la notation abrégée

$$|\,A\,|_u = h\big[[\,A\,]_u\big] = h[a(x_1, \ldots, x_{u-1})], \qquad 0 \leqq |\,A\,|_u \leqq p^{u-1}.$$

Le système de ces hauteurs (u de 1 à m)

$$<|\,A\,|_1, |\,A\,|_2, \ldots, |\,A\,|_m>,$$

sera appelé l'*indicatrice* du tableau A et désigné par $|\,A\,|$. La condition pour qu'un tableau soit de profondeur r est que le premier terme non nul de son indicatrice soit $|\,A\,|_{r+1}$, de rang $r+1$.

On définira une *comparaison* (partielle) des indicatrices des tableaux, éléments de $\mathfrak{P}_m$, par la condition

$$|\,A\,| \leqq |\,B\,| \quad \text{équivalent à} \quad |\,A\,|_u \leqq |\,B\,|_u, \qquad (u \text{ de } 1 \text{ à } m).$$

Ces notations précisées, nous allons indiquer quelques propriétés :

du *commutateur :* $(A, B) = ABA^{-1}B^{-1}$, de deux tableaux A et B;
du *transmué :* $A^B = BAB^{-1}$, du tableau A par B.

Propriétés du commutateur. — En utilisant la notation récurrente de la fin du Chapitre I et les formules de multiplication et d'inversion qui en résultent, on obtient

$$(3.1)\quad (A_{u+1}, B_{u+1}) = \big[A_u B_u A_u^{-1} B_u^{-1},\ a(X_u) - a\big(X_u^{A_u B_u A_u^{-1}}\big) + b\big(X_u^{A_u}\big) - b\big(X_u^{A_u B_u A_u^{-1} B_u^{-1}}\big)\big].$$

La valeur de la coordonnée de rang $u+1$ est, par suite,

$$(3.2)\qquad [(A, B)]_{u+1} = a(X_u) - a\big(X_u^{A_u B_u A_u^{-1}}\big) + b\big(X_u^{A_u}\big) - b\big(X_u^{A_u B_u A_u^{-1} B_u^{-1}}\big).$$

La coordonnée de rang 1 est manifestement nulle. L'application du lemme 1 aux deux derniers termes, considérés comme des transformés par la transformation A_u, donne l'égalité

$$h\big[b\big(X_u^{A_u}\big) - b\big(X_u^{A_u B_u A_u^{-1} B_u^{-1}}\big)\big] = h\big[b(X_u) - b\big(X_u^{B_u A_u^{-1} B_u^{-1}}\big)\big];$$

il en résulte l'inégalité fondamentale

$$(3.3)\quad |(A, B)|_{u+1} \leqq \max.\Big(h\big[a(X_u) - a\big(X_u^{A_u B_u A_u^{-1}}\big)\big],\ h\big[b(X_u) - b\big(X_u^{B_u A_u^{-1} B_u^{-1}}\big)\big]\Big);$$

il y a notamment égalité quand les deux hauteurs du second membre sont différentes.

Par application du corollaire 1, on obtient l'inégalité (ou l'indice $u+1$ est remplacé par u)

$$(3.4) \qquad |(A, B)|_u < \text{Max.}\big(h[a(X_{u-1})], h[b(X_{u-1})]\big) = \max.(|A|_u, |B|_u).$$

Il y a naturellement exception si les hauteurs du second membre sont nulles; alors

$$|A|_u = |B|_u = |(A, B)|_u.$$

On peut préciser l'inégalité (3.3), quand on fait sur A et B des hypothèses complémentaires.

1° A *et* B *de profondeur* r; en prenant $u \geqq r$, l'application du lemme 3 aux termes du second membre de (3.3) donne

$$h[a(X_u) - a(X_u^{A_u B_u A_u^{-1}})] \leqq p^u - p^r, \qquad h[b(X_u) - b(X_u^{B_u A_u^{-1} B_u^{-1}})] \leqq p^u - p^r$$

et

$$(3.5) \qquad |(A, B)|_{u+1} \leqq p^u - p^r, \qquad r \leqq u \leqq m-1.$$

En particulier $|(A, B)|_{r+1}$ est nul : le commutateur de deux tableaux de profondeur r est un tableau de profondeur au moins égale à $r+1$.

2° A *de profondeur* r *et* B *quelconque;* le même calcul donne l'inégalité

$$(3.6) \qquad |(A, B)|_{u+1} \leqq \max.(|A|_{u+1} - 1, p^u - p^r).$$

Propriétés du transmué. — Avec des calculs analogues, on obtient les résultats

$$(3.7) \qquad [{}_1^1BAB^{-1}]_{u+1} = a(X_u^{B_u}) + b(X_u) - b(X_u^{B_u A_u B_u^{-1}}).$$

La hauteur du premier terme du second membre est égale à (lemme 1)

$$h[a(X_u^{B_u})] = h[a(X_u)] = |A|_u;$$

et il en résulte l'inégalité [analogue à (3.3)]

$$(3.8) \qquad |BAB^{-1}|_u \leqq \max.\big(|A|_u, h[b(X_u) - b(X_u^{B_u A_u B_u^{-1}})]\big);$$

il y a notamment égalité quand les deux hauteurs du second membre sont différentes.

Considérons encore le cas particulier : A *de profondeur* r, B *quelconque:* l'inégalité devient [analogue à (3.6)]

$$(3.9) \qquad |BAB^{-1}|_{u+1} \leqq \max.(|A|_{u+1}, p^u - p^r).$$

Dans ce cas, on peut préciser l'expression (3.7), suivant le terme du second membre qui donne la valeur du maximum.

Premier cas. — Supposons

$$|\mathrm{A}|_{u+1} > p^u - p^r, \qquad \text{donc} \quad |\mathrm{BAB}^{-1}|_{u+1} = |\mathrm{A}|_{u+1}; \tag{3.10}$$

on peut alors calculer le *terme principal* du transmué; il est égal à celui du premier terme du second membre de (3.7), puisque

$$h[b(\mathrm{X}_u) - b(\mathrm{X}_u^{\mathrm{B}_u\mathrm{A}_u\mathrm{B}_u^{-1}})] \leqq p^u - p^r < |\mathrm{A}|_{u+1}.$$

Mais, d'après le lemme 1, le terme principal de $a(\mathrm{X}_u^{\mathrm{B}_u})$ est égal à celui de $a(\mathrm{X}_u)$, donc de $[\mathrm{A}]_{u+1}$; d'où, en remplaçant $u+1$ par u,

$$\text{terme pr. } [\mathrm{BAB}^{-1}]_u = \text{terme pr. } [\mathrm{A}]_u. \tag{3.11}$$

Deuxième cas. — Supposons

$$|\mathrm{A}|_{u+1} \leqq p^u - p^r.$$

D'après le lemme 4, il existe effectivement un polynome $b(\mathrm{X}_u)$ tel que

$$h[b(\mathrm{X}_u) - b(\mathrm{X}_u^{\mathrm{A}_u})] = p^u - p^r.$$

Construisons le tableau B_1, dont toutes les coordonnées sont nulles, sauf $[\mathrm{B}_1]_{u+1} = b(\mathrm{X}_u)$; l'égalité (3.7) devient

$$[\mathrm{B}_1\mathrm{AB}_1^{-1}]_{u+1} = a(\mathrm{X}_u) + b(\mathrm{X}_u) - b(\mathrm{X}_u^{\mathrm{A}_u}).$$

Le terme principal est, par hypothèse, de hauteur $p^u - p^r$, il ne peut être égal au terme de même hauteur dans $a(\mathrm{X}_u)$, terme qui est nul si $|\mathrm{A}|_{u+1} < p^u - p^r$, et qui, en tous cas, est modifié par le terme de cette hauteur dans $\left(b(\mathrm{X}_u) - b(\mathrm{X}_u^{\mathrm{A}_u})\right)$, qui lui, n'est pas nul. Dans ce deuxième cas, il existe donc une transformation B_1, telle que ($u+1$ étant remplacé par u)

$$\text{terme pr. } [\mathrm{B}_1\mathrm{AB}_1^{-1}]_u \neq \text{terme pr. } [\mathrm{A}]_u.$$

Il en résulte l'énoncé suivant :

LEMME 7. — *La condition nécessaire et suffisante pour que le terme principal de la coordonnée de rang u,* $[\mathrm{A}]_u$, *d'un tableau* A, *de rang m et de profondeur r,* ($r+1 \leqq u \leqq m$) *soit invariant pour tous les automorphismes intérieurs* (transmutations) *du groupe* $\mathfrak{P}_m$ *est que la hauteur* $|\mathrm{A}|_u$ *soit supérieure à* $p^{u-1} - p^r$.

Il est évident que la transmutation par un tableau dont toutes les coordonnées sont nulles, sauf celle de rang u, ne peut changer que les hauteurs des coordonnées de ce rang u. Cette remarque permet de démontrer le lemme suivant.

LEMME 8. — *Pour un tableau* A, *de profondeur r, il existe au moins un tableau* B, *tel que*

$$|\mathrm{BAB}^{-1}|_u \geqq p^{u-1} - p^r, \qquad \text{tout} \quad u \geqq r+1.$$

Pour chaque u, tel que $|A|_u < p^{u-1} - p^r$, choisissons, comme il a été fait dans la démonstration du lemme précédent, un tableau B_u, dont toutes les coordonnées sont nulles, sauf celle de rang u, déterminée par

$$[B_u]_u = b_u(X_{u-1}); \qquad h[b_u(X_{u-1}) - b_u(X_{u-1}^{A_{u-1}})] = p^{u-1} - p^r.$$

Il suffit alors de prendre pour tableau B, le produit des B_u, l'ordre des facteurs n'important pas.

CHAPITRE IV.

SUITES CENTRALES ASCENDANTES ET DESCENDANTES.

Notions générales. — Dans un groupe $\mathfrak{G}$ quelconque, la *suite centrale ascendante* (S. C. A.) est la suite de sous-groupes, nécessairement caractéristiques, $\mathfrak{Z}_u$, chacun contenu dans le suivant, définis par la récurrence suivante :

$$\mathfrak{Z}_0 = 1 \quad (\text{unité de } \mathfrak{G}); \qquad \mathfrak{Z}_{u+1} \,|\, \mathfrak{Z}_u = \text{centre de } \mathfrak{G} \,|\, \mathfrak{Z}_u;$$

il est équivalent de définir $\mathfrak{Z}_{u+1}$ comme l'ensemble de tous les éléments B (de $\mathfrak{G}$), tels que les commutateurs de B avec tous les éléments A, de $\mathfrak{G}$ soient dans $\mathfrak{Z}_u$.

Théorème 2. — *Dans un p-groupe $\mathfrak{G}$, le dernier terme de la S. C. A. est le groupe $\mathfrak{G}$ lui-même.*

En effet, pour que $\mathfrak{Z}_{c+1} = \mathfrak{Z}_c$, il faut et il suffit que le centre de $\mathfrak{G} \,|\, \mathfrak{Z}_c$ se se réduise à l'unité. Si $\mathfrak{G}$ est un p-groupe, il en est de même de $\mathfrak{G} \,|\, \mathfrak{Z}_c$, qui doit comme son centre se réduire à l'unité. Car dans un p-groupe, d'ordre supérieur à 1, le centre est aussi d'ordre supérieur à 1.

La *suite centrale descendante* (S. C. D.) est encore une suite de sous-groupes, nécessairement caractéristiques (1), chacun contenant le suivant, définis par la récurrence suivante :

$$\tilde{\mathfrak{Z}}_0 = \mathfrak{G}; \qquad \tilde{\mathfrak{Z}}_{u+1} = (\mathfrak{G}, \tilde{\mathfrak{Z}}_u)$$

(suivant la notation précisée, il faut entendre que $\tilde{\mathfrak{Z}}_{u+1}$ est constitué par tous les commutateurs d'un élément de $\mathfrak{G}$ avec un élément de $\tilde{\mathfrak{Z}}_u$).

Lemme 9. — *Dans un p-groupe le terme de rang u de la S. C. D. est contenu dans le terme de rang $c - u$ de la S. C. A.*

$$\tilde{\mathfrak{Z}}_u \subseteq \mathfrak{Z}_{c-u};$$

c rang du dernier terme de S. C. A.

---

(1) On a seulement rappelé ici les propriétés élémentaires des S. C. A. et des S. C. D., dont certaines (comme le théorème 2), sont bien connues. On en trouvera un exposé détaillé dans le mémoire de Ph. Hall (4 de l'Index bib.).

Le lemme se démontre par récurrence sur le rang u; il est vrai pour $u = 0$, puisque $\tilde{\mathfrak{Z}}_0 = \mathfrak{G} = \mathfrak{Z}_c$. Supposons-le vrai pour u, de sorte que

$$\tilde{\mathfrak{Z}}_u \subseteqq \mathfrak{Z}_{c-u}; \qquad \mathfrak{Z}_{c-u-1} \subseteqq \mathfrak{Z}_{c-u}.$$

Construisons le sous-groupe caractéristique $\tilde{\mathfrak{Z}}'_u$ avec les éléments de $\tilde{\mathfrak{Z}}_u$ et de $\mathfrak{Z}_{c-u-1}$; il vérifie les inclusions

$$\mathfrak{Z}_{c-u-1} \subseteqq \tilde{\mathfrak{Z}}'_u; \qquad \tilde{\mathfrak{Z}}'_u \subseteqq \mathfrak{Z}_{c-u};$$

il en résulte l'inclusion des groupes quotients

$$\tilde{\mathfrak{Z}}'_u \,|\, \mathfrak{Z}_{c-u-1} \subseteqq \mathfrak{Z}_{c-u} \,|\, \mathfrak{Z}_{c-u-1}.$$

Le premier est contenu dans le centre du groupe $\mathfrak{G} \,|\, \mathfrak{Z}_{c-u-1}$, de sorte que le commutateur

$$(\mathfrak{G} \,|\, \mathfrak{Z}_{c-u-1},\ \tilde{\mathfrak{Z}}'_u \,|\, \mathfrak{Z}_{c-u-1})$$

se réduit à l'unité. Par conséquent,

$$\mathfrak{Z}_{c-u-1} \supseteqq (\mathfrak{G}, \tilde{\mathfrak{Z}}'_u) \supseteqq (\mathfrak{G}, \tilde{\mathfrak{Z}}_u) = \tilde{\mathfrak{Z}}_{u+1}.$$

On en conclût notamment que

$$\tilde{\mathfrak{Z}}_c \subseteqq \mathfrak{Z}_{c-c} \subseteqq \mathfrak{Z}_0 = \text{unité de } \mathfrak{G}_n;$$

par suite, le dernier élément $\tilde{\mathfrak{Z}}_{c'}$, de la S. C. D. est égal à l'unité de $\mathfrak{G}$ et le rang c' est au plus égal au rang c du dernier terme de la S. C. A.

LEMME 10. — *Dans un p-groupe le terme de rang u de la S. C. A. est contenu dans le terme de rang $c' - u$ de la S. C. D.*

$$\mathfrak{Z}_u \supseteqq \tilde{\mathfrak{Z}}_{c'-u}.$$

Le lemme se démontre encore par récurrence sur le rang u; il est vrai pour $u = 0$, puisque $\mathfrak{Z}_0 = \text{unité de } \mathfrak{G} = \tilde{\mathfrak{Z}}_{c'}$. Supposons-le vrai pour u, de sorte que

$$\mathfrak{Z}_u \supseteqq \tilde{\mathfrak{Z}}_{c'-u} = (\mathfrak{G}, \tilde{\mathfrak{Z}}'_{c'-u-1}).$$

Construisons le sous-groupe caractéristique $\tilde{\mathfrak{Z}}''_{c'-u-1}$ avec les éléments de $\tilde{\mathfrak{Z}}_{c-u-1}$ et de $\mathfrak{Z}_u$. Il vérifie l'inclusion

$$(\mathfrak{G}, \tilde{\mathfrak{Z}}''_{c'-u-1}) \subseteqq \mathfrak{Z}_u,$$

de sorte que le commutateur des groupes quotients

$$(\mathfrak{G} \,|\, \mathfrak{Z}_u,\ \tilde{\mathfrak{Z}}''_{c'-u-1} \,|\, \mathfrak{Z}_u)$$

se réduit à l'unité. Donc le deuxième groupe est dans le centre du premier et il en résulte

$$\mathfrak{Z}_{u+1} \supseteqq \tilde{\mathfrak{Z}}''_{c'-u-1} \supseteqq \tilde{\mathfrak{Z}}_{c'-u-1}.$$

On en conclut notamment

$$\mathfrak{Z}_{c'} \supseteq \mathfrak{Z}_{c'+c'} = \mathfrak{Z}_0 = \mathfrak{G};$$

le rang c du dernier terme de la S. C. A. est au plus égal à c', donc (tenant compte du résultat précédent), lui est égal.

Les résultats de ces deux lemmes entraînent la propriété :

THÉORÈME 3. — *Dans un p-groupe $\mathfrak{G}$, le dernier terme de la S. C. D. est le groupe identique. Les deux suites ont le même nombre c de termes.*

Le nombre c est appelé la *classe* du p-groupe $\mathfrak{G}$.

On peut étendre la relation qui existe entre les termes successifs de la S. C. A. au cas d'un sous-groupe distingué quelconque. Dans un groupe $\mathfrak{G}$, nous appellerons *commutant d'un sous-groupe distingué*, quelconque $\mathfrak{H}$, le sous-groupe distingué $\mathfrak{H}^*$ tel que $\mathfrak{H}^* | \mathfrak{H}$ soit le centre de $\mathfrak{G} | \mathfrak{H}$.

Le commutant qu'on notera $)\mathfrak{G}, \mathfrak{H}($ est donc l'ensemble de tous les éléments B (de $\mathfrak{G}$), tels que les commutateurs de B avec tous les éléments A, de $\mathfrak{G}$ soient dans $\mathfrak{H}$. Dans la S. C. A., chaque terme est le commutant du précédent.

Etude du groupe $\mathfrak{P}_m$. Définition. — Nous appellerons *sous-groupe parallélotopique de $\mathfrak{P}_m$* (en abrégé G. P.) tout ensemble $\mathfrak{A}$ de ses éléments tel qu'il contienne tout tableau dont l'*indicatrice est au plus égale* à celle d'un de ses termes quelconque

$$A \in \mathfrak{A} \quad \text{et} \quad |X| \leq |A| \quad \text{entraînent} \quad X \in \mathfrak{A}.$$

L'ensemble $\mathfrak{A}$ est bien un groupe, car, en raison du lemme 1 (Chap. II) appliqué à la loi de composition (1.1) des tableaux, $\mathfrak{A}$ contient le produit de tout couple de ses éléments.

Pour chaque rang u (de 1 à m), déterminons le *maximum des hauteurs des coordonnées de rang u*, pour les tableaux de $\mathfrak{A}$, nous le noterons, par analogie avec les tableaux (Chap. III),

$$|\mathfrak{A}|_u = k_u = \text{Max.} |A|_u, \qquad A \in \mathfrak{A}, \qquad 0 \leq |\mathfrak{A}|_u \leq p^{u-1}.$$

Un groupe parallélotopique $\mathfrak{A}$ est manifestement déterminé par le système d'entiers

$$K = <k_1, k_2, \ldots, k_m>, \qquad k_u \leq p^{u-1};$$

qu'on appelle son *indicatrice* et qui sera désigné par

$$|\mathfrak{A}| = <\ldots |\mathfrak{A}|_u \ldots>.$$

Toujours, par analogie avec les tableaux, le groupe est dit de *profondeur r*, (Chap. I), quand le premier terme non nul de son indicatrice est de rang $r+1$.

Les G. P. ne sont pas en général des sous-groupes distingués, les lemmes 7 et 8 permettent de caractériser ceux qui le sont.

THÉORÈME 4. — *Pour qu'un* G. P. $\mathfrak{R}$ (de $\mathfrak{P}_m$), de profondeur r, *soit un sous-groupe distingué, il faut et il suffit que*

$$|\mathfrak{R}|_u \geq p^{u-1} - p^r; \qquad \text{pour tout } u, \quad r+1 \leq u \leq m.$$

Nous désignerons les G. P. distingués par l'abréviation G. P. I.; nous allons étudier quelques-unes de leurs propriétés pour aboutir à la conclusion remarquable que ce sont tous les sous-groupes caractéristiques de $\mathfrak{P}_m$.

THÉORÈME 5. — *Pour un G. P. I.* $\mathfrak{R}$, *de profondeur s et d'indicatrice*

$$< 0, \ldots, 0, k_{s+1}, \ldots, k_m >,$$

le commutateur $(\mathfrak{P}_m, \mathfrak{R})$ *est aussi un G. P. I. de profondeur s ou* $s+1$, *dont l'indicatrice*

$$< 0, \ldots, 0, k'_{s+1}, \ldots, k'_m >$$

est définie par

$$k'_u = \text{Max}(k_u - 1, p^{u-1} - p^s) \qquad \text{pour} \quad u : s+1 \leq u \leq m.$$

En particulier la profondeur est s ou $s+1$, suivant que k_{s+1} est supérieur à 1, ou égal à 1.

Appelons $\mathfrak{R}'$ le G. P. I. dont l'indicatrice est construite par les conditions du théorème. Formons les commutateurs

$$(B, A) \in (\mathfrak{P}_m, \mathfrak{R}), \qquad B \in \mathfrak{P}_m, \qquad A \in \mathfrak{R},$$

d'après la formule (3.6), A étant de profondeur au moins égale à s,

$$|(B, A)|_u \leq \text{Max}(|A|_u - 1, \quad p^{u-1} - p^s) \leq \text{Max}(k_u - 1, p^{u-1} - p^s) = k'_u.$$

D'après sa définition $\mathfrak{R}'$ contient donc ces commutateurs et par suite leur ensemble $(\mathfrak{P}_m, \mathfrak{R})$.

Réciproquement, montrons que $\mathfrak{R}'$ peut être engendré par des éléments de $(\mathfrak{P}_m, \mathfrak{R})$. Quels que soient u et h, vérifiant les conditions

$$s+1 \leq u \leq m, \qquad 0 \leq h \leq k_u;$$

$\mathfrak{R}$ contient un tableau $A(u, h)$ dont toutes les coordonnées sont nulles, sauf celle de rang u, égale à

$$[A(u, h)]_u = a(X_{u-1}), \qquad h[a(X_{u-1})] = h.$$

En outre, d'après le lemme 2, on peut trouver un tableau B_{u-1}, élément de $\mathfrak{P}_{u-1}$ tel que

$$h[a(X_{u-1}) - a(X_{u-1}^{B_{u-1}})] = h - 1.$$

Le commutateur des tableaux

$$A(u,h)=[o,\ldots,o\ a(X_{u-1}),o,\ldots,o],\qquad B=[B_{u-1},o,\ldots,o],\qquad A\in\mathfrak{U},\qquad B\in\mathfrak{P}_m$$

calculé par la formule (3.1) est

$$C(u,h)=[o,\ldots,o,\ a(X_{u-1})-a(X_{u-1}^{B_{u-1}}),\ o,\ \ldots,\ o],\qquad |C(u,h)|_u=h-1.$$

D'autre part $\mathfrak{R}$ contient un tableau

$$A'=[o,\ \ldots,\ o,f(X_s),\ o,\ \ldots,\ o]$$

dont toutes les coordonnées, sauf celle de rang $s+1$, sont nulles. D'après le lemme 4, on peut, pour tout u vérifiant la condition précédente, trouver un polynome $e(X_{u-1})$ tel que

$$h[e(X_{u-1})-e(X_{u-1}^{A'})]=p^{u-1}-p^s.$$

Le commutateur de A' et $B'=[o,e(X_{u-1}),o]$ appartenant à $\mathfrak{P}_m$ est

$$D(u)=[o,\ \ldots,\ o,\ e(X_{u-1})-e(X_{u-1}^{A'}),\ o,\ \ldots,\ o],\qquad |D(u)|_u=p^{u-1}-p^s.$$

Il est manifeste que les tableaux $C(u,h)$ et $D(u)$ engendrent le groupe $\mathfrak{R}'$ qui est ainsi contenu dans $(\mathfrak{P}_m,\mathfrak{R})$.

Corollaire. — *Le groupe quotient* $\mathfrak{R}\,|\,(\mathfrak{P}_m,\mathfrak{R})$ *est un groupe élémentaire dont le nombre* k *d'invariants est le nombre de coordonnées de rang* u, *de* $\mathfrak{R}$, *pour lesquelles* $|\mathfrak{R}|_u>p^{u-1}-p^s$, ($s$ *profondeur du G. P. I.* $\mathfrak{R}$), *son ordre est* p^k.

Le groupe $\mathfrak{P}_m$ étant lui-même un G. P. I., il résulte du théorème 5, que tout sous-groupe de la S. C. D. est aussi un G. P. I. Ce résultat peut être complété comme suit :

Théorème 6. — *Le terme* $\mathfrak{Z}_r$, *de rang* r, *de la S. C. D. est le G. P. I. dont l'indicatrice est*

$$|\mathfrak{Z}_r|=<k_1^{(r)},k_2^{(r)},\ \ldots,\ k_m^{(r)}>,\qquad k_u^{(r)}=\mathrm{Max}(o,p^{u-1}-r). \tag{4.1}$$

Sa profondeur est déterminée par les inégalités

$$p^s>r\geqq p^{s-1}\qquad\text{ou}\qquad s=E(\log r:\log p)+1. \tag{4.2}$$

Corollaire. — *Le groupe quotient* $\mathfrak{Z}_r\,|\,\mathfrak{Z}_{r+1}$ *est un groupe élémentaire, dont le nombre d'invariants est* m-(*profondeur de* $\mathfrak{Z}_r$).

Nous allons démontrer la propriété par récurrence. Elle est vraie pour le premier terme $\mathfrak{P}_m$, dont l'indicatrice est

$$<1,p,p^2,\ \ldots,p^{m-1}>;$$

sa profondeur étant $r=o$, on a bien

$$|\mathfrak{P}_m|_u=p^{u-1}=\mathrm{Max}(o,p^{u-1}-o).$$

Supposons la propriété vérifiée pour $\tilde{\mathfrak{Z}}_r$, dont la profondeur s est alors déterminée par l'inégalité du théorème. D'après le théorème 5, aux premiers termes nuls de $\tilde{\mathfrak{Z}}_r$ correspondent des termes nuls, de $\tilde{\mathfrak{Z}}_{r+1}$; A un terme de rang u, non nul de $\tilde{\mathfrak{Z}}_r$, correspond dans $\tilde{\mathfrak{Z}}_{r+1} = (\tilde{\mathfrak{Z}}_r, \mathfrak{P}_m)$,

$$|\tilde{\mathfrak{Z}}_{r+1}|_u = \mathrm{Max}(k_u - 1, p^{u-1} - p^s) = \mathrm{Max}(p^{u-1} - r - 1, p^{u-1} - p^s),$$

ce maximum est bien égal à $p^{u-1} - (r+1)$, car l'inégalité qui détermine s entraîne

$$p^s \geqq r+1 \qquad \text{et} \qquad p^{u-1} - (r+1) \geqq p^{u-1} - p^s.$$

On peut encore exprimer le théorème 6 en disant qu'on passe de l'indicatrice de $\tilde{\mathfrak{Z}}_r$ à celle de $\tilde{\mathfrak{Z}}_{r+1}$, *en conservant ses termes nuls et en diminuant les autres d'une unité.*

Le problème inverse ou dual du théorème 5, qui est la recherche du commutant, est résolu par la propriété suivante :

THÉORÈME 7. — *Pour un G. P. I. de profondeur s et d'indicatrice*

$$< 0, \ldots, 0, k_{s+1}, \ldots, k_m >,$$

le commutant $)\mathfrak{P}_m, \mathfrak{R}($ *est aussi un G. P. I., dont la profondeur* s' *et l'indicatrice*

$$< 0, \ldots, 0, k^*_{s'+1}, \ldots, k^*_m >,$$

sont définies par les conditions

$$p^{s'} \geqq p^{u-1} - k_u, \quad \text{tous } u; \qquad k^*_u = k_u + 1 \qquad \text{pour} \quad u \geqq s'+1.$$

En particulier ceci étant valable pour $u = s$

$$p^{s'} \geqq p^{s-1} - 0, \qquad s' \geqq s - 1,$$

dans le cas limite $s' = s-1$, le commutant est de profondeur $s-1$ et

$$p^{s-1} \geqq p^{u-1} - k_u, \quad \text{tous } u; \qquad k^*_{s'+1} = k^*_s = 1.$$

D'autre part, puisque $\mathfrak{R}$ est un G. P. I. de profondeur s, on a

$$k_u \geqq p^{u-1} - p^s, \qquad \text{donc} \qquad p^s \geqq p^{u-1} - k_u$$

et s vérifie l'inégalité du théorème, d'où $s' \leqq s$.

Appelons $\overline{\mathfrak{R}}^*$ le G. P. I. formé par les conditions du théorème et formons le commutateur $(\mathfrak{P}_m, \overline{\mathfrak{R}}^*)$ d'après la règle du théorème 5. Les s' premiers termes de l'indicatrice (en nombre au moins égal à $s-1$) sont nuls, les suivants sont

$$\mathrm{Max}(k^*_u - 1, p^{u-1} - p^{s'}) = \mathrm{Max}(k_u, p^{u-1} - p^{s'}) = k_u,$$

ceci en raison de la condition imposée à s' (et restant éventuellement valable pour $u = s$, k_u étant nul). Les termes sont donc nuls ou égaux à ceux de l'indicatrice de $\mathfrak{R}$, donc $(\mathfrak{P}_m, \overline{\mathfrak{R}}^*) \subset \mathfrak{R}$ et $\overline{\mathfrak{R}}^*$ est inclus dans le commutant cherché.

Reste à vérifier l'inclusion inverse, ce qu'on peut établir sous la forme : pour tout élément B non dans $\overline{\mathfrak{N}}^*$, il existe au moins un élément A, de $\mathfrak{P}_m$, tel que le commutateur (A, B) ne soit pas dans $\mathfrak{N}$. Si B n'appartient pas à $\overline{\mathfrak{N}}^*$, il y a au moins une de ses hauteurs $|B|_\nu$ qui est supérieure à la hauteur de même rang $|\overline{\mathfrak{N}}^*|_\nu$. Nous allons distinguer deux cas, suivant la comparaison de ν à s'.

PREMIER CAS :

$$\nu > s' \geqq s-1, \qquad |B|_\nu > |\overline{\mathfrak{N}}^*|_\nu = k_\nu^* = k_\nu + 1 \geqq 1,$$

ν est supérieur à 1, car, si $s'=0$; $|\mathfrak{N}^*|_1$ étant égal à 1, $|B|_1$ ne peut lui être supérieur. Il est alors commode de l'écrire. $\nu = u+1$ et les conditions peuvent être exprimées par

$$[B]_{u+1} = b(X_u), \qquad h[b(X_u)] > k_{u+1}+1.$$

Par application du lemme 2, construisons un tableau A comme suit :

$$h[b(X) - b(X_u^{A'_u})] = h[b(X_u)] - 1 > k_{u+1}, \qquad A = [B_u^{-1} A'_u B_u, 0],$$

les coordonnées de rang supérieur à u, notamment $a(X_u)$ étant nulles, il en résulte, par application de (3.2)

$$[(B, A)]_{u+1} = b(X_u) - b(X_u^{B_u A_u B_u^{-1}}) = b(X_u) - b(X_u^{A'_u}),$$

de sorte que

$$h[(B, A)_{u+1}] > k_{u+1} \qquad \text{et} \qquad (B, A) \notin \mathfrak{N}.$$

DEUXIÈME CAS :

$$\nu \leqq s', \qquad |B|_\nu > |\overline{\mathfrak{N}}^*|_\nu = 0.$$

La profondeur r de B, est inférieure à ν, donc à s', d'après la détermination de s', il existe nécessairement un rang $u+1$ tel que

$$p^r < p^u - k_{u+1} \qquad (r < u)$$

(en particulier si $r < s-1$, cette inégalité est vérifiée pour la valeur $u+1=s$). Le tableau B_u est aussi de rang r, donc par application du lemme 4, on peut trouver un polynome $a(X_u)$ tel que

$$h[a(X_u) - a(X_u^{B_u})] = p^u - p^r > k_{u+1}.$$

Formons le tableau A, de coordonnées toutes nulles, sauf

$$[A]_{u+1} = a(X_u),$$

et formons le commutateur (B, A). D'après (3.2)

$$[(B, A)]_{u+1} = a(X_u) - a(X_u^{A_u B_u A_u^{-}}) + b(X_u^{A_u}) - b(X_u^{A_u B_u A_u^{-1} B_u^{-1}}).$$

Mais A_u, de coordonnées nulles est une transformation identique dans E_u, de sorte que pour X_u

$$A_u B_u A_u^{-1} = B_u, \qquad A_u B_u A_u^{-1} B_u^{-1} = 1;$$

la différence des deux derniers termes est donc nulle et il reste

$$|(\mathrm{B},\mathrm{A})|_{u+1} = h[a(\mathrm{X}_u) - a(\mathrm{X}_u^{\mathrm{B}_u})] = p^u - p^r > k_{u+1}, \qquad (\mathrm{B},\mathrm{A}) \notin \mathfrak{U}.$$

Appliquons ce théorème à la S. C. D., qui a déjà été déterminée par le théorème 6, il montre que *le commutant d'un terme de la S. C. D. est son précédent*

(4.3) $$)\mathfrak{P}_m, \tilde{\mathfrak{Z}}_r(= \tilde{\mathfrak{Z}}_{r-1}.$$

Les termes de l'indicatrice de $\tilde{\mathfrak{Z}}_r$ et sa profondeur s sont données par

$$k_u = \max(0, p^{u-1} - r), \qquad p^s > r \geqq p^{s-1}.$$

La profondeur s' du commutant est déterminée par

$$p^{s'} \geqq p^{u-1} - k_u = p^{u-1} - \max(0, p^{u-1} - r) = \min(p^{u-1}, r),$$

ce qui est équivalent à

$$p^{s'} \geqq r \geqq p^{s-1}.$$

La profondeur s' est égale en général à la profondeur s, elle n'est plus égale qu'à $s-1$ dans le cas de $r = p^{s-1}$.

Les éléments de l'indicatrice sont

$$k'_u = \max\big(0, p^{u-1} - (r-1)\big).$$

On obtient ainsi une formation de la S. C. D.; dans le sens ascendant, elle coïncide avec celle de la S. C. A., en outre le dernier terme de la première est l'unité qui est le premier terme de la deuxième. D'où la propriété :

THÉORÈME 8. — *Dans le groupe $\mathfrak{P}_m$ les suites centrales ascendantes et descendantes coïncident.*

(4.4) $$3r = \tilde{\mathfrak{Z}} p^{m-1} - r.$$

L'indicatrice est

$$\langle h_1^{(r)}, \quad h_2^{(r)}, \quad \ldots, \quad h_m^{(r)} \rangle \qquad h_u^{(r)} = \max(0, p^{u-1} - p^{m-1} + r).$$

CHAPITRE V.

SOUS-GROUPES CARACTÉRISTIQUES DE $\mathfrak{P}_m$.

Dans ce Chapitre nous allons établir la propriété, déjà annoncée au Chapitre IV, de l'identité des G. P. I. et des sous-groupes caractéristiques de $\mathfrak{P}_m$. Nous supposerons toutefois essentiellement que *le nombre premier p est impair*, la propriété n'étant plus vraie pour $p = 2$.

THÉORÈME 9. — *Un sous-groupe caractéristique de $\mathfrak{P}_m$ est un G. P. I. Nous démontrerons la propriété plus générale : tout sous-groupe de $\mathfrak{P}_m$, invariant pour un certain groupe $\mathfrak{V}_m$, d'automorphismes de $\mathfrak{P}_m$, est un G. P. I.*

Construction du groupe $\mathfrak{V}_m$. — Considérons un système

$$W = (w_1, w_2, \ldots, w_m)$$

de m éléments, *non nuls*, de G_p (classes, mod$p$, premières avec p) et la transformation W(A), qui, à un tableau A, de coordonnées $a(x_1, x_2, \ldots, x_{s-1})$, fait correspondre le tableau de coordonnées

$$w_s a(w_1^{-1}x_1, w_2^{-1}x_2, \ldots, w_{s-1}^{-1}x_{s-1}),$$

c'est un *automorphisme* du groupe $\mathfrak{P}_m$.

D'une part, cette transformation conserve la multiplication : par application de la formule (1.1), la coordonnée, de rang s, de W(A) × W(B) est

$$(5.1)\quad w_s a(\ldots, w_i^{-1}x_i, \ldots) + w_s b\Big(\ldots, w_i^{-1}\big(x_i - w_i a(\ldots, w_j^{-1}x_j, \ldots)\big), \ldots\Big)$$
$$= w_s\Big(a(\ldots, w_i^{-1}x_i, \ldots) + b\Big(\ldots, \big(w_i^{-1}x_i - a(\ldots, w_j^{-1}x_j, \ldots)\big), \ldots\Big)\Big),$$

ce qui est bien la coordonnée, de rang s de W(AB).

D'autre part, la transformation est biunivoque, puisqu'elle a manifestement une inverse

$$W^{-1} = (w_1^{-1}, w_2^{-1}, \ldots, w_m^{-1}).$$

Le produit, ou succession de deux opérateurs est

$$W \times W' = (w_1 w'_1, w_2 w'_2, \ldots, w_m w'_m),$$

c'est un automorphisme de même nature, indépendant de l'ordre du produit. L'ensemble des transformations W est donc un groupe abélien $\mathfrak{W}_m$ isomorphe à un produit direct de groupes cycliques d'ordre $p-1$ (groupes multiplicatifs des classes, mod$p$, premières avec p).

Considérons d'autre part le groupe $\mathfrak{I}_m \cong \mathfrak{P}_m | \mathfrak{Z}_1$ des automorphismes intérieurs (ou transmutations) de $\mathfrak{P}_m$, le groupe $\mathfrak{V}_m$ est le groupe engendré (1) par $\mathfrak{I}_m$ et $\mathfrak{W}_m$.

Démonstration. — Nous allons établir la propriété par récurrence sur m; elle est manifestement vraie pour $\mathfrak{P}_1$, supposons-la vraie pour $\mathfrak{P}_{m-1}$ et considérons un groupe $\mathfrak{H}$ de tableaux H, invariant pour les automorphismes de $\mathfrak{V}_m$. Les tableaux H_{m-1} forment un groupe $\mathfrak{H}_{m-1}$, évidemment invariant pour les

(1) Le groupe ainsi constitué ne contient pas tous les automorphismes de $\mathfrak{P}_m$, mais on peut aisément démontrer qu'il est constitué par ceux de ces automorphismes qui sont en même temps des automorphismes intérieurs du groupe symétrique $\mathfrak{S}_{p^m}$, dont $\mathfrak{P}_m$ est un p-groupe de Sylow.

automorphismes de $\mathfrak{P}_{m-1}$; c'est donc par l'hypothèse de récurrence, un G. P. I. de $\mathfrak{P}_{m-1}$, donc défini par une indicatrice

$$< k_1, k_2, \ldots, k_{m-1} >.$$

Appelons k_m le maximum des hauteurs $|\mathrm{H}|_m$, des tableaux de $\mathfrak{H}$, il existe un tableau H tel que

$$\mathrm{H} = [\mathrm{H}_{m-1}, g(\mathrm{X}_{m-1})], \qquad h[g(\mathrm{X}_{m-1})] = k_m.$$

Considérons alors une transformation

$$\mathrm{W} = (1, 1, \ldots, w) \qquad (w \neq 1),$$

(ce qui suppose $p > 2$) et formons $\mathrm{W}(\mathrm{H})\mathrm{H}^{-1}$, qui est toujours dans $\mathfrak{H}$, par application des formules (1.1′) et (2.2′)

$$\begin{aligned} \mathrm{W}(\mathrm{H})\,\mathrm{H}^{-1} &= [\mathrm{H}_{m-1}, w\,g(\mathrm{X}_{m-1})]\left[\mathrm{H}_{m-1}^{-1}, -g\left(\mathrm{X}_{m-1}^{\mathrm{H}_{m-1}^{-1}}\right)\right] \\ &= [0, \ldots, 0, (w-1)\,g(\mathrm{X}_{m-1})], \qquad h[(w-1)\,g(\mathrm{X}_{m-1})] = k_m. \end{aligned}$$

Donc, par application du corollaire du lemme 2, $\mathfrak{H}$ étant distingué, contient tout tableau de la forme

$$\mathrm{A} = [0, \ldots, 0, a(\mathrm{X}_{m-1})], \qquad h[a(\mathrm{X}_{m-1})] \leqq k_m.$$

Considérons alors des fonctions quelconques $d(\mathrm{X}_s)$, vérifiant les conditions

$$h[d(\mathrm{X}_{s-1})] \leqq k_s, \qquad (s \text{ de } 1 \text{ à } m-1), \qquad h[d(\mathrm{X}_{m-1})] \leqq k_m.$$

Par application de l'hypothèse de récurrence et de la détermination de k_m, il existe dans $\mathfrak{H}$, un tableau

$$\mathrm{D}_1 = [\ldots, d(\mathrm{X}_i), \ldots, a(\mathrm{X}_{m-1})], \qquad h[a(\mathrm{X}_{m-1})] \leqq k_m,$$

il y existe d'autre part le tableau

$$\mathrm{D}_2 = [\ldots, 0, \ldots, d(\mathrm{X}_{m-1}) - a(\mathrm{X}_{m-1})],$$

et par suite le tableau

$$\mathrm{D}_2 \times \mathrm{D}_1 = [d, d(\mathrm{X}_1), \ldots, d(\mathrm{X}_{m-2}), d(\mathrm{X}_{m-1})].$$

C'est dire que le groupe $\mathfrak{H}$ contient tous les tableaux dont l'indicatrice est au plus égal à

$$< k_1, k_2, \ldots, k_{m-1}, k_m >;$$

comme il n'en contient pas d'autre, d'après la détermination des hauteurs k_s, c'est bien le G. P. I. défini par cette indicatrice.

THÉORÈME 10. — *Les G. P. I. de $\mathfrak{P}_m$ en sont des sous-groupes caractéristiques.*

La démonstration va être faite en plusieurs étapes, exprimées par des lemmes, qui présentent en eux-mêmes un certain intérêt.

LEMME 11. — *Tout G. P. I.* $\mathfrak{D}_s$ *est un sous-groupe caractéristique de* $\mathfrak{P}_m$.

Rappelons que $\mathfrak{D}_s$ est l'ensemble de tous les tableaux dont la profondeur est au moins égale à s, c'est-à-dire dont les s premières coordonnées sont nulles, son indicatrice est

$$< 0, \ldots, 0, p^s, p^{s+1}, \ldots, p^{m-1} >.$$

Nous allons démontrer ce lemme par récurrence sur m, en le supposant vrai pour $\mathfrak{P}_{m-1}$ (il est manifeste pour $\mathfrak{P}_1$), il suffit de le vérifier pour

$$\mathfrak{D}_{m-1} \text{ dans } \mathfrak{P}_m \text{ d'indicatrice } < 0, \ldots, 0, p^{m-1} >.$$

Dans la S. C. A. de $\mathfrak{P}_m$ formons le terme $\mathfrak{Z}_r$, de rang $r = p^{m-2} + 1$, les termes de son indicatrice sont

$$\max(0, p^{u-1} - p^{m-1} + 1 + p^{m-2}).$$

Or, pour u inférieur à m (toujours en tenant compte de $p > 2$)

$$p^{u-1} - p^{m-1} + 1 + p^{m-2} < 1 + 2p^{m-2} - p^{m-1} \leq 0.$$

De sorte que $\mathfrak{Z}_r$ est le groupe abélien constitué par les tableaux

$$(5.2) \qquad [0, \ldots, 0, a(x_1, \ldots, x_{m-1})], \qquad h[a(x_1, \ldots, x_{m-1})] \leq p^{m-2} + 1 = h[x_{m-1}].$$

On peut alors vérifier que $\mathfrak{D}_{m-1}$ est le *centralisateur* de ce groupe $\mathfrak{Z}_r$, d'une part il le contient, et comme il est abélien, il est contenu dans ce centralisateur. D'autre part si A est un tableau qui n'est pas dans $\mathfrak{D}_{m-1}$, il a une coordonnée de rang $u < m$, non nulle

$$[\mathrm{A}]_u = a(\mathrm{X}_{u-1}) \not\equiv 0;$$

il existe dans $\mathfrak{Z}_r$ un tableau B dont la dernière coordonnée (la seule non nulle) est x_u et il en résulte

$$(\mathrm{A}, \mathrm{B}) = [0, \ldots, 0, -a(\mathrm{X}_{u-1})] \not\equiv \text{unité de } \mathfrak{P}_m.$$

Par suite A n'est pas dans le centralisateur de $\mathfrak{Z}_r$, qui ne contient donc que les termes de $\mathfrak{D}_{m-1}$.

$\mathfrak{D}_{m-1}$ étant centralisateur d'un sous-groupe caractéristique de $\mathfrak{P}_m$, est lui-même caractéristique.

COROLLAIRE. — *La profondeur d'un tableau est un invariant pour tous les automorphismes du groupe* $\mathfrak{P}_m$.

LEMME 12. — *Tout G. P. I.* $\mathfrak{F}_{h,s}$ *dont l'indicatrice est*

$$< 0, \ldots, 0, h, p^{s+1}, \ldots, p^{m-1} >, \qquad 0 \leq h \leq p^s;$$

est un sous-groupe caractéristique de $\mathfrak{P}_m$.

Dans la S. C. D. de $\mathfrak{P}_m$, le terme $\tilde{\mathfrak{Z}}_r$, de rang $r = p^s - h$ a pour coordonnée de rang $s+1$ (th. 6)

$$|\,\mathfrak{Z}_r\,|_{s+1} = p^s - (p^s - h) = h \geqq 0,$$

il en résulte que

$$\mathfrak{F}_{h,s} = \{\,\mathfrak{D}_s \cap \tilde{\mathfrak{Z}}_r,\ \mathfrak{D}_{s+1}\,\};$$

les groupes qui entrent dans cette construction étant caractéristiques, il en est de même du résultat $\mathfrak{F}_{h,s}$.

Appelons *hauteur principale* d'un tableau la hauteur de sa première coordonnée non nulle; c'est $|\,A\,|_{s+1}$ pour un tableau A, de profondeur s.

Lemme 13. — *La hauteur principale d'un tableau est un invariant pour tous les automorphismes du groupe* $\mathfrak{P}_m$.

Considérons un tableau A, de profondeur s et de hauteur principale h, son transformé A^α, où α est un automorphisme de $\mathfrak{P}_m$ est aussi de profondeur s (Corollaire du lemme 11). D'autre part A étant contenu dans $\mathfrak{F}_{h,s}$ qui est caractéristique, il en est de même de A^α, de sorte que

$$|\,A^\alpha\,|_{s+1} \leqq h = |\,A\,|_{s+1}.$$

Mais le même raisonnement, appliqué à A^α et à la transformation α^{-1} donne

$$|\,A\,|_{s+1} = |\,(A^\alpha)^{\alpha-1}\,|_{s+1} \leqq |\,A^\alpha\,|_{s+1};$$

il y a donc égalité des hauteurs principales A et d'un de ses transformés, quelconque A^α.

Remarque. — Si $\mathfrak{R}$ et $\mathfrak{R}'$ sont deux G. P. (non nécessairement distingués) différents, il y a au moins un rang s tel que $|\,\mathfrak{R}\,|_s$ et $|\,\mathfrak{R}'\,|_s$ soient différents. Supposons par exemple que le premier soit le plus grand; il contient des tableaux A, de profondeur $s-1$ et de hauteur principale $|\,A\,|_s = |\,\mathfrak{R}\,|_s$. D'après le lemme 13, pour tout α, automorphisme de $\mathfrak{P}_m$,

$$|\,A^\alpha\,|_s = |\,A\,|_s = |\,\mathfrak{R}\,|_s > |\,\mathfrak{R}'\,|_s \qquad \text{et} \qquad A^\alpha \notin \mathfrak{R}'.$$

Donc aucun transformé de $\mathfrak{R}^\alpha$ de $\mathfrak{R}$ ne peut être égal à $\mathfrak{R}'$ (et de même $\mathfrak{R}'^\alpha$ ne peut être égal à $\mathfrak{R}$, sinon $\mathfrak{R}^{\alpha^{-1}}$ serait égal à $\mathfrak{R}'$).

Lemme 14. — *Pour un tableau* A *de profondeur* $s \leqq m-2$, *le nombre de zéros de son premier terme* (non nul) $|\,A\,|_{s+1} = a(X_s)$ *est un invariant pour tous les automorphismes du groupe* $\mathfrak{P}_m$.

Par zéro de $a(X_s)$ on entend, bien entendu un vecteur X_s (de coordonnées $x_i, \ldots, x_s$, définies mod$p$) qui annule le polynome.

Formons le groupe $\mathfrak{L}(A)$ des tableaux de $\mathfrak{D}_{s+1}$ qui sont permutables avec A, au module près $\mathfrak{D}_{s+2}$, puis le groupe quotient $\overline{\mathfrak{L}}(A) = \mathfrak{L}(A)|\mathfrak{D}_{s+2}$. Il reste iso-

morphe à lui-même dans tout automorphisme α, qui remplace A par A^{α} et laisse invariants les sous-groupes caractéristiques $\mathfrak{D}_{s+1}$ et $\mathfrak{D}_{s+2}$. L'ordre de ce groupe quotient est donc un invariant; pour le calculer nous pouvons évidemment remplacer A par le tableau de profondeur $s+2$

$$[0, \ldots, 0, a(X_s), \ldots], \qquad a(X_s) = [A]_{s+1}.$$

Pour qu'un tableau D, de $\mathfrak{D}_{s+1}$, et de première coordonnée $d(X_{s+1})$ soit dans $\overline{\mathfrak{L}}(A)$, il faut et il suffit que le commutateur

$$(D_{s+2}, A_{s+2}) = [0, \ldots, 0, d(X_{s+1}) - d(X_{s+1}^{A_{s+1}}]$$

soit l'unité de $\mathfrak{P}_{s+2}$, c'est-à-dire que

$$d(X_{s+1}) - d(X_{s+1}^{A_{s+1}}) = 0. \tag{5.3}$$

Or, d'après le lemme 5, le nombre de solutions de cette équation fonctionnelle est $p^{t(A_{s+1})}$, où $t(A_{s+1})$ est le nombre de domaines de transitivité de la transformation $X_{s+1}^{A_{s+1}}$, qui est définie par

$$x_u^{A_{s+1}} = x_u \quad (\text{pour} \quad u < s+1), \qquad x_{s+1}^{A_{s+1}} = x_{s+1} - a(X_s).$$

Les vecteurs

$$X_{s+1} = (X_s, x_{s+1}), \qquad a(X_s) = 0,$$

sont conservés par la transformation A_{s+1} et constituent chacun un domaine de transitivité; leur nombre est $pn(A)$ où $n(A)$ est le nombre de zéros de $a(X_s)$.

Les autres vecteurs forment des domaines de transitivité de chacun p éléments (pour chaque valeur de X_s et les p valeurs de x_{s+1}); le nombre de ces domaines est $p^s - n(A)$.

Finalement

$$t(A_{s+1}) = p^s - n(A) + pn(A) = p^s + (p-1)n(A).$$

C'est un invariant, comme l'ordre $p^{t(A_{s+1})}$ et il en est de même du nombre $n(A)$ de zéros de $a(X_s)$.

En outre, si pour deux tableaux A et B, les nombres $n(A)$ et $n(B)$ sont différents, il en est de même des ordres de $\overline{\mathfrak{L}}(A)$ et de $\overline{\mathfrak{L}}(B)$; il n'y a donc aucun automorphisme α qui transforme A en B.

Lemme 15. — *Si, dans un tableau de profondeur s* et d'ordre p, *la première coordonnée non nulle* $[A]_{s+1} = a(X_s)$ *n'a aucun zéro, les hauteurs des coordonnées suivantes vérifient les inégalités*

$$|A|_u \leq p^{u-1} - p^s, \qquad u \geq s+2.$$

Il suffit de démontrer que, les conditions de l'énoncé étant remplies, on peut trouver un tableau B, de profondeur supérieure à s tel que

$$B^{-1}AB = [0, \ldots, 0, a(X_s), 0, \ldots, 0] = A', \tag{5.4}$$

car l'application de (3.9) montre alors que

$$|A|_u = |BA'B^{-1}|_u \leqq \mathrm{Max}(|A'|_u, p^{u-1} - p^s) = p^{u-1} - p^s.$$

Raisonnons par récurrence et supposons obtenu un tableau B_r tel que

$$C = B_r^{-1} A B_r = [0, \ldots, 0, a(X_s), 0, \ldots, c(X_r), \ldots], \qquad r > s,$$

c'est-à-dire que dans C, les $(r-s-1)$ coordonnées qui suivent celle de rang $s+1$ sont nulles ($r-s-1$ pouvant être nul). Calculons la puissance p

$$C^p = [0, \ldots, 0, c(X_r) + c(X_r^{c_r}) + \ldots + c(X_r^{c_r^{p-1}}), \ldots],$$

cette puissance est l'unité de $\mathfrak{P}_m$, puisque C est d'ordre p, donc

$$0 = \Sigma c(X_r^{c_r^u}) = \Sigma c[x_1, \ldots, x_s, x_{s+1} - u\,a(X_s), x_{s+2}, \ldots, x_r];$$

(u de 0 à $p-1$, toutes valeurs des x_i).

Comme $a(X_s)$ n'est pas nul, pour des valeurs déterminées de X_s et x_{s+1}, la différence $x_{s+1} - u\,a(X_s)$ prend toutes les valeurs de zéro à $p-1$, pour les valeurs de u variant dans les mêmes limites. Par suite, pour des valeurs déterminées des x_i, les vecteurs de la somme sont les domaines de transitivité du tableau C_r dans E_r et l'identité est équivalente à

$$\mathbf{S}_{T(C)} c(X_r) = 0, \qquad T(C), \text{ domaines de transitivité de C.}$$

D'après le lemme 6, l'équation fonctionnelle

$$f(X_r) - f(X_r^{c_r}) = c(X_r),$$

a donc une solution. Posons

$$B'_r = [0, \ldots, 0, f(X_r), 0, \ldots, 0], \qquad B_{r+1} = B_r B'_r,$$

et formons le tableau

$$C' = B_r'^{-1} C B'_r = B_{r+1}^{-1} A B_{r+1} = [0, \ldots, 0, a(X_s), 0, \ldots, 0, c'(X_r), \ldots],$$

le terme de rang $r+1$

$$c'(X_r) = -f(X_r) + f(X_r^{c_r}) + c(X_r^{c_r}),$$

y est nul. Donc, dans C' construit avec B_{r+1}, le premier terme non nul, après celui de rang $s+1$ est celui de rang au moins $r+2$ (au lieu de $r+1$). On peut ainsi construire de proche en proche un tableau B vérifiant la condition (5.4).

LEMME 16. — *Le G. P. I. $\mathfrak{C}_s$ dont l'indicatrice est*

$$< 0, \ldots, 0, p^s, p^{s+1} - p^s, \ldots, p^{m-1} - p^s >,$$

est un sous-groupe caractéristique de $\mathfrak{P}_m$.

Remarquons que, en supposant toujours $p \neq 2$, il existe des polynomes en $x_1, \ldots, x_s$, de hauteur (maximum) p^s, qui n'ont pas de zéro; notamment

$$x_1^{p-1} x_2^{p-1} \ldots x_s^{p-1} + 1.$$

Considérons alors l'ensemble des tableaux θ vérifiant les conditions suivantes :

1° Tout tableau θ est de profondeur s;
2° Tout tableau θ est d'ordre p;
3° La coordonnée de rang $s+1$ de θ n'a pas de zéro.

D'après les lemmes 11 et 14, cet ensemble est invariant pour tous les automorphismes du groupe $\mathfrak{P}_m$. Le groupe $\mathfrak{C}_s$ qu'ils engendrent est donc un sous-groupe caractéristique, donc un G. P. I. Il contient le tableau

$$[0, \ldots, 0, x_1^{p-1} \ldots x_s^{p-1} + 1, 0, \ldots, 0],$$

de sorte que $|\mathfrak{C}_s|_{s+1} = p^s$.

D'autre part, d'après le lemme 15, pour tout tableau θ,

$$|\theta|_u \leq p^{u-1} - p^s, \qquad u \geq s+2.$$

Mais le théorème 4 donne la même limite inférieurement, de sorte que

$$|\mathfrak{C}_s|_u = p^{u-1} - p^s, \qquad u \geq s+2.$$

Lemme 17. — *Le G. P. I. $\mathfrak{C}_{s,h}$, dont l'indicatrice est*

$$< 0, \ldots, 0, h, p^{s+1} - p^s, \ldots, p^{m-1} - p^s >,$$

est un sous-groupe caractéristique de $\mathfrak{P}_m$.

Construisons par récurrence, les sous-groupes

$$\mathfrak{C}_{s,p^s} = \mathfrak{C}_s, \qquad \mathfrak{C}_{s,h-1} = (\mathfrak{C}_{s,h}, \mathfrak{P}_m),$$

ils sont caractéristiques. D'autre part le théorème 5 montre que le sous-groupe $\mathfrak{C}_{s,h}$ ainsi construit a bien l'indicatrice indiquée par le lemme.

Démonstration du théorème 10. — Considérons un G. P. I., quelconque, de profondeur s et d'indicatrice

$$< 0, \ldots, 0, k_{s+1}, \ldots, k_m > \qquad \text{avec} \quad k_u \geq p^{u-1} - p^s;$$

il est engendré par les sous-groupes

$$\mathfrak{E}_{s,k_{s+1}}, \quad \mathfrak{E}_{s+1,k_{s+2}}, \quad \ldots, \quad \mathfrak{E}_{m-1,k_m},$$

qui sont caractéristiques, il est donc lui-même caractéristique.

Nous allons compléter ces divers résultats en déterminant parmi les sous-groupes caractéristiques, les *dérivées successives* $\mathfrak{K}_s$ de $\mathfrak{P}_m$ et les groupes $\mathfrak{L}_l$ engendrés par les *puissances d'exposant* p^l, des éléments de $\mathfrak{P}_m$.

Rappelons que les dérivées successives, d'un groupe $\mathfrak{G}$ quelconque sont définis par les relations de récurrence

$$\mathfrak{K}_0 = \mathfrak{G}, \qquad \mathfrak{K}_{s+1} = (\mathfrak{K}_s, \mathfrak{K}_s).$$

THÉORÈME 11. — *La dérivée* $\mathfrak{K}_s$, *de rang* s, *de* $\mathfrak{P}_m$, *est le G. P. I. de profondeur* s, *qui a pour indicatrice*

$$< 0, \ \ldots, \ 0, \ , p^s - p^{s-1}, \ \ldots, \ p^{m-1} - p^{s-1} >$$

ou

$$| \mathfrak{K}_s |_u = p^{u-1} - p^{s-1}, \qquad u \geqq s.$$

Nous allons démontrer la propriété par récurrence sur s; elle est vraie pour $\mathfrak{K}_1 = \mathfrak{Z}_1$ d'indicatrice

$$< 0, \ p - 1, \ p^2 - 1, \ \ldots, \ p^{m-1} - 1 >.$$

Supposons-la établie pour $\mathfrak{K}_s$; sa profondeur étant s, la formule (3.5) appliquée à deux tableaux quelconques A et A′ de cette dérivée donne

$$| (\mathrm{A}, \mathrm{A}') |_{u+1} \leqq p^u - p^s;$$

la profondeur de la dérivée suivante $\mathfrak{K}_{s+1}$ est donc au moins $s+1$.

Reste à montrer que, pour tout $u > s$, il existe au moins deux tableaux, pour lesquels cette comparaison devient une égalité.

Or, $\mathfrak{K}_s$ contient le tableau

$$\mathrm{A} = [0, \ \ldots, \ 0, \ x_s, \ 0, \ \ldots, \ 0], \qquad | \mathrm{A} |_{s+1} = p^{s-1} + 1 < p^s - p^{s-1} = | \mathfrak{K}_s |_{s+1},$$

il contient d'autre part, quel que soit $u > s$, le tableau

$$\mathrm{A}' = [0, \ \ldots, \ 0, \ (x_1^{p-1} \ldots x_s^{p-2} \ldots x_u^{p-1}), \ 0, \ \ldots, \ 0],$$

dont le seul terme, non nul, de rang $u+1$, a pour hauteur

$$h[x_1^{p-1} \ldots x_s^{p-2} \ldots x_u^{p-1}] = p^u - p^{s-1} = | \mathfrak{K}_s |_{u+1}.$$

Leur commutateur a pour terme de rang $u+1$

$$\begin{aligned} [(\mathrm{A}, \mathrm{A}')]_{u+1} &= - x_1^{p-1} \ldots x_s^{p-2} \ldots x_u^{p-1} + x_1^{p-1} \ldots x_s^{p-2} (x_{s+1} - x_s)^{p-1} x_{s+2}^{p-1} \ldots x_u^{p-1} \\ &= - (p-1) x_1^{p-1} \ldots x_s^{p-1} x_{s+1}^{p-2} x_{s+2}^{p-1} \ldots x_u^{p-1} + \text{termes hauteur inf.} \end{aligned}$$

dont la hauteur est bien égale à $p^u - p^s$.

Pour résoudre le deuxième problème établissons encore un lemme :

LEMME 18. — *La puissance A^{p^l} d'un tableau quelconque est de profondeur au moins l et les hauteurs de ses coordonnées non nulles vérifient*

$$|A^{p^l}|_u \leq p^{u-1} - p^l + 1, \qquad u \geq l+1,$$

il y a égalité, si quel que soit u

$$|A|_u = p^{u-1}.$$

Remarquons d'abord qu'un monome, de variable X_{u-1}, ne peut être de hauteur au moins égale à $p^{u-1} - p^l + 1$ que dans le cas où les puissances des variables de x_{l+1} à x_{u-1} sont toutes d'exposant $p-1$. Car si une variable $x_\nu (l+1 \leq \nu \leq u-1)$ était de puissance inférieure, la hauteur du monome serait au plus égale à

$$p^{u-1} - p^{\nu-1} \leq p^{u-1} - p^l.$$

En outre

$$h(x_{l+1}^{p-1} \dots x_{u-1}^{p-1}) = p^{u-1} - p^l + 1.$$

L'énoncé est donc équivalent a l'affirmation que dans $[A^{p^l}]_u = a(X_{u-1})$, il n'y a pas de monomes de la forme $f(X_l) x_{l+1}^{p-1} \dots x_{u-1}^{p-1}$, sauf avec $f(X_l)$ constant. En particulier, il entraîne

$$|A^{p^l}|_l = a(x_1, \dots, x_{l-1}) = \text{const.}$$

On peut établir la propriété par récurrence sur l: elle est manifeste pour $l = 0$, puisque

$$|A|_u \leq p^{u-1} = p^{u-1} - p^0 + 1.$$

Supposons-la vraie pour

$$B = A^{p^{l-1}} = [0, \dots, b, \dots, b(X_{u-1}), \dots], \qquad b \text{ de rang } l;$$

il suffit de la vérifier pour les coordonnées de $A^{p^l} = B^p$, qui sont :

$$[B^p]_u = \Sigma b\left(X_{u-1}^{Bi_u}\right); \qquad i \text{ de } 0 \text{ à } p-1.$$

le terme de rang l est manifestement nul et la profondeur est au moins l. Les monomes qui dépasseraient la limite indiquée dans cette somme, ne peuvent provenir que des monomes de $b(X_{u-1})$, qui seraient de l'une des deux formes (s'il en existe)

$$x_1^{i_1} \dots x_l^{i_l} x_{l+1}^{p-1} \dots x_{u-1}^{p-1}, \qquad i_l < p-1, \qquad x_l^{p-1} x_{l+1}^{p-1} \dots x_{u-1}^{p-1}.$$

En étudiant les termes qui en proviennent on constate que le premier ne donne que des termes de hauteur inférieure et que le second donne des termes de hauteur au plus égal à $p^{u-1} - p^l + 1$. L'égalité n'a lieu que si $b \neq 0$, ou $|B|_l = 1$. L'existence de monomes de la deuxième forme exige, par ailleurs, pour tout u

$$|B|_u = p^{u-1} - p^{l-1} + 1,$$

les égalités sont alors vérifiées pour B^p. On obtient donc, par récurrence, la forme nécessaire de A, indiquée par le lemme

$$|A|_u = p^{u-1} \qquad \text{ou} \qquad |A| = <1,\ p,\ p^2,\ \ldots,\ p^{m-1}>,$$

d'où

$$|A^{p^l}| = <\ldots,\ \text{Max}(0,\ p^{u-1} - p^l + 1),\ \ldots>.$$

THÉORÈME 12. — *Le groupe $\mathfrak{L}_l$, engendré par des puissances, d'exposant p^l, des tableaux de $\mathfrak{P}_m$ est le G. P. I., de profondeur l, qui a pour indicatrice*

$$<0,\ \ldots,\ 0,\ 1,\ p^{l+1} - p^l + 1,\ \ldots,\ p^{m-1} - p^l + 1>.$$

Comme il est caractéristique, ce groupe est un G. P. I.; son indicatrice résulte immédiatement du lemme précédent.

CHAPITRE VI.

ÉTUDE DU GROUPE $\mathfrak{P}_2$.

Ce Chapitre est consacré à l'étude du p-groupe $\mathfrak{P}_2$ de Sylow, du groupe symétrique de degré p^2, son ordre est $p^p + 1$. Il possède ainsi que ses sous-groupes transitifs, non commutatifs $\mathfrak{H}$, un sous groupe distingué abélien, élémentaire, d'indice p. Des groupes possédant cette propriété ont été étudiés par G. A. Miller(1) et, avec une autre méthode, par H. R. Brahana(2).

L'algorithme des tableaux permet de faire une étude très détaillée de $\mathfrak{P}_2$. Nous déterminerons d'une part son groupe d'automorphismes, d'autre part ses sous-groupes (leur type et leur position respective).

Il est isomorphe à l'ensemble des tableaux de rang 2, $A = [a,\ a(x)]$ avec la loi de composition

$$[a,\ a(x)]\,[b,\ b(x)] = [a + b,\ a(x) + b(x - a)], \tag{6.1}$$

l'unité est le tableau $[0, 0]$, l'inverse de $A = [a,\ a(x)]$ est $A^{-1} = [-a, -a(x+a)]$.

La S. C. A. qui coïncide avec la S. C. D. a $p + 1$ termes (la classe de $\mathfrak{P}$ est p)

$$\mathfrak{Z}_0 = \text{unité de } \mathfrak{P}_2, \qquad \mathfrak{Z}_1,\ \ldots,\ \mathfrak{Z}_u,\ \ldots,\ \mathfrak{Z}_p = \mathfrak{P}_2,$$

le terme $\mathfrak{Z}_u$ est l'ensemble des tableaux

$$[0,\ a(x)], \qquad h[a(x)] \leq u \qquad \text{ou} \qquad \text{degré } a(x) \leq u - 1.$$

---

(1). *Determination* (*Bull. of Amer. Math. Soc.*, Série 2, Vol. 8, 1909, p. 398).

(2) *On isomorphism of abelian groupe* (*Amer. Journal*, Vol. LVI, 1934, p. 53 à 61).

En plus de ces sous-groupes, $\mathfrak{P}_2$ posséde deux sous-groupes caractéristiques

$$\mathfrak{D}_1 : \text{ensemble } [0, a(x)], \qquad \text{degré } a(x) \leq p-1,$$
$$\mathfrak{E} : \text{ensemble } [a, a(x)], \qquad \text{degré } a(x) \leq p-2.$$

Les indicatrices des G. P. I. sont en effet (th. 4)

$$<1, p>, \quad <1, \quad p-1> \quad \text{et} \quad <0, i>, \quad 0 \leq i \leq p.$$

Recherche des automorphismes. — Le groupe $\mathfrak{P}_2$ peut être engendré par les deux tableaux $A_1=[1, 0]$, $A_2=[0, x^{p-1}]$. Un automorphisme α sera donc caractérisé par la donnée des tableaux A_1^α, A_2^α. Or

$$A_1 \in \mathfrak{E} \quad \text{et} \quad A_1 \notin \mathfrak{D}_1 \quad \text{entraînent} \quad A_1^\alpha \in \mathfrak{E} \quad \text{et} \quad A_1^\alpha \notin \mathfrak{D}_1;$$

puisque ces sous-groupes sont caractéristiques, on en conclut que A_1^α ne peut qu'être de la forme

$$[c, c_{p-2}x^{p-2} + \ldots + c_0] \qquad (c \neq 0),$$

ce qui donne $(p-1)p^{p-1}$ transformations possibles.

De la même façon

$$A_2 \in \mathfrak{D}_1 \quad \text{et} \quad A_2 \notin \mathfrak{Z}_{p-1} \quad \text{entraînent} \quad A_2^\alpha \in \mathfrak{D}_1 \quad \text{et} \quad A_2^\alpha \notin \mathfrak{Z}_{p-1},$$

de sorte que A_2^α ne peut qu'être de la forme

$$[0, dx^{p-1} + d_{p-2}x^{p-2} + \ldots + d_0] \qquad (d \neq 0),$$

ce qui donne $(p-1)p^{p-1}$ formes possibles.

Les combinaisons de ces transformations donnent une majoration du nombre des automorphismes dont on désigne le groupe par $\mathfrak{A}$

$$\text{ordre de } \mathfrak{A} \leq (p-1)^2 p^{2p-2}. \tag{6.2}$$

Nous allons montrer que ce maximum est en effet atteint, de sorte qu'on a bien construit ainsi tous les automorphismes.

On peut construire un automorphisme en faisant correspondre à tout tableau A, le tableau

$$\Phi(A) = [a, a(x) + f_1 a'(x) + f_2 a''(x) + \ldots + f_{p-1} a^{(p-1)}(x)],$$

où $a'(x)$, $a''(x)$, ... sont les dérivées successives de $a(x)\big(a^{(p)}(x)=0\big)$ et $[f_0=1, f_1, f_2, \ldots, f_{p-1}]$ est un système d'éléments de G_p, qui sera désigné par φ et auquel sera asssocié le polynome

$$\varphi(y) = f_0 + f_1 y + f_2 y^2 + \ldots + f_{p-1} y^{p-1} \pmod{y^p}.$$

On vérifie immédiatement que cette transformation conserve l'opération

$$\Phi(A)\Phi(B) = \Phi(AB).$$

En outre,

$$\Phi(A_1) = A_1, \qquad \Phi(A_2) = [0, x^{p-1} + g(x)], \qquad \text{degré } g(x) < p-1,$$

de sorte que $\Phi(A_1)$ et $\Phi(A_2)$ engendrent le groupe et la transformation est biunivoque.

Le produit de deux automorphismes

$$\varphi = [f_0, f_1, \ldots, f_{p-1}], \qquad \varphi' = [f'_0, f'_1, \ldots, f'_{p-1}], \qquad f_0 = f'_0 = 1$$

est

$$\psi = \left[f_0 f'_0, f_0 f'_1 + f_1 f'_0, \ldots, \sum_{i+j=k} f_i f'_j, \ldots, \sum_{i+j=p-1}{}' f_i f'_j \right],$$

ce qu'on peut exprimer par

$$\psi(y) \equiv \varphi(y)\varphi'(y) \pmod{y^p} \quad (\text{dans } G_p).$$

En outre,

$$[\varphi(y)]^p = \varphi(y^p) \equiv 1 \pmod{y^p}.$$

L'ensemble des automorphismes ainsi construits forme donc un groupe abélien $\mathfrak{F}$, dont tous les termes sont d'ordre p, c'est-à-dire encore qui est un groupe élémentaire, produit de $p-1$ groupes d'ordre p.

Formons l'intersection de $\mathfrak{F}$ avec le groupe $\mathfrak{I}$ des automorphismes intérieurs (ou transmutations) de $\mathfrak{P}_m$, qui est isomorphe à $\mathfrak{P}_m | \mathfrak{Z}_1$, donc d'ordre p^p. Le tableau $A_1 = [1, 0]$, qui est invariant pour les automorphismes Φ (de $\mathfrak{F}$), est transformé par une transmutation en

$$[a, a(x)][1, 0][-a, -a(x+a)] = [1, a(x) - a(x-1)],$$

il ne reste invariant que pour les transmutations définies par les tableaux $[a, c]$, où c est une constante. Mais ces tableaux, pour une même valeur de a, et les diverses valeurs de c, définissent un automorphisme Φ, car

$$[a, c][b, b(x)][-a, -c] = [b, b(x-a)],$$

et

$$b(x-a) = b(x) + (-a)b'(x) + \frac{1}{2!}(-a)^2 b''(x) + \ldots + \frac{1}{(p-1)!}(-a)^{p-1} b^{(p-1)}(x).$$

Comme $\mathfrak{I}$ est sous-groupe distingué de $\mathfrak{A}$, le groupe $\{\mathfrak{I}, \mathfrak{F}\}$, construit avec les éléments de $\mathfrak{I}$ et de $\mathfrak{F}$, est d'ordre $(p^{p-1} p^p) : p = p^{2p-2}$. Tenant compte de l'inégalité (6.2), c'est un p-groupe de Sylow de $\mathfrak{A}$.

Considérons d'autre part les automorphismes W, du groupe $\mathfrak{W}$, construit dans la théorie générale (Cahp. V), dans le cas actuel ce sont

$$W = (w_1, w_2), \qquad W(a, a(x)) = [w_1 a, w_2 a(w_1^{-1} x)],$$

il y en a $(p-1)^2$. On vérifie par un calcul immédiat que $\mathfrak{F}$ est permutable dans son ensemble avec les opérations W, et il en est de même du groupe précédent $\{\mathfrak{J}, \mathfrak{F}\}$. Donc :

Le groupe $\{\mathfrak{W}, \mathfrak{J}, \mathfrak{F}\}$ *est un groupe d'ordre* $(p-1)^2 p^{2p-2}$, *qui est donc* [en raison de l'inégalité (6.2)] *le groupe* $\mathfrak{A}$ *de tous les automorphismes de* $\mathfrak{P}_2$.

Éléments conjugués. — Le transmué d'un tableau $A = [a, a(x)]$ par un tableau $Q = [q, q(x)]$ est

$$QAQ^{-1} = [a, a(x-q) + q(x) - q(x-a)].$$

La première coordonnée a d'un tableau est donc un invariant pour les automorphismes intérieurs. Un autre invariant est le coefficient a_{p-1} de x^{p-1} dans $a(x)$, c'est une conséquence du lemme 1 ; un calcul simple permet aussi de le vérifier directement.

Premier cas $a \not\equiv 0$. — Les deux invariants a et a_{p-1} suffisent pour déterminer l'ensemble des éléments conjugués de A. En effet, l'équation fonctionnelle en $t(x)$

$$t(x-a) - t(x) = a(x) - a_{p-1}x^{p-1},$$

a une solution ; et, en transmuant A par le tableau $T = [0, t(x)]$, on obtient

$$TAT^{-1} = [a, a_{p-1}x^{p-1}].$$

a. Les tableaux, pour lesquels a_{p-1} est nul, sont d'ordre p. Pour que deux d'entre eux soient conjugués, il faut et il suffit qu'ils aient même première coordonnée. Il en résulte que tous les sous-groupes cycliques d'ordre p, qui contiennent des tableaux dont la première coordonnée n'est pas nulle, sont conjugués dans $\mathfrak{P}_2$.

b. Les tableaux, pour lesquels a_{p-1} n'est pas nul, sont d'ordre p^2. On peut engendrer un groupe cyclique, indifféremment par un tableau A, d'invariants a, a_{p-1}, ou par sa puissance A^i (i premier avec p), d'invariants ia, ia_{p-1}. Le quotient $c = a : a_{p-1}$ (défini mod p), est un invariant de ce groupe et les sous-groupes cycliques, d'ordre p^2, de même invariant c, sont conjugués, ils forment $p-1$ classes.

Relativement au groupe $\mathfrak{V} = \{\mathfrak{J}, \mathfrak{W}\}$ d'automorphismes, ils ne forment plus qu'une seule classe, car une transformation $W = (w_1, w_2)$ remplace les invariants a, a_{p-1} d'un tableau par $w_1 a$, $w_2 a_{p-1}$ et l'invariant c par $w_1 w_2^{-1} c$.

Deuxième cas $a = 0$. — Le transmué de $A = [0, a(x)]$ par un tableau Q est

$$QAQ^{-1} = [0, a(x-q)].$$

Suivant que $a(x)$ est ou n'est pas constant, la classe des conjugués de A contient 1 ou p éléments. Les tableaux [0, const.] sont les éléments du centre.

Dans un système de tableaux conjugués, pour lesquels $a(x)$ n'est pas constant, on peut prendre pour tableau réduit, celui dont le coefficient du deuxième terme est nul

$$A = [0,\ a_m x^m + a_{m-2}x^{m-2} + \ldots + a_0].$$

Sous-groupes de $\mathfrak{P}_2$. — Premier cas. — Les tableaux du sous-groupe $\mathfrak{H}$ ont tous leur première coordonnée nulle; alors $\mathfrak{H}$ est sous-groupe de $\mathfrak{D}_1$, qui est un groupe élémentaire d'ordre p^p, dont on sait former tous les sous-groupes.

Deuxième cas. — Il y a dans le sous-groupe $\mathfrak{H}$ au moins un tableau A dont la première coordonnée n'est pas nulle, et peut toujours être supposée égale à 1 (en remplaçant A par une puissance convenable A^i). Nous dirons qu'un tel sous-groupe est *essentiel*.

Lemme 19. — *Tout sous-groupe essentiel propre de* $\mathfrak{P}_2$ *est de la forme* $\{A, \mathfrak{Z}_m\}$, *c'est-à-dire est engendré par un tableau* $A = [1,\ a(x)]$ *et les tableaux d'un groupe* $\mathfrak{Z}_m$, *de la S. C. A.*

Ce lemme est vrai si $\mathfrak{H}$ est le groupe cyclique de base $A_1 = [1,0]$. Sinon, $\mathfrak{H}$ contient des tableaux dont la première coordonnée est nulle. En effet, à partir d'un tableau $B = [b,\ b(x)]$, qui n'est pas une puissance de A, il suffit de former

$$A^b B^{-1} = [0,\ c(x)] \qquad \left(B \neq A^b \text{ entraîne } c(x) \neq 0\right).$$

L'ensemble des tableaux de $\mathfrak{H}$, dont la première coordonnée est ainsi nulle, forme un sous-groupe distingué $\overline{\mathfrak{H}}$ de $\mathfrak{H}$; il est élémentaire et $\mathfrak{H} \mid \overline{\mathfrak{H}}$ est cyclique d'ordre p, de sorte que $\mathfrak{H} = \{A, \overline{\mathfrak{H}}\}$.

Dans $\mathfrak{H}$, prenons un tableau $C = [0, c(x)]$, dont la hauteur m soit maximum, et formons, par récurrence, la suite

$$C_0 = C = [0,\ c(x)], \qquad C_l = (A,\ C_{l-1}), \qquad c_l(x) = c_{l-1}(x-1) - c_{l-1}(x),$$

$c_l(x)$ est de hauteur $m - l$. Le groupe $\{C_0, \ldots, C_m\}$, qui coïncide avec $\overline{\mathfrak{H}}$ contient tous les tableaux

$$[Q,\ d(x)], \quad h[d(x)] \leq m.$$

C'est le G. P. I. d'indicatrice $< 0, m >$. Si $m < p$, c'est le groupe $\mathfrak{Z}_m$; si $m = p$, c'est le groupe $\mathfrak{D}_1$, $\mathfrak{H}$ coïncide avec $\mathfrak{P}_2$, et n'est plus propre.

Théorème 13. — *Deux sous-groupes essentiels de* $\mathfrak{P}_2$ *sont isomorphes s'ils sont de même classe et ont même exposant.*

S'ils sont d'exposant p, ils sont conjugués (déduits l'un de l'autre par un automorphisme intérieur).

S'ils sont d'exposant p^2, *ils sont déduits l'un de l'autre par un automorphisme du groupe* $\mathfrak{V} = \{\mathfrak{J}, \mathfrak{W}\}$.

Rappelons que l'*exposant* d'un groupe $\mathfrak{G}$ est le plus petit entier l tel que, pour tout élément de $\mathfrak{G}$, la puissance d'exposant l soit égale à l'unité. La classe d'un p-groupe est le nombre de termes de ses S. C. A. et S. C. D. (th. 3).

Le commutateur d'un sous-groupe essentiel $\{A, \mathfrak{Z}_m\}$ est $\mathfrak{Z}_{m-1}$, donc d'ordre p^{m-1} et le groupe est de classe m. Pour que deux sous-groupes $\{A, \mathfrak{Z}_m\}$, $\{B, \mathfrak{Z}_{m'}\}$ soient isomorphes, il est donc nécessaire que $m = m'$, donc qu'ils soient de même classe.

Si A est d'ordre p, il en est de même de tout élément de $\{A, \mathfrak{Z}_m\}$, car $|\{A, \mathfrak{Z}_m\}|_2 \leq p-1$ [D'après la terminologie de Dickson et Miller, c'est un groupe conforme au groupe abélien de type $(p, \ldots, p)$]. Donc deux sous-groupes essentiels $\{A, \mathfrak{Z}_m\}$ et $\{B, \mathfrak{Z}_m\}$ ne peuvent être isomorphes que si A et B sont à la fois d'ordre p, ou d'ordre p^2. Reste à montrer que ces conditions sont suffisantes.

PREMIER CAS. — A et B sont d'ordre p. Il existe un automorphisme intérieur qui transforme A en B; comme il laisse invariant $\mathfrak{Z}_m$ (qui est caractéristique), il transforme $\{A, \mathfrak{Z}_m\}$ en $\{B, \mathfrak{Z}_m\}$.

DEUXIÈME CAS. — A et B sont d'ordre p^2. Il existe alors un automorphisme, dans le groupe $\mathfrak{V} = \{\mathfrak{J}, \mathfrak{W}\}$ qui transforme A en B, et par suite $\{A, \mathfrak{Z}_m\}$ en $\{B, \mathfrak{Z}_m\}$.

Dans chacun de ces cas, on peut aisément distinguer des tableaux *réduits*

$$\text{exp. } p \text{ , classe } m : [1, a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \ldots + a_m x^m],$$
$$\text{exp. } p^2, \text{ classe } m : [1, a_{p-1}x^{p-1} + a_{p-2}x^{p-2} + \ldots + a_m x^m], \quad a_{p-1} \neq 0.$$

Il y a donc p^{p-m-1} sous-groupes différents du premier type et $(p-1)p^{p-m-1}$ sous-groupes différents du deuxième type.

INDICATIONS BIBLIOGRAPHIQUES.

1. A. KOUROCH, *Théorie des groupes*, Moscou, 1944.
2. A. SPEISER, *Die Theorie der Gruppen von endlicher Ordnung*, 3 Aufl., Berlin, 1937.
3. H. ZASSENHAUSS, *Lehrbuch des Gruppentheorie*, Berlin-Leipzig, 1937.
4. PH. HALL, *A contribution to the theorie of groups of prime power order* (*Proc. of London Math. Soc.*, 36, 1933, p. 29-95).
5. G. A. MILLER, *Determination of all groups of order p^m* (*Bull. of Amer. Math. Soc.*, Série 2, Vol. 8, 1902, p. 391).
6. BRAHANA, *On isomorphisms of abelian groups of type* $(1, \ldots, 1)$ (*Amer. Journ.*, Vol. LVI, 1934, p. 53-61).
7. A. CHATELET, *Les groupes abéliens finis*, Paris-Lille, 1925.