MÉMORIAL DES SCIENCES MATHÉMATIQUES

DE SÉGUIER
POTRON

Théorie des groupes abstraits

Mémorial des sciences mathématiques, fascicule 91 (1938)
<http://www.numdam.org/item?id=MSM_1938__91__1_0>

MÉMORIAL

DES

SCIENCES MATHÉMATIQUES

PUBLIÉ SOUS LE PATRONAGE DE

L'ACADÉMIE DES SCIENCES DE PARIS,

DES ACADÉMIES DE BELGRADE, BRUXELLES, BUCAREST, COÏMBRE, CRACOVIE, KIEW, MADRID, PRAGUE, ROME, STOCKHOLM (FONDATION MITTAG-LEFFLER), DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE, AVEC LA COLLABORATION DE NOMBREUX SAVANTS.

DIRECTEUR:

Henri VILLAT

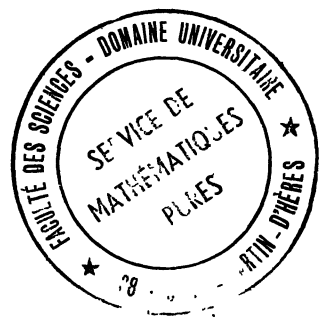
Membre de l'Institut,
Professeur a la Sorbonne,
Directeur du « Journal de Mathématiques pures et appliquées ».

FASCICULE XCI

Théorie des groupes abstraits

Par M. l'Abbé De SÉGUIER
Docteur es sciences mathématiques

et M. l'Abbé POTRON
Ancien élève de l'École Polytechnique
Docteur ès sciences mathematiques
Professeur à l'Institut Catholique de Paris



PARIS
GAUTHIER-VILLARS, IMPRIMEUR-ÉDITEUR
LIBRAIRE DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE
Quai des Grands-Augustins, 55.

1938

THÉORIE DES GROUPES ABSTRAITS

Par M. l'Abbé De SÉGUIER,

Docteur ès sciences mathématiques

et M. l'Abbé POTRON,

Ancien élève de l'École Polytechnique Docteur ès sciences mathématiques,
Professeur à l'Institut catholique de Paris.

CHAPITRE I.

PREMIÈRES DÉFINITIONS ET CONSÉQUENCES.

1. La notion d'ensemble étant supposée acquise, soient E un ensemble quelconque, $a, b, \ldots, l$ des éléments de E, F_n l'ensemble des arrangements n à n avec répétition de tous les éléments de E, F l'ensemble des arrangements des F_n. A chaque élément de F faisons correspondre un élément de E. Disons maintenant, pour simplifier : si l'élément x de E répond à $ab \ldots k$, x est *composé* de $a, b, \ldots, k$ dans cet ordre; et écrivons $x = a \approx b \approx \ldots \approx k$. Lorsque aucune confusion n'est à craindre, on assimile la composition à une multiplication, parfois aussi à une addition, où l'ordre des termes n'est pas indifférent : on écrira ainsi $x = ab \ldots k$ dans la notation multiplicative, et $x = a + b + \ldots + k$ dans la notation additive. Sauf avis contraire, nous emploierons toujours la notation multiplicative.

Si, pour les deux éléments x et y de E, on a $x = ab \ldots k$, $y = ab \ldots kl$, on n'a pas nécessairement $y = xl$. Mais on peut évidemment, après avoir établi arbitrairement la correspondance de E à F_0, déterminer la correspondance de E à $F_1, F_2, \ldots$ successivement, de manière que l'on ait toujours $ab \ldots kl = xl$ si $ab \ldots k = x$, c'est-

à-dire $ab\ldots kl=(ab\ldots k)l$. Nous supposerons désormais qu'il en est ainsi.

La correspondance ainsi établie s'appelle une *loi de composition* des éléments de E. Il n'y a pas, dans cette correspondance, un postulat, mais une convention.

Plus généralement, on pourrait établir arbitrairement la correspondance de E à F_k (k donné >2), puis une correspondance de E à $F_{k+1(k-1)}$, $F_{k+2(k-1)}$, ... vérifiant des conditions analogues [6]. On pourrait composer ainsi les substitutions linéaires de déterminant -1 en prenant $k=3$ ¦[13], [1]¦.

2. Si la composition est *associative*, c'est-à-dire si, dans chaque produit, on peut, sans altérer le produit, remplacer un nombre quelconque de facteurs consécutifs par leur produit (d'après la convention précédente, cela a déjà lieu quand les facteurs consécutifs précèdent tous les autres), E est un *corps*. Il faut et suffit pour cela que $abc=a(bc)$, a, b, c étant trois éléments quelconques (postulat I). Si, quels que soient a et b dans un corps E, $ax=b$ a toujours une solution dans E (postulat II), et de même $xa=b$ (postulat III), E est un *groupe*. Alors, a et b étant quelconques dans le groupe E, axb parcourt E en même temps que x.

Au lieu de supposer E pourvu d'une loi de composition, on peut le supposer seulement contenu dans un ensemble F ayant cette propriété. Pour que E soit un groupe, il faut et il suffit alors que soient vérifiés, avec les postulats II et III, un postulat I', qui peut s'énoncer : si a, b, c, ab, bc, $(ab)c$, $a(bc)$ sont des éléments de E, alors $(ab)c=a(bc)$ [7].

Il suffit évidemment que ces conditions soient réalisées quand a parcourt seulement un système S d'éléments tels que tout élément de E soit un produit d'éléments de S : les éléments de S sont dits *générateurs* de E. Le nombre, fini ou non, des éléments de E est l'ordre du groupe E. Nous écrirons souvent un g_n pour un groupe d'ordre n.

Si S est formé de plusieurs systèmes S', S'', ..., on écrit

$$E=\{S'\ S''\ \ldots\}.$$

Plus généralement, si A, B, ... sont des systèmes quelconques

d'éléments de E, $\{A, B, \ldots\}$ désigne l'ensemble des produits d'éléments de A, B, ...

Considérons par exemple l'ensemble des $n!$ permutations de n symboles, désignés par $1, \ldots, n$; et prenons pour E l'ensemble des substitutions qui font passer de l'une quelconque de ces permutations à une autre. Il est clair que ces substitutions forment un groupe d'ordre $n!$ appelé *le symétrique de degré n*. On voit d'ailleurs aisément que chacune de ces substitutions est le produit d'un certain nombre de transpositions (échanges de deux symboles), qu'une transposition (xy) est le produit de trois transpositions $(1x)(1y)(1x)$, et, de proche en proche, que toute transposition $(1x)$ peut s'exprimer par un produit de transpositions du type $(h, h+1) = s_h$. Le symétrique de degré n dérive donc des s_h $(h = 1. \ldots, n-1)$.

Or, si l'on pose $s_1 = a$, $s_{n-1}s_{n-2}\ldots s_1 = b$, on a $s_{i+1} = b^{-i}ab^i$ $(i = 2. \ldots, n-2)$. Le symétrique dérive donc aussi de a et b.

On démontre aisément que, dans les divers produits de transpositions qui donnent une même substitution, le nombre de ces transpositions a toujours la même parité, qui définit la *parité* de la substitution [20, n° 38, p. 37]. Il est clair que toutes les substitutions paires sur n symboles forment un groupe d'ordre $n!/2$, appelé *l'alterné de degré n*.

L'alterné dérive, pour n impair, des substitutions circulaires (123), (145), ..., $(1, n-2, n-1)$, $(1, n-1, n)$; et, pour n *pair*, de (123), (145), ..., $(1, n-2, n-1)$, $(12n)$ [20, n° 70, p. 90]. Il dérive aussi des substitutions $c' = (132)$ et $s'_i = (12)(i+1, i+2)$ $(i = 1, \ldots. n-3)$, ou bien des substitutions $a' = s'_1$, $b' = (34\ldots n)$ ou $(12)(34\ldots n)$, suivant que n est impair ou pair, et c'.

Pour la généralisation obtenue en supprimant un des postulats II ou III (le corps étant supposé fini), voir [24].

3. Supposons que E soit un groupe. E contiendra un élément u tel que $ua = a$, d'où $uax = ax$ quel que soit x, et, ax parcourant E avec x, $ub = b$ quel que soit b. Il y a de même un élément u' vérifiant $cu' = c$ quel que soit c. En faisant $a = u'$ et $c = u$, on a $uu' = u = u'$. Pour tout élément v jouissant de la même propriété que u, on a $uv = u = v$. L'élément unique u est l'*unité* de E et se représente ordinairement par 1 (par 0 dans la notation additive). Si $ya = az = 1$, on déduit de $ax = ax'$ que $yax = yax'$, ou $x = x'$;

et de $xa = x'a$ que $xaz = z'az$, ou $x = x'$. Donc la solution dans E de $ax = b$ ou de $xa = b$ est unique.

Soit a^{-1} la solution de $ax = 1$. En multipliant à gauche par a^{-1}, on a $a^{-1}aa^{-1} = a^{-1}$, d'où $a^{-1}a = 1$. a^{-1} est l'*inverse* de a (en notation additive, on désigne cet inverse par $-a$). Par définition $a^{-n} = (a^{-1})^n$ et $a^0 = 1$.

On peut remplacer les postulats II et III par ceux-ci : E a un élément unité (postulat IV), et chaque élément de E a un inverse (postulat V). Car alors, de $ax = b$, on déduit d'abord $a^{-1}ax = a^{-1}b$, puis $x = a^{-1}b$; et, de $xa = b$, on déduit de même $x = ba^{-1}$.

Supposons, par exemple, que les éléments $x, y, \ldots$ de E soient des points de l'espace à r dimensions. Soient $x_1, \ldots, x_r$ les coordonnées de x, et $y_1, \ldots, y_r$ celles de y. Définissons le produit $z = xy$ par la condition que $z_i = \varphi_i(x_1, \ldots, x_r, y_1, \ldots, y_r)$ φ_i étant une fonction analytique des x_k et y_k; j'écrirai alors $z_i = \varphi_i(x, y)$, $z = \varphi(x, y)$. On peut considérer $z = \varphi(x, \eta)$ comme une transformation ponctuelle, de paramètres $\eta_1, \ldots, \eta_r$, amenant x en z. Les postulats II et III exigent que le système des équations $z_i = \varphi_i(x, y)$ soit résoluble en $x_1, \ldots, x_r$ et en $y_1, \ldots, y_r$. Si $z = abc$, $ab = \alpha$, $bc = \beta$, le postulat I donne la condition $z = \varphi(\alpha, c)$, $= \varphi(a, \beta)$, c'est-à-dire que la transformation résultant de l'application successive des transformations $\alpha = \varphi(a, b)$, $z = \varphi(\alpha, c)$ est la transformation $z = \varphi(a, \beta)$. L'étude de cette condition rentre donc dans celle plus générale, de la condition pour que des transformations invertibles

$$x'_i = f_i(x_1, \ldots, x_n, a_1, \ldots, a_r) = f_i(x, a)$$

à r paramètres de l'espace à n dimensions forment un groupe *quand on les compose en les appliquant successivement*, c'est-à-dire pour que l'élimination des x'_i entre les équations précédentes et $x''_i = f_i(x', b)$ fournisse un résultat de la forme $x''_i = f_i(x, c)$, c étant de la forme $\varphi(a, b)$, c'est-à-dire c_i de la forme $\varphi_i(a, b)$. On remarquera que la condition d'associativité, qui est vérifiée identiquement par trois transformations quelconques, impose aux φ_i, si les transformations f_i forment un groupe, la condition

$$\varphi[a, \varphi(b, c)] = \varphi[\varphi(a, b), c].$$

4. Si l'on remplace les postulats II et III par ceux-ci : $ax = b$ a au plus une solution dans E, en sorte que $ax = ax'$ entraîne $x = x'$ quel que soit a dans E, et de même pour $xa = b$, en sorte que $xa = x'a$ entraîne $x = x'$, nous dirons que E est un *semi-groupe*. Ainsi l'ensemble des entiers > 0, composés par la multiplication ordinaire, forme un semi-groupe. Si l'on joint 0, on n'a plus qu'un corps. D'après les postulats IV et V, un semi-groupe contenant l'inverse de chacun de ses éléments est un groupe.

Un semi-groupe fini E est toujours un groupe, car, x parcourant E, ax et xa parcourent chacun tous les éléments de E. Si un semi-groupe E contient 1 et une solution x de $ax = 1$, on en conclut, en multipliant à droite, puis en divisant à gauche par a, que $xa = 1$, et que x est l'inverse de a.

Si l'on remplace le postulat I par le double postulat

$$(ab) = (ac)(bc), \qquad c(ab) = (ca)(cb),$$

et si l'on conserve les postulats II, III, IV, V, on obtient ce que MM. Burstin et Mayer appellent un *groupe distributif* [4]. Par exemple, étant donné trois éléments a, b, c, ces postulats sont vérifiés par la loi de composition $a^2 = a$, $ab = ba = c$, $ac = ca = b$, $b^2 = b$, $bc = cb = a$, $c^2 = c$. Un groupe distributif n'a pas d'élément unité.

De nombreux exemples montrent que les postulats introduits ne sont pas contradictoires. Pour une étude logique des postulats, *voir* [18, p. 7], [20, p. 216-217] et [5].

5. Soient a, b, ... des éléments d'un groupe E. $b^{-1}ab$ est dit le *transformé* de a par b. Soit $b^{-1}ab = ac$, d'où $ab = bac$ et $ba = abc$ [1]; c et c^{-1} sont les deux *commutateurs* de a et b. Si $ba = ab$, on a $c = c^{-1} = 1$. Les éléments a et b sont alors dits *permutables*. Si les éléments sont tous permutables deux à deux, E est dit *commutatif* ou *abélien*.

Considérons un certain nombre d'éléments a, b, ... d'un groupe E, les commutateurs de ces éléments, les commutateurs de ces commutateurs, et ainsi de suite. Disons que, dans l'ensemble ainsi formé, les éléments a, b, ... sont des *commutateurs complexes de poids* 1, et que le commutateur de deux éléments de poids m_1 et m_2 est un *commutateur complexe de poids* $m_1 + m_2$ relativement aux éléments a,

$b, \ldots$. Soient a et b deux éléments quelconques d'un groupe E. Considérons tous les commutateurs complexes relatifs à ces deux éléments; rangeons-les par ordre de poids croissant, ceux d'un même poids étant dans un ordre arbitraire. Soit $c_1, c_2, \ldots$ la suite ainsi formée, m_i étant le poids des c_i. *Alors* [7, p. 63] *on peut former une fois pour toutes une suite correspondante de polynomes* $f_i(x)$ *à coefficients entiers, s'annulant avec* x $[f_1(x) = f_2(x) = x]$ *de degrés* $\mu_i \leqq m_i$ et tels que l'on ait identiquement, *quels que soient les éléments* a *et* b, *et l'entier* x,

$$(ab)^x = c_1^{f_1(x)} c_2^{f_2(x)} \ldots .$$

6. Si a^m est la première puissance de a qui soit égale à 1, m est l'*ordre* de a. C'est aussi celui de a^{-1}. Nous écrirons e_m pour *élément d'ordre* m, et $e_{(m)}$ pour *élément dont l'ordre divise* m. Si m est fini, les éléments $1, a, \ldots, a^{m-1}$ forment évidemment un groupe $\{a\}$ abélien (l'égalité $a^h a^k = a^k a^h$ résulte de l'associativité) d'ordre m, qui est dit *cyclique*. Si m est infini, les éléments $1, a, a^2, \ldots$ ne forment qu'un semi-groupe; mais, en leur adjoignant $a^{-1}, a^{-2}, \ldots$, on a un groupe cyclique infini $\{a, a^{-1}\}$. Les entiers $0, \pm 1, \pm 2$, composés par l'addition. forment un groupe de cette sorte.

Si a est d'ordre fini $m = \alpha\beta$, α étant premier à β, on a, en désignant par x, y une solution de $\alpha x + \beta y = 1$, et en posant $a^{\alpha x} = u$, $a^{\beta y} = v$ (u, v ne dépendent pas de la solution x, y choisie). $a = uv = vu$. Inversement, si $a = uv = vu$, u et v étant d'ordres respectifs β et α, on a $a^{\alpha x} = u^{\alpha x} = u^{1-\beta y} = u$, et de même $a^{\beta y} = v$. L'extension au cas de plusieurs facteurs permutables est immédiate.

7. L'ensemble des relations telles que $ab = c$ constitue la table de multiplication du groupe E. On peut évidemment considérer les éléments de E comme formant un système de générateurs. Toutes les relations qui lient les éléments de E résultent de la table de multiplication. Soient, en général, $\alpha_1, \alpha_2, \ldots$ un système de générateurs, et A un système d'équations entre les α tels que toutes les relations liant les α résultent de A. On dit que A est *un système d'équations de* E.

Si E est le symétrique de degré n engendré (2) par les transpositions $\alpha_h = (h, h+1)$ $(h = 1, \ldots, n-1)$, un système A d'équations

de E est [20, n° 69, p. 89]

$$\alpha_h^2 = (\alpha_i \alpha_{i+1})^3 = (\alpha_j \alpha_{j+k})^2 = 1$$

$(h = 1, \ldots, n-1;\quad i = 1, \ldots, n-1;\quad j = 1, \ldots, n-3;\quad k = 2, \ldots, n-j-1).$

Soit B un système d'équations de E avec d'autres générateurs β_1, β_2, ...; A et B sont dits *équivalents* en ce sens que A résulte de B et B de A par un changement de générateurs : pour préciser, si A_β désigne les expressions des α par les β, et B_α celles des β par les α, B résulte de A et de B_α, et A résulte de B et de A_β.

Par exemple le symétrique de degré n est aussi engendré par $\beta_1 = \alpha_1$, et $\beta_2 = \alpha_{n-1}\alpha_{n-2}\ldots\alpha_1$ (2). Un système B, équivalent à A, d'équations du symétrique [20, ibid.] est alors, en écrivant a pour β_1 et b pour β_2,

$$b^n = a^2 = (ba)^{n-1} = (ab^{-1}ab)^3 = (ab^{-j}ab^j)^2 = 1;$$

$j = 2, 3, \ldots, n/2$ si n est pair; $j = 2, \ldots, (n-1)/2$ si n est impair > 3.

On peut remarquer que l'équation $(ab^{-1}ab)^3 = 1$ est une conséquence des autres. Posons en effet $(ab^{-1}ab)^3 = c$, et écrivons l'équation $(ba)^{n-1} = 1$ sous la forme $(ab^{-1})^{n-1} = 1$, ou en remplaçant b^{-1} par $b^h b^{-h-1}$ $(h = 1, \ldots, n-2)$,

$$ab^{-1}abb^{-2}ab^2b^{-3}ab^3\ldots b^{2-n}ab^{n-2}b = 1.$$

En remplaçant alors $ab^{-1}ab$ par $cb^{-1}abab^{-1}aba$, et $b^{-h}ab^h$ par $ab^{-h}ab^ha$, en vertu des équations $(ab^{-j}ab^j)^2 = 1$ transformées par ab^{-j}, cette équation devient

$$cb^{-1}abab^{-1}abaab^{-2}ab^2a\ldots ab^{2-n}ab^{n-2}ab = 1,$$

ou

$$cb^{-1}ab(ab^{-1})^{n-2}ab^{-2}ab = 1;$$

or,

$$(ab^{-1})^{n-2} = ba;$$

il reste donc $c = 1$. (*Cf.* [19] et [11].)

On peut donner aussi, pour l'alterné, deux systèmes d'équations [20, n° 70]. Avec les générateurs c', $\alpha'_i = s'_i$ (2), on a

$$c'^3 = (c'\alpha'_1)^3 = \alpha_i'^2 = (c'\alpha'_h)^2 = (\alpha'_j\alpha'_{j+1})^3 = (\alpha'_i\alpha'_{i+k})^2 = 1$$

$(i = 1, \ldots, n-3;\quad j = 1, \ldots, n-4;\quad k = 2, \ldots, n-i-3;\quad h = 2, \ldots, n-3).$

Il faut supprimer, si $n = 4$, les trois derniers systèmes; et, si $n = 5$, le dernier seulement.

Avec les générateurs a', b', c', on a

$$b'^{n-1} = c'^{3} = a'^{2} = (b'a')^{n-3} = (a'c')^{3} = (a'b'^{-1}a'b')^{3}$$
$$= (c'b'^{-k}a'b'^{k})^{2} = (a'b'^{-j}a'b'^{j})^{2} = 1,$$

$j = 2 \ldots\ldots \left[\frac{n-2}{2}\right]$; $k = 1, \ldots\ldots n-4$. Si $n = 4$, il faut supprimer la 6ème équation et les deux derniers systèmes; et, si $n = 5$, le dernier système seulement.

Il importe d'observer qu'un système absolument quelconque d'équations entre les éléments regardés comme générateurs n'est jamais incompatible. Ces équations sont analogues aux équations homogènes (la notation additive le met mieux en évidence) : on n'en déduira jamais que l'identité de certains éléments, et la seule proposition qu'elles pourraient contredire est celle que ces éléments sont distincts. Mais elles ne définissent un groupe (le calcul des générateurs étant supposé associatif) que si elles définissent l'inverse de chaque générateur.

8. Si B se déduit de A en remplaçant α_1, α_2, ... par β_1, β_2, ..., la correspondance ainsi obtenue de E à lui-même s'appelle un *automorphisme* de E. Ainsi, on obtient un automorphisme du groupe cyclique $\{a\}$ d'ordre fini n en remplaçant a par a^h, h étant premier à n. Si un groupe E′ admet des générateurs α'_1, α'_2, ... vérifiant les mêmes équations que α_1, α_2, ..., E et E′ sont dits *isomorphes*. Un automorphisme de E est donc un isomorphisme de E avec lui-même.

Un élément x sera dit indépendant d'un système S d'éléments de E si x n'est pas dans $\{S\}$. Les éléments de S seront dits indépendants (entre eux) si chacun est indépendant du système des autres. Un élément x sera dit *absolument indépendant* d'un système S d'éléments, si aucune puissance de x n'est dans $\{S\}$. Les éléments de S seront dits absolument indépendants entre eux si chacun est absolument indépendant du système des autres. Un système de générateurs absolument indépendants sera dit une *base*. Les générateurs eux-mêmes seront dits *basiques*, et leurs ordres des ordres basiques.

Une base composée du plus petit nombre possible de générateurs sera dite *minima;* le nombre des générateurs d'une base minima

sera dit le *rang* du groupe. Il peut arriver qu'un groupe G admette une base $a_1, \ldots, a_m$ telle que tout élément de G ait une expression et une seule de la forme $a_1^{x_1} a_2^{x_2} \ldots a_m^{x_m}$. Une telle base sera dite *monogène*.

Considérons par exemple le groupe abélien G engendré par n générateurs a_i indépendants d'ordre premier p (ils sont donc absolument indépendants). Les équations sont $a_i^p = 1$, $a_i a_k = a_k a_i$. Les p^n formes possibles $a_1^{x_1} \ldots a_n^{x_n}$ $(x_i = 1, \ldots, p)$ pour les éléments de G sont distinctes. Donc l'ordre de G est p^n. Un groupe de cette forme sera dit *abélien principal*.

9. *Soit* G *un groupe de générateurs* $a_1, a_2, \ldots$ (1), *et* S *un système d'équations de la forme* $F_1 = 1, F_2 = 1, \ldots$ (*où peuvent figurer les* a_i^{-1}) *définissant* G. *Chacune des conséquences de* S *peut, par des transformations identiques* (*c'est-à-dire ne supposant aucune équation autre que* $a_i a_i^{-1} = a_i^{-1} a_i = 1$ *entre des produits formellement distincts*), *être mises sous la forme typique*

$$V^{-1} F^{\pm 1} V = 1,$$

F *parcourant un système de* F_i, *où le même peut revenir plusieurs fois*, V *parcourant, indépendamment de* F, *des produits quelconques des* a_i *et des* a_i^{-1}, *et* V *étant écrit de manière que* $V^{-1} V = 1$ *identiquement*. On le démontre en observant qu'on ne peut déduire une conséquence d'un système d'équations que par la répétition de deux opérations : multiplier les deux membres par un même facteur; substituer à un produit d'éléments un autre produit égal (soit identiquement, soit en vertu du système).

10. Soit G un groupe de générateurs $a_1, a_1^{-1}, a_2, a_2^{-1}, \ldots$. Lorsque le système S est équivalent au système des seules équations $a_i a_i^{-1} = a_i^{-1} a_i = 1$, le groupe est dit *libre*. On démontre alors que tout groupe H ayant pour générateurs des produits $b_1, b_2, \ldots$ des générateurs de G est aussi un groupe libre [9]. Le nombre des b peut être infini, même si celui des a est fini; on le voit en prenant,

(1) Le lecteur suppléera à l'insuffisance de la notation quand l'ensemble des générateurs n'est pas dénombrable. Cette observation suffira sans doute pour les cas analogues qui se présenteront dans la suite.

par exemple, $b_i = a_1^i a_2 a_1^i$. On voit, en prenant un nombre quelconque de ces b_i, que l'on peut obtenir un groupe K, contenu dans G, ayant un nombre quelconque de générateurs.

Il est clair que deux groupes libres ayant le même nombre de générateurs sont isomorphes.

Supposons qu'aux équations d'un groupe libre, de générateurs $a_1, \ldots, a_n$, on ajoute une équation $F = 1$, où figure a_n. Considérons toutes les équations déduites de $F = 1$ par permutations circulaires des symboles de F. Elles sont toutes équivalentes, chacune étant la transformée de la précédente par le premier symbole de celle-ci. Pour que l'équation $F = 1$ ait une conséquence $f = 1$ entre $a_1, \ldots, a_{n-1}$, il faut et il suffit que l'une de ces équations ne contienne pas a_n, et alors F a identiquement la forme $T^{-1} f T$, T contenant a_n. Inversement, si F peut s'écrire ainsi, il est clair que, par une permutation circulaire des éléments de F, on obtiendra f [10]. Deux équations $F_1 = 1$, $F_2 = 1$ sont dites équivalentes quand chacune est équivalente à l'autre. Alors chacune est la transformée de l'autre [10].

11. Soit A un groupe de générateurs $a_1, a_2, \ldots$ (quelques-uns des a_i pouvant être les inverses d'autres a_i), et désignons d'une manière générale par $X(a_i) = X(a)$ des produits des a. Soient

$$A_i(a) = 1 \qquad (i = 1, 2, \ldots)$$

les équations de A. Soit, avec des notations analogues, B un groupe de générateurs $b_1, b_2, \ldots$, défini par $B_j(b) = 1$ $(j = 1, 2, \ldots)$. Considérons le système S des équations

$$(1) \quad A_i(a) = 1, \quad B_j(b) = A'_j(a) \quad b_k^{-1} a_l b_k = A_l^{b_k}(a) \quad (i, j, k, l = 1, 2, \ldots).$$

S définit un groupe G. Désignons par S_a le système des équations de S où ne figurent que les a, par $S_{a=1}$ ce que devient S quand on y remplace les a_i par 1 (S_a défini A et $S_{a=1}$ définit B).

Si $S_{a=1}$ résulte de S, G contient B (toute conséquence de S entre les seuls b résulte de $S_{a=1}$, comme le montre sa forme typique en y remplaçant les a par 1).

S_a résulte toujours de S. Mais, pour que G contienne A, il faut et il suffit que S n'établisse pas entre les a d'autres relations que S_a. Pour cela, deux conditions sont évidemment nécessaires :

1° D'après la dernière équation (1), on doit obtenir un automorphisme de A en remplaçant a_l par $A_l^{b_\lambda}(a)$. J'appellerai condition ou conditions d'*automorphisme* l'ensemble des conditions que les différents automorphismes de cette sorte imposent à S.

2° En posant $A_l^{b_\lambda}(A_i^{b_m}) = A_l^{b_\lambda b_m}$, et, plus généralement,

$$A_l^{\beta(b)}\left[A_i^{\gamma(b)}\right] = A_l^{\beta(b)\gamma(b)},$$

il faut que, dans A, on ait $A_j'^{-1} a_l A_j' = A_{l'}^{\beta_j}$. Cette condition sera dite de *fermeture*.

Soit maintenant S' le système formé de S_a et des $b_\lambda^{-1} A_l b_\lambda = A_l^{b_\lambda}$.

Si les A_j' se réduisent à 1, les conditions d'automorphisme et de fermeture suffisent pour que toutes les conséquences de S entre les a résultent de S'; et alors G contient A[18, 19].

Si B est cyclique et fini, les $B_j = A_j'$ se réduisent à une équation de la forme $b_1'' = A_1'$, et S donne $b_1^{-1} A_1' b_1 = A_1'$. Donc $A_1'(A_1^{b_1}) = A_1'$ doit résulter de S_a. J'appellerai cette nouvelle condition *condition de permutabilité*. Si elle est vérifiée, toute conséquence de S entre les a résulte encore de S', et G contient encore A.

Prenons par exemple pour A le g_n cyclique C_n défini par $a^n = 1$, et pour B un g_2. Les conditions précédentes fournissent entre autres le g_{2n} diédral D_n défini par $a^n = b^2 = 1$, $b^{-1} ab = a^{-1}$, et, pour $n = 2\nu$, le g_{4n} Δ_n défini par $a^n = 1$, $b^2 = a^\nu$, $b^{-1} ab = a^{-1}$. Ce dernier, qui se présente souvent, sera appelé *dicyclique*. D_2 est un g_4 abélien principal que j'appellerai le *groupe carré*. Δ_1 est un g_8 nommé groupe des *quaternions*. Les unités complexes des quaternions d'Hamilton engendrent un groupe isomorphe à Δ_1.

En prenant pour A le g_4 D_2 et pour B un g_3, on obtient entre autres le g_{12} *tétraédral* **T** défini par les équations de D_2 jointes à $c^3 = 1$, $c^{-1} ac = b$, $c^{-1} bc = ab$. En prenant pour A le g_{12} **T** et pour B un g_2, on obtient entre autres le g_{24} *octaédral* **O** défini par les équations de **T** jointes à $d^2 = 1$, $d^{-1} ad = a$, $d^{-1} b d = ab$, $d^{-1} c d = c^2$ (1).

(1) Les noms des groupes $\mathbf{D}_n$, **T**, **O** viennent de leur représentation géométrique par des groupes de rotations conservant respectivement un polygone régulier, un tétraèdre, un octaèdre. Comme il y a toujours deux rotations qui superposent une arête d'un polyèdre régulier P à elle même, il est clair que, si P a n arêtes, le groupe des rotations conservant P est un g_{2n}.

CHAPITRE II.

DIVISEURS.

12. Lorsqu'il est question de composer les éléments de plusieurs corps, on suppose tacitement que ces corps sont contenus dans un corps unique.

Soient A, B, C, D, ... des parties ou complexes d'un corps G. $A+B$ désignera l'ensemble des éléments contenus dans A et B (la notation est supposée multiplicative). $A=B$ signifie que A et B sont composés des mêmes éléments distincts. $A<B$, que B contient tous les éléments de A, qui peut se réduire à un seul élément, et d'autres encore. Le *produit formel* $A\times B$ sera l'ensemble des éléments, distincts ou non, obtenus en multipliant chaque élément de A à droite par un élément de B. Le *produit* AB de A par B se déduit de $A\times B$ en ne prenant que les éléments distincts.

Si $\mathfrak{A}$ est le système des parties $A_1, A_2, \ldots$, c'est-à-dire l'ensemble $\Sigma(A_i)$, dont les éléments sont les A_i et non les éléments des A_i, et si de même $\mathfrak{B}=\Sigma(B_i)$, $\mathfrak{A}\mathfrak{B}=\Sigma(A_iB_k)$. Si $\mathfrak{A}\mathfrak{B}=\mathfrak{B}\mathfrak{A}$, $\mathfrak{A}$ et $\mathfrak{B}$ sont dits *permutables*.

Des complexes n'ayant aucun élément $\neq 1$ commun à tous seront dits *premiers entre eux*. Un complexe jouissant d'une certaine propriété sera dit *maximum* parmi les complexes qui en jouissent s'il n'est contenu dans aucun d'eux, sauf G, *minimum* s'il n'en contient aucun $\neq 1$.

Soit $H=\Sigma x$ un groupe quelconque (x parcourant les éléments de H). $x^{-1}Ax$ sera dit *conjugué de* A *par* H (ou par x), et *semblable* à A. Supposons les x permutables à G. Alors, deux quelconques des $x^{-1}Ax$ sont conjugués entre eux. L'ensemble des $x^{-1}Ax$ est le *système complet* ou *la classe des conjugués* de A par H, et l'on peut décomposer G en classes d'éléments conjugués par H. [Si A et B sont permutables, $x^{-1}Ax$ et $x^{-1}Bx$ le sont aussi, et $(x^{-1}Ax)''=x^{-1}A''x$].

Soit maintenant $H=G$. On dit alors simplement que les $x^{-1}Ax$ sont conjugués. Si $x^{-1}Ax$, $x^{-1}Bx$, ... reproduisent, à l'ordre près, A, B, ..., on dit que le système A, B, ... est *invariant* ou *normal* dans G.

13. Un complexe d'éléments de G qui constitue un groupe est un *sous-groupe* ou *diviseur* de G. Ainsi l'ensemble des éléments normaux de G est un diviseur normal qui sera dit *central* de G. Il est clair que $x^{-1}Ax$ est un groupe en même temps que A. Un groupe qui ne contient d'autre diviseur normal que lui-même et 1 est dit *simple*. (On ne connaît pas de groupe simple non cyclique d'ordre impair.) Sinon, il est *composé*. On nomme *hamiltoniens* les groupes qui, comme le g_8 des quaternions, n'ont que des diviseurs normaux.

Si A est une partie de groupe, on a $A^2 \leqq A$, A est un semi-groupe, et inversement.

Si $A^2 \leqq A$, et si A contient l'inverse de chacun de ses éléments, A est un groupe. Car, si a, b, x sont trois de ces éléments, $ax = b$ a la solution $x = a^{-1}b$, et $xa = b$ a la solution $x = ba^{-1}$. Ainsi, A et B étant deux groupes, si $(AB)^2 \leqq AB$, AB est un groupe, car, a et b étant deux éléments de A et B respectivement, $b^{-1}a^{-1}$ est dans A(BA)B. De même si $BA \leqq AB$, AB est un groupe et réciproquement.

Si un groupe C est le produit AB de deux groupes A et B il est dit *décomposable;* A et B sont ses *composants*. Si $A_1, \ldots A_n$ sont des groupes dont chacun est premier avec le produit des autres, et si chaque élément de A_i est permutable à chaque élément de A_k $(i, k = 1, \ldots, n; i \neq k)$, le groupe ΠA_i est le *produit direct* des A_i, et les A_i sont ses *facteurs directs*. Ainsi le g_{p^2} abélien (p premier) défini par $a^p = b^p = 1$, $ab = ba$ est le produit direct de deux quelconques des trois groupes $\{a\}$, $\{b\}$, $\{ab\}$, mais non des trois.

Si G est le produit direct de deux groupes A et B, on dit encore que A (ou B) se *sépare* de G.

L'ensemble des éléments communs à plusieurs groupes A, B, ..., qui est évidemment un groupe, est le p. g. c. d. H de A, B, ... Si le système A, B, ... est normal dans le groupe G, H est aussi normal dans G. Si B, C, ... sont normaux dans G, H est normal dans A.

A, B, ... étant ou non des groupes, l'ensemble $M = \{A, B, \ldots\}$, déjà défini, est dit *dérivé* de A, B, ..., ou *p. p. c. m.* de A, B, ..., ou de leurs éléments. Si A, B, ... forment un système normal dans le groupe G, M est évidemment normal dans G.

Le p. p. c. m. des commutateurs d'un groupe G est un groupe K normal dans G. K est le *groupe des commutateurs*, ou le *commutant*, ou le *dérivé* de G, ou, plus précisément, le premier commutant, le premier dérivé, le second étant le dérivé du premier, le troisième

le dérivé du deuxième, et ainsi de suite. Un groupe qui coïncide avec son dérivé est dit parfait.

Décomposition suivant un module. Homomorphisme.

14. Soient $A = \Sigma a$, $B = \Sigma b$ deux diviseurs, distincts ou non, de $G = \Sigma x = \Sigma y$. Deux complexes $Ax B$, $Ay B$ n'ont aucun élément commun à moins de coïncider. S'ils coïncident, on dit que x et y sont *équivalents* ou *congrus* selon les modules A, B, et l'on écrit $x \equiv y \pmod{A, B}$. S'ils sont distincts, $Bx^{-1}A$ et $By^{-1}A$ le sont aussi. Si $G = \Sigma A x B$ représente la décomposition de G en complexes *distincts* $Ax B$, la décomposition $G = \Sigma B x^{-1} A$ fournira le même nombre de complexes. On dit que $\Sigma A x B$ est la décomposition de G (mod A, B), que les $Ax B$ sont les complexes relatifs à A, B et que x ou y parcourt un *système* de restes (mod A, B). Quand l'un des deux modules est 1, et qu'il n'y a pas danger de confusion, on le sous-entend.

Soit $B = 1$, donc,

$$G = \Sigma A x = A \Sigma x = \Sigma x^{-1} A = (\Sigma x^{-1}) A.$$

Chaque Ax (ou $x^{-1}A$) contient autant d'éléments que A. A est le seul Ax qui soit un groupe (1). Le nombre des Ax, ou des $x^{-1}A$ se nomme, du moins quand G est dénombrable, l'*indice* de A dans G, et se désigne par (G, A). *Si* $(G, A) = 2$, A *est normal dans* G. On a $(G, A) \times (A, 1) = (G, 1)$.

Si G est un groupe continu de points $(x_1, \ldots, x_n)$, je supposerai que chaque Ax est, dans G, une variété à p dimensions, et que ces variétés forment un faisceau à $n - p$ paramètres. Dans ce cas, on est amené à entendre par (G, A) et à appeler indice de A dans G le nombre $n - p$. On a alors $(G, A) + (A, 1) = (G, 1)$.

Voici deux applications de l'importante relation $(G, 1)(A, 1) = (G, 1)$. *Tout* g_{p^a} (p *premier*) *ayant un élément d'ordre* $> p^{a-1}$ *est cyclique*. Les conjugués d'un g_a A divisant le g_N G contenant au plus $N(a - 1)/a$ éléments n'épuisent jamais tous les éléments de G. *Si* G *est le produit direct des groupes* A, B, ... *d'ordres premiers*

(1) Si $b_i = a_i x$ parcourt les éléments de A_x, $b_h b_k^{-1} b_i = a_h a_k^{-1} a_j x$ est aussi dans Ax (2).

entre eux deux à deux, tout diviseur G′ *de* G *est produit direct de ses p. g. c. d.* A′, B′, ..., *avec* A, B, ... *respectivement.*

15. *L'ensemble* B *des éléments d'un groupe* G *qui sont permutables à* $\mathfrak{A} = \Sigma A_\iota$ (les parties A_ι étant contenues ou non dans G) *est un groupe.* Cette sorte de groupe se présentant souvent, il sera commode d'appeler B le *normalisant* de $\mathfrak{A}$ dans G. *L'ensemble* B_0 *des éléments de* B *permutables à chacun des* A (c'est-à-dire, le p. g. c. d. des normalisants des A_i dans B) *est normal dans* B. Si x parcourt un système de restes de G mod B, les conjugués de $\mathfrak{A}$ dans G sont les $x^{-1}\mathfrak{A}x$, au nombre de (G, B).

Voici quelques applications. *Tout diviseur normal d'un* g_{p^m} (*p premier*) B *contient des éléments* $\neq 1$ *normaux dans* B.

Si A *est une partie de* G, *et si les conjuguées de* A *sont encore conjuguées dans leur p. p. c. m.* M, *on a* G = MB.

Un diviseur A *du groupe fini* G *ne peut, s'il est* < G, *contenir des éléments dans toutes les classes d'éléments de* G.

Si un élément e est permutable au groupe fini G *et à une classe d'éléments de* G, *il est permutable à un élément de* G.

16. Si A est normal dans $G = \Sigma Ax$, les Ax sont les éléments d'un groupe qu'on désigne par $G \mid A$, ou $\frac{G}{A}$, ou G:A. On dit que $G \mid A$ est le *complémentaire* ou *réciproque* de A, qu'il est le *quotient* de G par A, ou groupe *facteur* de G (relatif à A), et que G est *composé* de $G \mid A$ et de A. Si A est le commutant de $G = Ax + Ay + \ldots$, $G \mid A$ est abélien (car $AxAy = Axy = Ayxy^{-1}x^{-1}xy = Ayx$). Inversement, si $G \mid B$ est abélien, B contient le commutant de G. Si donc G est parfait, aucun groupe facteur de G n'est abélien.

A chaque élément x de G faisons correspondre le complexe Ax qui le contient. Au produit de deux éléments x, y de G répondra le complexe Axy. Alors à chaque diviseur de $G \mid A$ répond, dans G, un diviseur B contenant A. Si $B = \Sigma Az$ est normal dans $G = \Sigma By = \Sigma Ax$, $B \mid A$ est normal dans $G \mid A$ et réciproquement, car $Ax^{-1}AzAx = Ax^{-1}zx$. Comme $G \mid A = \Sigma(Azy) = \Sigma(Ax)(Ay) = \Sigma(By)$, on a

$$G \mid A : B \mid A = G \mid B.$$

Si A′ est normal dans G′, et si GG′ est le produit direct de G et G′,

on a

$$G \mid A . G' \mid A' = GG' \mid AA'.$$

Si C est le commutant de G, celui de $G \mid A$ est $AC \mid A$.

17. Inversement, et plus généralement, supposons entre les groupes A et B une correspondance telle qu'à chaque élément de A réponde au moins un élément de B, et à chaque élément de B au moins un élément de A, et que, si a_ι de A et b_ι de B se correspondent, $a_\iota a_k$ et $b_\iota b_k$ se correspondent aussi. On dit que A et B sont *homomorphes*. Alors les complexes A_0, B_0 répondant aux unités de B et de A respectivement sont des semi-groupes, car, si $b_{0\iota}$ et b_{0k} sont dans B_0, $b_{0\iota} b_{0k}$ répond à 1 de A, donc sera aussi dans B_0; d'où $B_0^2 \leqq B_0$.

Si maintenant b et b_ι sont deux éléments de B répondant respectivement à a_ι^{-1} et à a_ι, bb_ι et $b_\iota b$ sont dans B_0. donc b dans $B_0 b_\iota^{-1}$ et dans $b_\iota^{-1} B_0$. Mais les éléments de $B_0 b_\iota^{-1} (\geqq B_0 b)$ ou de $b_\iota^{-1} B_0 (\geqq b B_0)$ ne répondent pas tous à a_ι^{-1} (comme on le voit pour $A = \{a, a^{-1}\}$, $B = \{b, b^{-1}\}$, $B_0 = b^h \{b\}$, $A_0 = a^{-h} \{a\}$; $b^\iota B^0$ répond à a^ι, donc $a^i A_0$ à b^ι). D'ailleurs, à $a_\iota^{-1} a_\iota = 1$ répondent toujours tous les éléments de $b B_0 b_\iota$, d'où $b B_0 b_\iota \leqq B_0$. *Si donc, quel que soit le couple* a_i, b_ι *d'éléments correspondants,* b_ι^{-1} *répond à* a_i^{-1} (*cela a toujours lieu si* B_0 *est un groupe, donc si* B_0 *est fini*), on a

$$b_\iota^{-1} B_0 b_\iota \leqq B_0, \qquad \text{et} \qquad b_\iota B_0 b_\iota^{-1} \leqq B_0, \qquad \text{d'où} \quad b_\iota^{-1} B_0 b_\iota = B_0,$$

et B_0 est normal dans B. *Si* B_0 *est un groupe*, tout élément de $B_0 b_i^{-1}$ répond à a_ι^{-1}; en prenant a_ι dans A_0, on peut faire $b_\iota = 1$; donc a_ι^{-1} répond alors à tout élément de B_0, et en particulier à 1; donc a_ι^{-1} est dans A_0, et A_0 est un groupe [18, p. 66; 20, p. 219]. Je supposerai désormais que A_0 et B_0 sont des groupes. Si alors b_ι et b'_ι sont deux éléments de B répondant à un élément a_ι de A, $b_\iota^{-1} b'_i$ répondra à $a_\iota^{-1} a_\iota = 1$, et sera dans B_0. Donc les éléments de B répondant à a_ι sont ceux de $B_0 b_\iota$, et ceux de A repondant à a_ι sont ceux de $A_0 a_i$. Donc $\Sigma(A_0 a_\iota)$ et $\Sigma(B_0 b_\iota)$ se correspondent biunivoquement. Si A_0 et B_0 sont > 1, A et B sont dits *fractionnairement homomorphes*. Si $B_0 = 1$, A est *multiplement homomorphe* à B, et B *partiellement ou mériédriquement* homomorphe à A. Si $A_0 = B_0 = 1$, A est dit *isomorphe* à B, (8), et nous écrirons $A \equiv B$. Ainsi $A \mid A_0 \equiv B \mid B_0$. Si, par exemple, $B = \Sigma B_0 b_\iota$ divise $A = \Sigma A_0 a_\iota$ et si B_0 est le p. g. c. d. de B

et A_0, les b_i sont incongrus mod A_0 (car $b_i b_i^{-1}$ ne peut être dans A_0 sans être dans B_0) et $A = \Sigma A_0 a_i = A_0 B$.

Si A_1 *est normal dans* A *et si* B_1 *lui correspond dans* B, B_1 *contient évidemment* B_0 *et est normal dans* B. *Si, de plus,* A_1 *est normal maximum dans* A, *et si* B_1 *est* $< B$, A_1 *contient* A_0 (*supposé* > 1). Sans quoi, $A_1 A_0$ correspondant évidemment à B_1, on aurait

$$A_1 A_0 \mid A_0 \equiv B_1 \mid B_0 < B \mid B_0 \equiv A \mid A_0, \qquad \text{d'où} \qquad A_1 A_0 < A,$$

et A_1 ne serait pas normal maximum.

18. Soit G un diviseur du produit direct $\mathfrak{P}$ des groupes $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$. Chaque élément g de G est de la forme $a_1 \ldots a_n$, a_i étant dans $\mathfrak{A}_i$; nous dirons que a_i *est le constituant de* g dans $\mathfrak{A}_i$, et que $a_1, \ldots, a_n$ se correspondent. Pour un i déterminé, les a_i figurant dans les éléments g de G forment évidemment un groupe A_i qui est dit le *constituant* de G dans $\mathfrak{A}_i$.

Pour $n = 2$, la correspondance de a_1 à a_2 pour chaque g établit un homomorphisme entre A_1 et A_2. Posons $\mathfrak{A}_1 = \mathfrak{A}$, $\mathfrak{A}_2 = \mathfrak{B}$, $A_1 = A$, $A_2 = B$. A l'unité de A répond le p. g. c. d. B_0 de G, B, et les éléments de B qui répondent à a de A forment le complexe bB_0, b étant l'un d'eux. Donc $A \equiv G \mid B_0$, et de même $B \equiv G \mid A_0$, A_0 étant le p. g. c. d. de G, A. De plus, $A \mid A_0 \equiv B \mid B_0 \equiv G \mid A_0 B_0$. Soit $A = \Sigma A_0 a$, $B = \Sigma B_0 b$, $A_0 a$ correspondant à $B_0 b$ dans l'isomorphisme de $A \mid A_0$ à $B \mid B_0$. On aura

$$G = A_0 B_0 \Sigma ab \qquad \text{et} \qquad AB = \Sigma Ga = \Sigma Gb.$$

Si $A_0 = B_0 = 1$, $G = \Sigma ab$ est dit l'*assemblage* de ses constituants A et B. De même, pour $n > 2$, si G est premier à $A_1, A_2, \ldots, A_n$, il sera dit l'*assemblage* de $A_1, \ldots, A_n$.

Pour que G soit normal dans $\mathfrak{A}\mathfrak{B}$, il faut et il suffit que A_0 soit normal dans $\mathfrak{A}$ et B_0 dans $\mathfrak{B}$, et que $A \mid A_0$ divise le central de $\mathfrak{A} \mid A_0$ et $B \mid B_0$ celui de $\mathfrak{B} \mid B_0$. Si alors $\mathfrak{A} = A$ et $\mathfrak{B} = B$, on a $AB \mid G \equiv A \mid A_0 \equiv B \mid B_0$.

On peut d'ailleurs considérer tout groupe comme diviseur d'un produit direct [16]. Mais ce n'est là qu'une expression différente de la représentation de G en groupe intransitif, qui sera exposée dans un autre fascicule.

19. Nous appellerons *minimal* un diviseur normal minimum de G. Le produit de tous les minimaux de G est évidemment un diviseur normal, que nous appellerons le p. m. de G. Deux minimaux isomorphes $A = \Sigma a_\iota$, $B = \Sigma b_\iota$ (a_ι et b_ι se correspondant dans un isomorphisme de A à B) seront dits *assemblables dans* G, si G transforme entre eux tous les produits $a_\iota b_\iota$. Deux minimaux distincts ne peuvent être assemblables dans G que s'ils sont abéliens. Le produit des diviseurs normaux assemblables à l'un d'entre eux dans G (donc deux à deux assemblables dans G) est évidemment un diviseur normal du p. m., que j'appellerai un p. m. a. de G. Un p. m. a. peut être mis, en général de plusieurs manières, sous forme d'un produit direct de minimaux. Tout minimal de ce p. m. a. est l'assemblage (18) de quelques-uns de ces facteurs directs [15].

20. Soit $\mathfrak{T}_0$ le central de $\mathfrak{T}$ (18). $\mathfrak{T}_0$ est évidemment le produit des centraux de $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$. Deux diviseurs G, G' de P sont dits *centralement isomorphes* dans $\mathfrak{T}$ quand on peut établir entre eux une correspondance isomorphique où l'élément a' de G' qui répond à l'élément a de G est $\equiv a \mod \mathfrak{T}_0$ (alors $\mathfrak{T}_0 G = \mathfrak{T}_0 G'$). Une telle correspondance effectivement établie sera dite *correspondance centrale* de G à G' dans $\mathfrak{T}$ [26].

Soit $\mathfrak{T}'$, produit direct de $\mathfrak{A}'_1, \ldots, \mathfrak{A}'_{n'}$ un groupe centralement isomorphe à $\mathfrak{T}$ dans le produit direct de $\mathfrak{T}$ par un groupe abélien quelconque K ($\mathfrak{T}K = \mathfrak{T}'K$). Si les $\mathfrak{A}_\iota$ et les $\mathfrak{A}'_\iota$ ne sont plus eux-mêmes des produits directs, on a $n' = n$, et l'on peut établir entre $\mathfrak{T}$ et $\mathfrak{T}'$ une correspondance centrale dans $\mathfrak{T}K$, où chaque $\mathfrak{A}'_\iota$ correspond centralement à un $\mathfrak{A}_\iota$ [26]. On ramène d'abord la question au cas où aucun des $\mathfrak{A}_\iota$, $\mathfrak{A}'_\iota$ n'est abélien, et l'on considère les constituants dans $\mathfrak{A}_\iota$ du groupe répondant à $\mathfrak{A}'_\iota$ par une correspondance centrale de $\mathfrak{T}$ à $\mathfrak{T}'$ [17, 21].

21. Si, dans un automorphisme (8) j, les correspondants des éléments $a, b, \ldots$ de G sont $a', b', \ldots$, nous dirons que cet automorphisme *remplace* $a, b, \ldots$ par $a', b', \ldots$, et nous écrirons

$$j = \begin{pmatrix} a, & b, & \ldots \\ a', & b', & \ldots \end{pmatrix}.$$

Un diviseur de G que tout automorphisme remplace par lui-même est dit *caractéristique*.

22. Soient Γ l'ensemble (dénombrable ou non) des générateurs γ_1, γ_2, ... d'un groupe G satisfaisant à un système d'équations S; T un autre système d'équations $t_\iota = 1$ entre les γ; Γ' un ensemble d'éléments γ'_ι biunivoquement rapportés à Γ (γ'_ι correspondant à γ_ι); S' et T' deux systèmes formés avec les γ' comme S et T avec les γ''; A le p. p. c. m. des $x^{-1} t_\iota x$, x parcourant G. On démontre, à l'aide du théorème du n° 9 [18, n° 66], que *le groupe* G' *défini par* S' *et* T' *est isomorphe à* G/A.

Ainsi, des équations de G on déduit celles de G/A en adjoignant T à S. Si, par exemple, les t_ι sont tous les commutateurs des γ_ι, A divise le commutant C de G. D'ailleurs G/A est abélien. Donc $A \geq C$ (15). Donc $A = C$.

23. Soit $D = \Sigma d_\iota$ d'ordre δ le p. g. c. d. du g_α $A = \Sigma a_\iota = XD$ et du g_β $B = \Sigma b_\iota = DY$, $X = \Sigma x_\iota$ et $Y = \Sigma y_\iota$ étant des systèmes de restes de A (mod 1, D) et de B (mod D, 1) respectivement. On aura $A \times B = XD \times DY$. L'équation $x_\iota d_a y_\jmath = x_k d_b y_h$, qui équivaut à $x_k^{-1} x_\iota = d_b y_h y_\jmath^{-1} d_a^{-1}$ exige que $x_k^{-1} x_\iota$ soit dans D. Donc, dans $A \times B$, $x_\iota d_a y_\jmath$ ne sera répété que dans $x_\iota D \times D y_\jmath$, et il le sera autant de fois qu'il y a, dans D, de solutions (t_1, t_2) à l'équation $t_1 t_2 = d_a$, c'est-à-dire δ fois. *Donc chacun des* $\alpha\beta$ *éléments est répété* δ *fois exactement.* Considérons maintenant $AB = XDY = AY = XB$. L'équation $a_\iota y_\iota = a_k y_k$ ou $a_k^{-1} a_\iota = y_k y_\iota^{-1}$ montre que $y_k y_\iota^{-1}$ est dans D, d'où $y_k = y_\iota$. Donc $AB = A \times Y = X \times B$. Soit γ l'ordre de $C = \{A, B\}$. C est toujours $\geq AB$. Donc, si $C = AY$ ou si $C = XB$, AB sera un groupe (= C), et réciproquement. On sait d'ailleurs (12) que, si $BA = AB$, AB est un groupe (= C), et réciproquement. De $C = A \times Y = X \times B$, on déduit $(C, A) = (B, D)$, $(C, B) = (A, D)$, et réciproquement si C est fini. Donc, si γ est fini, et si $\gamma = \alpha\beta/\delta$, AB est un groupe, et réciproquement.

Si A, est permutable à chaque b_ι, donc normal dans $C = AB$, les Ay_ι forment un groupe; si alors $Ay_\iota Ay_k = Ay_h$, $y_\iota y_k y_h^{-1}$ est dans A, donc dans D, et $Dy_\iota Dy_k = Dy_h$; d'où $C \mid A \equiv B \mid D$.

Supposons maintenant A permutable à chaque b_ι et B à chaque a_i, donc A et B normaux dans $C = AB$. Alors $a_\iota^{-1} b_k^{-1} a_i b_k$ étant à la fois dans A et dans B est dans D, donc $a_i b_k$ dans $b_k a_\iota D$. Donc, D étant ici normal dans AB, $a_\iota D . b_k D = b_k D . a_\iota D$, c'est-à-dire que $AB \mid D$ est produit direct de $A \mid D$ et $B \mid D$.

Si chaque élément de A est permutable à B et à chacun des conjugués $x^{-1}Px$ dans B d'une partie P de B, et si aucun élément $\neq 1$ de B n'est permutable à chaque $x^{-1}Px$ (A est donc premier à B), AB est produit direct de A par B [18, n° 69].

Soient n groupes $A_1, \ldots, A_n$ d'ordres $a_1, \ldots, a_n$. Si les A_i sont deux à deux permutables, le produit $A_1 \ldots A_n$ est un groupe. Ce groupe est d'ordre $a_1 \ldots a_n$ toujours et seulement si les A_i sont premiers entre eux deux à deux.

Si chaque élément de A_i est permutable à chaque élément de A_k $(i, k = 1, n; i \neq k)$, nous dirons [22] que le groupe $\mathfrak{A} = A_1 \ldots A_n$ est une *association* des groupes $A_1, \ldots, A_n$. Il est clair que, pour chaque combinaison $i_1, \ldots, i_h$ des indices $1, \ldots, n$, chacun des groupes $B_1 = A_{i_1} \ldots A_{i_h}$ et $B_2 = A_{i_{h+1}} \ldots A_{i_n}$ est une association divisant $\mathfrak{A}$, et que $\mathfrak{A}$ est l'association $B_1 B_2$. Soit D_k le p. g. c. d. (abélien) de A_k et du produit des autres A_i. Le produit $D_1 \ldots D_n$ sera dit l'*associateur*. Si les A_i sont premiers entre eux deux à deux l'association est un produit direct.

Dans ce cas, supposons en outre que $A_1, \ldots, A_n$ contiennent respectivement des diviseurs normaux $A_{10}, \ldots, A_{n0}$ tels que

$$A_1 \mid A_{10} \equiv \ldots \equiv A_n \mid A_{n0}.$$

Soit $A_i = \sum_{\wedge} A_{i0} a_{ik}$, les complexes $A_{i0} a_{ik}$ se correspondant dans ces isomorphismes. L'ensemble des éléments des $A_{10} \ldots A_{n0} a_{1k} \ldots a_{nk}$ constitue un groupe $\mathfrak{A}'$, qui sera dit un *assemblage* des groupes $A_1, \ldots, A_n$, et représenté par $(A_1, \ldots, A_n)$. Le groupe $\mathfrak{A}' / A_{10} \ldots A_{n0}$ sera dit l'*assembleur*.

On peut toujours former un assemblage en prenant $A_{i0} = A_i$ $(i = 1, \ldots, n)$. L'assembleur se réduit alors à l'unité, et l'assemblage au produit direct.

Soit B'_1 l'assemblage $(A_{i_1} \ldots A_{i_h})$, l'assembleur étant

$$B'_1 \mid A_{i_1 0} \ldots A_{i_h 0},$$

et B'_2 l'assemblage $(A_{i_{h+1}} \ldots A_{i_n})$, l'assembleur étant $B'_2 \mid A_{i_{h+1} 0} \ldots A_{i_n 0}$. Il est clair que $\mathfrak{A}'$ est l'assemblage $(B'_1 B'_2)$, l'assembleur étant le même que précédemment.

24. Théorème de Frobenius. — P *étant une partie normale d'un*

g_N G, *le nombre* ν_m *des solutions de* $x^m \leqq P$ *dans* G *est multiple de m et* N [20, p. 220]. On ramène la proposition au cas où $m = p^\alpha$, p premier, puis, par récurrence, au cas où P se réduit à un élément a, d'ordre α, et l'on distingue les deux cas où $\alpha \not\equiv$ ou $\equiv 0 \bmod p$.

COROLLAIRE I. — *a étant un diviseur de* N, *le nombre des* $e_{(a)}$ *de* G *est multiple de a.*

COROLLAIRE II. — 1° *Soit* $N = np^\alpha$ (*p premier ne divisant pas n*). *Quel que soit* $\beta \leqq \alpha$, G *a un* g_{p^β}; *si* $\beta < \alpha$, *tout* g_{p^β} *de* G *sera contenu dans un* $g_{p^{\beta+1}}$, *et normal dans tout* $g_{p^{\beta+1}}$ *qui le contient.*

2° *Le nombre* n_δ *des* $g_{p^{\gamma+\delta}}$ *de* G *qui contiennent un* g_{p^γ} ($\gamma \geqq 0$) *déterminé* C *est* $\equiv 1$ *mod p.* On procède par récurrence (en considérant, pour la première partie, le normalisant d'un e_p de G) [18, n° 75]. En particulier *un* g_{p^2} *est toujours abélien*, car, s'il n'est pas cyclique, deux quelconques de ses e_p devront être permutables.

COROLLAIRE III. — *Si* H *est un* $g_{h^{p^\beta}}$ ($\beta \leqq \alpha$) *normal dans* G, *le nombre des* g_{p^β} *de* G *normaux dans un* g_{p^α} *de* G *qui sont contenus dans* H *est* $\equiv 1$ *mod p.*

COROLLAIRE IV. — *L'ordre du groupe* A *engendré dans* G *d'ordre ab par les* $e_{(a)}$ *est* $\equiv 0$ *mod a. Quand a est premier à b, cet ordre est égal à a si* G *a un* g_a *normal ou si* A *est abélien.*

COROLLAIRE V. — *Si* G, *d'ordre* νab (*a, premier à b*) *contient exactement a* $e_{(a)}$ *désignés par* $\alpha_1, \ldots, \alpha_a$, *et b* $e_{(b)}$ *désignés par* $\beta_1, \ldots, \beta_b$, *chaque* α *est permutable à chaque* β, *et* G *contient exactement ab* $e_{(ab)}$, *qui sont les* $\alpha_i\beta_k$. *Si* $\nu = 1$, G *est le produit direct d'un* g_a *par un* g_b.

Décomposition suivant deux modules. Théorème de Sylow.

25. [18, n° 81; 20, n° 56] Soit A un g_a et B un g_b du g_N G, et $G = \Sigma A x B$, x parcourant un système de restes de G (mod A, B). Le nombre m des x, que l'on peut appeler l'indice du couple A, B dans G, se désigne par (G : A. B). *Soit* D *un diviseur de* A *et* B, *normal dans* G. *Quand x parcourt un système de restes* (*mod* A. B), Dx *parcourt un système de restes de* G | D (*mod* A | D, B | D) *et réciproquement.*

Comme $Ax \times B$ correspond biunivoquement à $x^{-1}Ax \times B$, chaque élément de $Ax \times B$ est répété d_x fois, d_x étant l'ordre du p. g. c. d. de $x^{-1}Ax$ et B. Donc $N = \sum \frac{ab}{d_x}$.

Soit c_x le nombre des éléments distincts de AxB. On aura $c_x d_x = ab$. C'est là le nombre des solutions α, β, ξ de $\alpha\xi\beta = \xi$, quand α est dans A, β dans B, et ξ dans AxB. Ce nombre est indépendant de x. $\Sigma c_x d_x = mab$ est le nombre des solutions α, β, ξ de $\alpha\xi\beta = \xi$ quand α, β, ξ parcourent respectivement A, B, G. Or, cette équation équivaut à la condition que $\xi\beta\xi^{-1}$ soit dans A. Or, soient C_1, C_2, ... les classes de G; N_i l'ordre de C_i; a_i, b_i les nombres respectifs des éléments de A, B qui sont dans B_i. Quand ξ parcourt G, chaque élément $\xi\beta\xi^{-1}$ est répété N/N_i fois si β est dans C_i. Il arrive donc Na_i/N_i fois que $\xi\beta\xi^{-1}$ soit dans A. Donc $mab = N\sum \frac{a_i b_i}{N_i}$. [*Cf.* 20, n° 56].

26. [18, n^{os} 82-89] Théorème de Sylow. — *Dans un groupe* G, *d'ordre* $g = np^\alpha$ (p *premier ne divisant pas* n) *les* g_{p^α} [*dont le nombre est* $\equiv 1 \mod p$ (24)] *sont tous conjugés.* Soient en effet, dans G, A un g_{p^α}, B un g_{p^β} ($\beta \leq \alpha$), $G = \Sigma AxB$ la décomposition de G (mod A, B). On aura $n = \Sigma p^{\beta - \delta_x}$, p^{δ_x} étant l'ordre du p. g. c. d. de $x^{-1}Ax$ et B. Comme n est premier à p, un des δ_x est égal à β, c'est-à-dire que B divise un conjugué de A.

Soit $1 + kp$ le nombre des conjugués de A. Si $p^{\alpha+\rho}$ *est l'ordre maximum du p. g. c. d. de deux conjugués de* A, *on a* $kp \equiv 0 \mod p^\rho$. *Si, inversement* $kp \equiv 0 \mod p^\rho$ *et* $\not\equiv 0 \mod p^{\rho+1}$, *l'ordre maximum du p. g. c. d. de deux conjugués de* A *est* $\geq p^{\alpha-\rho}$.

Soit C, d'ordre $n'p^\alpha$, le normalisant de A dans G [C est son propre normalisant (15)]; D, d'ordre $\alpha = \nu p^{\beta+\gamma}$ (ν premier à p) le normalisant d'un $g_{p^\beta} B \leq A$ dans G; et supposons que B soit un p. g. c. d. maximum de deux conjugués de A, c'est-à-dire que B n'est contenu dans aucun p. g. c. d. $>$ B de deux conjugués de A. Alors 1° le p. g. c. d. de D et A est un $g_{p^{\beta+\gamma}}$, en sorte que *le nombre des conjugués de* A *qui contiennent* B *est de la forme* $1 + lp^\gamma$; 2° A *contient* $\frac{n'p^\alpha(1+lp^\gamma)}{d}$ *des conjugués de* B *dans* G; 3° D *contient des éléments d'ordre premier à* p *qui ne sont pas dans* C.

Deux complexes normaux dans A *et conjugués dans* G *sont*

aussi conjugués dans C. Si donc A divise le central de C, tous ses éléments appartiennent à des classes distinctes de G.

Si l'élément a, d'ordre p^α (*p premier*) *est permutable à un groupe* G, *d'ordre premier à p, et à un système de parties* P, P', ... *de* G *conjuguées dans* G, *a est permutable à un conjugué de* P.

Les relations entre les groupes de Sylow, relatifs aux divers diviseurs premiers de l'ordre du groupe, ainsi que les relations entre les groupes de Sylow d'un groupe et ceux de son commutant, ont été étudiées par O. Grun [25]. Soient : p un diviseur premier de l'ordre de G; P un de ses p-groupes de Sylow; N le normalisant de P dans G; G', P', N' les commutants respectifs de G, P, N; $G_0 \mid G'$ et $N_0 \mid N'$ les diviseurs maximums d'ordre premier à p de $G \mid G'$ et $N \mid N'$; P_0 le p. g. c. d. de P et N'; Q le p. p. c. m. des p. g. c. d. de P avec les conjugués de P' dans G; R le produit QP_0; alors *les groupes* $G \mid G_0$ *et* $P \mid R$ *sont isomorphes;* $P \mid P_0$ *appartient au central de* $N \mid P_0$, *et* P_0 *est le diviseur normal minimum de* N *ayant cette propriété.*

Théorème de Jordan-Holder.

27. Une suite G, A, B, ..., 1 de groupes en nombre fini dont chacun est normal maximum *dans le précédent* (et continu fini si G est continu fini) se nomme une *suite* ou *série de composition* de G. $G \mid A$, $A \mid B$, ... sont les *groupes facteurs*, (G, A), (A, B), ... *les facteurs* de la composition. *Si* G, A', B', ... 1 *est une autre suite de composition de* G, *la série* $G \mid A$, $A \mid B$, ... *coïncide, à l'ordre près, avec la série* $G \mid A'$, $A' \mid B'$ ... (18, n° 90). Le théorème étant évident pour les groupes simples, supposons-le vrai pour tous les diviseurs de G autres que G. A et A' étant normaux maxima, $G = AA'$, et $G \mid A$, $G' \mid A'$ sont simples; si donc D est le p. g. c. d. de A et A', $A \mid D \equiv G \mid A'$ et $A' \mid C \equiv G \mid A$ (23), D est normal maximum dans A et A', et le théoreme est démontré pour deux suites de composition de la forme G, A, D, E, ..., 1 et G, A', D, F, ..., 1. Or, il est supposé vrai pour les deux suites A, D, E, ..., 1 et A, B, ..., 1 comme pour les deux suites A', D, F, ..., 1 et A', B', ..., 1. Donc il l'est pour les deux proposées.

27$_a$. Un groupe fini dont tous les facteurs de compositions sont premiers est dit *résoluble*. Ainsi, les groupes abéliens et les $g_{p^\alpha}(24)$ sont résolubles. Pour qu'un groupe $G = G_0$ soit résoluble, il faut et il suffit que la suite des dérivés successifs G_1, G_2 ... (13) se termine par 1 (16).

Les groupes résolubles possèdent des propriétés intéressantes, établies par M. Hall [27]. En voici quelques-unes.

Soit G un groupe résoluble d'ordre $\Pi_1^r p_i^{\alpha_i}$ (les p_i premiers distincts). Si m est le produit d'un nombre quelconque de facteurs $p_i^{\alpha_i}$ distincts, G contient au moins un g_m. Ces diviseurs, dont l'ordre et l'indice sont premiers entre eux, sont les S-*sous-groupes* de G. Leurs propriétés sont analogues à celles des groupes de Sylow. Tous les S-sous-groupes de même ordre sont conjugués. Tout diviseur de G dont l'ordre divise celui d'une classe de S-sous-groupes est contenu dans un des S-sous-groupes de cette classe.

Pour qu'un groupe G, d'ordre $\Pi_1^r p_i^{\alpha_i}$ soit résoluble, il faut et il suffit qu'il contienne au moins r diviseurs d'indices $p_i^{\alpha_i}$ ($i = 1, \ldots, r$), soit $S'_1, \ldots, S'_r$.

Soit $h_1, \ldots, h_k$ une combinaison quelconque de k des nombres $1, \ldots, r$, et $D_k(h)$ le p. g. c. d. de $S'_{h_1}, \ldots, S'_{h_k}$. Pour chaque k, il existe C_r^k groupes $D_k(h)$. Le nombre total de ces groupes est donc $2^r - 1$. En leur adjoignant G, on obtient un système de 2^r groupes, appelé *système de Sylow* du groupe G. Deux groupes quelconques d'un même système de Sylow sont permutables. En particulier, pour $k = r - 1$, on obtient comme plus grands communs diviseurs r groupes de Sylow $S_1, \ldots, S_r$. Ainsi, dans tout groupe résoluble, il existe au moins un système de groupes de Sylow, deux à deux permutables, où chaque classe a exactement un représentant.

Inversement, les 2^r produits des groupes de Sylow d'un tel système forment un système de Sylow.

Tout groupe d'un système de Sylow est un S-sous-groupe. Tout système de S-sous-groupes deux à deux permutables fait partie d'un système de Sylow.

Dans un groupe résoluble, tous les systèmes de Sylow sont conjugués.

28. Une suite G, A, B, ..., 1 où chacun des groupes A, B, ... est normal dans G, et maximum parmi les diviseurs du précédent qui

sont normaux dans G, s'appelle une *suite ou série principale de composition de* G. Tout groupe G admet évidemment au moins une suite principale contenant un diviseur normal donné de G. D'une suite de composition, on ne peut pas toujours déduire une suite principale par la simple suppression de certains termes. Mais, d'une suite principale. on peut toujours déduire une suite de composition par l'insertion de nouveaux groupes.

La série $G|A, A|B, \ldots$ *des groupes facteurs d'une suite principale coïncide, à l'ordre près, avec la série* $G|A', A'|B', \ldots$ *des groupes facteurs d'une autre série principale.*

Dans une suite de composition G, ..., A, B, ..., K, L, ..., 1, *soient* A *et* L *deux diviseurs normaux de* G *consécutifs;* $A|L$ *est le produit direct de groupes simples isomorphes à* $A|B$ *et conjugués dans* $G|L$.

On voit que *tout groupe invariant minimum de* G *est le produit direct de groupes simples isomorphes* (d'ordre premier si G est résoluble). J'appellerai *principal* tout groupe de ce type. Inversement, *tout diviseur normal de* G, *produit direct de groupes simples non cycliques conjugués dans* G, *est normal minimum.*

29. Si A est le *central* (13) du groupe G, $G|A = C$ est le *cogrédient* de G. Plus précisément $A = A_1$ sera le *premier central*, et $C = C_1$ le *premier cogrédient* de G; le $i^{\text{ième}}$ central de G sera le diviseur A_i répondant dans G au central $A_i|A_{i-1}$ de $G|A_{i-1}$, et $G|A_i = C_i$ sera le $i^{\text{ième}}$ *cogrédient* de G ($A_0 = 1$, $C_0 = G$). Il y aura évidemment une valeur minima μ ($\geqq 0$) de i, telle que $A_i = A_\mu$ pour $i \geqq \mu$.

Si α_i est l'ordre maximum d'un élément de $A_i|A_{i-1}$, α_{i+1} est $\leqq \alpha_i$. Aucun élément $Ag \neq A$ de $G|A$ ne peut être une puissance de tous les autres. Donc $G|A$ n'est jamais hamiltonien. Tout élément a de A_2 est permutable à tout commutateur $x^{-1}y^{-1}xy$ de G.

Si $A_\mu = G$, G sera dit *spécial*. La suite 1, A_1, ..., $A_\mu = G$ des centraux sera dite *suite* ou *série spéciale* de G, et μ la *spécialité* de G. Les groupes abéliens sont de spécialité 1. Les groupes de spécialité 2 sont dits *métabéliens*.

Si G est produit direct de groupes G_k admettant les séries spéciales A_{hk} ($h = 0, 1, \ldots$), A_h est le produit direct des A_{hk}.

La propriété fondamentale d'un groupe spécial G d'ordre $\Pi p_i^{\alpha_i}$ est qu'il est produit direct de ses groupes de Sylow, et inversement.

Si $A_{\mu-1} \neq 1$, $G \mid A_{\mu-1}$ n'est pas cyclique.

Toute série principale d'un groupe spécial est une série de composition.

Si A et B sont deux groupes consécutifs d'une série principale du groupe spécial G, chaque élément de A|B est normal dans G. Inversement, si tout groupe facteur d'une seule série principale d'un groupe G a ses éléments normaux dans G, G est spécial.

Si, dans une série principale $A'_0 = 1, A'_1, A'_2, \ldots, G$, tout A'_{h+1}/A'_h divise $G|A'_h$, G est le produit direct de groupes d'ordres p^a, q^b, ..., $p, q, \ldots$ étant des nombres premiers distincts [14].

Supposons que tous les groupes facteurs principaux de G soient cycliques. Le commutant C de G sera contenu dans un diviseur normal P de G, produit direct de groupes d'ordres $p_i^{\alpha_i}$; et G|P sera abélien comme G|C. Soient A un diviseur normal d'ordre p^a du groupe G, x un élément de G d'ordre h premier à p, $G, \ldots, A_a = A$, $A_{a-1}, \ldots, 1$ une série principale de G; on peut trouver dans A_t hors de A_{t-1}, un élément a_t tel que

$$x^{-1} a_t x = a_t^{k_t} a_t, \qquad k_t^h \equiv 1 \bmod p^a.$$

30. Dans un groupe hamiltonien (13), toute série de composition est évidemment une série principale. D'autre part, tout groupe hamiltonien est produit direct de ses groupes sylowiens; et est par suite (29) un groupe spécial. Tous ces groupes sylowiens sont abéliens, sauf peut-être, si l'ordre du groupe est pair, le groupe sylowien H qui est d'ordre pair 2^m. Ce groupe H est le produit direct du g_8 des quaternions (le groupe Δ_1 du n° 11) par un groupe abélien principal (8) d'ordre 2^{m-3}.

CHAPITRE III.

GROUPES ABÉLIENS.

Groupes abéliens infinis.

31. Les éléments d'ordre fini d'un groupe abélien infini G y forment évidemment un diviseur A, fini ou non, et G|A n'a que des

éléments d'ordre infini. Si G | A admet une base (9) Ab_1, Ab_1^{-1}, Ab_2, Ab_2^{-1}, ..., G, qui contient toujours le p. p. c. m. B des b_i et b_i^{-1}, est le produit direct de A par B.

Supposons G dénombrable et sans éléments d'ordre fini. Il sera commode ici de modifier un peu la définition déjà donnée du *rang* (8) en ne comptant que pour un deux générateurs inverses l'un de l'autre et de ne mentionner explicitement que l'un deux.

Pour que le rang de G (*supposé sans éléments d'ordre fini*) *soit fini, il faut évidemment qu'il y ait un nombre r tel que, pour* $\rho > r$, ρ *éléments quelconques* $a_1, \ldots, a_\rho$ *de* G *soient liés par une relation de la forme* $\Pi_1^\rho a_i^{\alpha_i} = 1$, *où les* α_i *ne soient pas tous nuls, cela n'ayant pas toujours lieu pour* $\rho \leq r$. Car, si $e_1, \ldots, e_r$ forment une base de G, et si $a_i = \Pi_1^r e_k^{\lambda_{ik}}$, il suffit pour vérifier $\Pi_1^\rho a_i^{\alpha_i} = 1$, de déterminer les α_i par les équations $\Sigma_1^\rho \lambda_{ik}\alpha_i = 0$ $(k = 1, \ldots, r)$, qui sont toujours résolubles pour $\rho > r$.

Supposons cette condition remplie, et soient $a_1, \ldots, a_r$, r éléments de G entre lesquels n'existe aucune relation de la forme $\Pi a_i^{\alpha_i} = 1$, où les α_i ne sont pas tous nuls. Tout élément de G vérifiera une seule équation de la forme $x^\xi = \Pi a_i^{\xi_i}$, ξ étant minimum. On peut représenter x par les r rapports $\xi_i/\xi = X_i$. *Si les* $|X_i|$ *restent supérieurs à un nombre fixe positif, le rang de* G *est fini.*

32. Supposons G de rang fini n, admettant la base $a_1, \ldots, a_n$.

Supposons d'abord que, outre les équations

$$a_k a_k^{-1} = a_k^{-1} a_k = 1, \qquad a_j a_k = a_k a_j \qquad (j, k = 1, \ldots, n)$$

on ait encore $\Pi a_k^{\alpha_{ik}} = 1$. On peut [**18.** n^{os} **205, 207**], en introduisant de nouveaux générateurs $a'_1, \ldots, a'_n$, ramener les équations à la forme

$$a_1'^{e_1} = \ldots = a_r'^{e_r} = 1, \qquad a'_k a_k'^{-1} = a_k'^{-1} a'_k = 1, \qquad a'_j a'_k = a'_k a'_j \quad (j, k = 1, \ldots, n),$$

r étant le rang de la matrice $\alpha = (\alpha_{ik})$. G est donc le produit direct du groupe $A = \{a'_1, \ldots, a'_r\}$ et du groupe $I = \{a'_{r+1}, \ldots, a'_n\}$.

Supposons maintenant que G n'ait pas d'autres équations que

$$a_k a_k^{-1} = a_k^{-1} a_k = 1, \qquad a_j a_k = a_k a_j \qquad (j, k = 1, \ldots, n).$$

G est évidemment le produit direct des groupes $\{a_k, a_k^{-1}\}$.

Soit $b_1, \ldots, b_m$ une autre base de G, où $b_k = \Pi_1^n a_i^{\alpha_{ik}}$ $(k = 1, \ldots, m)$.

On voit qu'il faut $m = n$, et qu'il faut et suffit que le déterminant $|\alpha|$ de la matrice $\alpha = (\alpha_{ik})$ soit égal à ± 1.

Soient $b_j = \Pi_1^n a_i^{\beta_{ij}}$ $(j = 1, \ldots, \nu)$ ν éléments quelconques de G. Pour qu'ils puissent faire partie d'une base de G, il faut et suffit que les déterminants d'ordre ν de la matrice $\beta = (\beta_{ij})$ soient premiers entre eux. Le systeme des b_j est alors dit *primitif*.

Tout diviseur de G admet une base de rang $\leq n$. Soit B un diviseur de G ayant pour base $b_1, \ldots, b_m$, où $b_i = \Pi a_k^{\beta_{ik}}$ $(i = 1, \ldots, m)$. La matrice $\beta = (\beta_{ik})$ est de rang m. Par un changement de générateurs de G et de B, on peut ramener cette matrice à la forme normale [18, n° 205]. Les générateurs de B ont alors la forme

$$b'_1 = a'^{r_1}_1, \ldots, b'_m = a'^{e_m}_m.$$

Supposons $m = n$. Soit C un autre diviseur de G, de base $c_1, \ldots, c_n$, où $c_i = \Pi a_k^{\gamma_{ik}}$. Soit D le p. g. c. d. de B et C. On voit que le rang de D est encore n. Soit $d_1, \ldots, d_n$ une base de D, et

$$d_i = \Pi a_k^{\delta_{ik}} = \Pi b_h^{\mu_{ih}} = \Pi c_j^{\nu_{ij}}.$$

Si $\gamma = (\gamma_{ik})$, $\delta = (\delta_{ik})$, $\mu = (\mu_{ih})$, $\nu = (\nu_{ij})$, on voit que $\delta = \mu\beta = \nu\gamma$.

Groupes abéliens finis.

33. G étant un groupe abélien fini, G_1, G_2, ... des diviseurs de $G = \Pi G_i$, la forme Πx_i, où x_i parcourt chaque G_i, fournit chaque élément de G le même nombre de fois (18, n° 71), ce nombre se réduisant à 1 si les G_i sont premiers entre eux deux à deux. En particulier, soit $g_1, \ldots, g_n$, g_i étant d'ordre γ_i, un système de générateurs de G. Si x_i parcourt les nombres $0, \ldots, \gamma_i - 1$, chaque élément se présente sous la forme $\Pi g_i^{x_i}$ le même nombre de fois.

Tout groupe abélien est un produit direct de groupes cycliques, autrement dit *admet une base monogène* (8).

Si A est un groupe abélien d'ordre p^α, les ordres basiques et le nombre des générateurs basiques sont les mêmes dans toutes les bases de A. Si les ordres basiques sont p^a, p^b, ..., p^l, on dit que A est du *type* $(a, b, \ldots. k)$.

Plus généralement, soient G un groupe abélien, $A_1, \ldots, A_n$ ses

groupes sylowiens, $a_{i1}, \ldots, a_{im_i}$, une base de A_i, les ordres de ces générateurs n'allant jamais en croissant. Les éléments $g_k = \Pi_1^n a_{ik}$ (a_{ik} désignant 1 pour $k > m_i$) forment une base de G où l'ordre de g_{k+1} divise celui de g_k. Une base ayant cette propriété est dite *normale* (1)

Soient $p_i^{\alpha_i}$ l'ordre de A_i, et $p_i^{\alpha_{ik}}$ celui de a_{ik}; l'exposant de la plus haute puissance de p_i divisant l'ordre d'un générateur basique quelconque de G est l'un des nombres $\alpha_{i1}, \ldots, \alpha_{im_i}$.

Le rang de G est le plus grand des m_i. Le rang d'un diviseur de G est au plus égal à celui de G. Les ordres basiques sont les mêmes dans toutes les bases normales.

Soit $b_1, \ldots, b_n$ une base de G, b_k étant d'ordre β_k. Pour que les $c_i = \Pi_1^n b_k^{\gamma_{ik}}$ ($i = 1, \ldots, n'$) forment un système de générateurs de G, il faut et il suffit que la matrice des coefficients des n formes $\Sigma_1^{n'} \gamma_{ik} x_i + \beta_k y_k$ soit de rang n. Si G est d'ordre p^α et de rang r, pour que les c_i, en nombre $n' \geqq n$, forment un système de générateurs de G, il faut et il suffit qu'un des déterminants d'ordre r de la matrice des γ_{ik} soit premier à p.

34. Si G est principal d'ordre p^n, pour que $\{c_1, \ldots, c_h\}$ soit d'ordre p^h, il faut et suffit qu'un des déterminants d'ordre h de la matrice des γ_{ik} soit premier à p.

Si l'on pose $\Pi_1^x (p^i - 1) = P_x$, le nombre des g_{p^h} d'un g_{p^n} abélien principal est $P_n / P_h P_{n-h}$.

Si G' est diviseur d'un groupe abélien quelconque G, les ordres basiques normaux de G' divisent ceux de même rang de G.

A tout diviseur H d'un groupe abélien G répond au moins un diviseur H' isomorphe à G | H et tel que G | H' soit isomorphe à H; H et H' sont dits *réciproques dans* G [22].

Il existe toujours deux groupes abéliens infinis $\mathfrak{A}$ et $\mathfrak{C} < \mathfrak{A}$ tels que $\mathfrak{A} \mid \mathfrak{C} \equiv G$. Soient $a_1, \ldots, a_n$ une base de $\mathfrak{A}$, et $c_1, \ldots, c_n$ une base de $\mathfrak{C}$, où $c_i = \Pi a_k^{\gamma_{ik}}$. Au diviseur H de G correspond un diviseur $\mathfrak{B}$ de $\mathfrak{A}$ tel que $\mathfrak{B} \mid \mathfrak{C} \equiv H$. Soit $b_1, \ldots, b_n$ une base de $\mathfrak{B}$, où $b_i = \Pi a_k^{\beta_{ik}}$. On a aussi, pour les c_i, des expressions de la forme

(1) On remarquera que la base $a'_1, \ldots, a'_r$ du groupe A du n° 32 est une base normale [18, n° 205].

$c_i = \Pi b_k^{\mu_{ik}}$. Au diviseur H' de G correspond de même un diviseur $\mathcal{B}'$ de $\mathcal{A}$ contenant $\mathcal{C}$, et tel que $\mathcal{B}' \mid \mathcal{C} \equiv H'$. On peut introduire pour $\mathcal{A}$ et $\mathcal{C}$ de nouveaux générateurs $a'_1, \ldots, a'_n, c'_1, \ldots, c'_n$, et prendre, pour $\mathcal{B}'$, d'abord des générateurs $b'_1, \ldots, b'_n$, tels que l'on ait $c'_i = \Pi b_k'^{\beta_{ik}}$, ensuite des générateurs $b'_j = \Pi a_k'^{\mu_{jk}}$. On voit alors que, dans l'isomorphisme de H' à G | H, les b'_k liés par $c'_i = 1$ correspondent respectivement aux a_k liés par $b_i = 1$; et que, dans l'isomorphisme de H à G | H', les b_k liés par $c_i = 1$, correspondent respectivement aux a'_k liés par $b'_j = 1$ [22].

Si l'ordre de G est une puissance de p, le nombre de ses diviseurs d'ordre p^a est égal au nombre de ses diviseurs d'indice p^a [2].

Le nombre des diviseurs d'ordre p^a qui sont caractéristiques est égal au nombre des diviseurs d'indice p^a qui sont caractéristiques [2].

Soit $\mathcal{A}$ le produit direct des groupes abéliens $A_1, \ldots, A_n$ et G un diviseur de $\mathcal{A}$ ayant n diviseurs, distincts ou non, respectivement isomorphes à $A_1, \ldots, A_n$.

1° $\mathcal{A}$ *contient* n *diviseurs* $X_1, \ldots, X_n$ *respectivement isomorphes à* $A_1, \ldots, A_n$, *et tels que l'association* (23) $\mathfrak{X} = X_1 \ldots X_n$ *soit isomorphe à* G.

2° Considérons n groupes isomorphes premiers entre eux $\mathcal{A}_1 = \mathcal{A}, \mathcal{A}_2, \ldots, \mathcal{A}_n$, précisons leur correspondance isomorphique, et désignons par X'_i le diviseur de $\mathcal{A}_i$ correspondant à X_i de A. *Il existe un assemblage* (23) $\mathfrak{X}' = (X'_1 \ldots X'_n)$ *isomorphe à* G.

3° Soit $i_1, \ldots, i_h$ une combinaison quelconque des indices $1, \ldots, n$, $X = X_{i_1} \ldots X_{i_h}$, et $Y = X_{i_{h+1}} \ldots X_n$. On a (23) $\mathfrak{X} = XY$. Si B'_1 désigne l'assemblage $(A_{i_1} \ldots A_{i_h})$, l'assembleur étant $B'_1 \mid A_{i_1 0} \ldots A_{i_h 0}$, et B'_2 l'assemblage $(A_{i_{h+1}} \ldots A_{i_n})$, l'assembleur étant $B'_2 \mid A_{i_{h+1} 0} \ldots A_{i_n 0}$, il est clair que $\mathfrak{X}'$ est l'assemblage $(B'_1 B'_2)$, l'assembleur étant le même que précédemment. Dans ces conditions, *l'assembleur de* $(B'_1 B'_2)$ *est isomorphe à l'associateur de* XY [22].

35. Soient $G = \Sigma x$ un groupe abélien, E_h le diviseur de G formé des $e_{(h)}$ de G, P_h le diviseur de G formé des x^h de G. On a

$$(G, 1) = (E_h, 1)(P_h, 1).$$

Si G est d'ordre p^α, de rang r, et d'ordres basiques p^{α_i} $(\alpha_i \geq \alpha_{i+1})$,

si $h = p^m$, et si $\alpha_n \geqq m > \alpha_{n+1}$, on a

$$\varepsilon_h = (E_h, 1) = p^{mn+\alpha_1+\ldots+\alpha_n} \geqq h^r.$$

Si $h = p$, on a $(E_p, 1) = p^r$.

Le nombre des e_h est $\varepsilon_h(1 - p^{-n})$.

Soient $G_1, G_2, \ldots$ (G_i d'ordre $p_i^{\alpha_i}$) les groupes sylowiens d'un groupe abélien quelconque G. Soit $h = \Pi h_i$ ($h_i = p_i^{r_i}$). Soit E_{h_i} le groupe formé des $e_{(h_i)}$ de G_i, ε_{h_i} son ordre. Il est clair que $\varepsilon_h = \Pi \varepsilon_{h_i}$.

Un e_h x de G est dit *primitif* si la première de ses puissances qui est dans P_h est $x^h = 1$. On aura $x = \Pi x_i$, x_i étant d'ordre h_i. Pour que x soit un e_h primitif de G, il faut et il suffit que chaque x_i soit un e_{h_i} primitif de G_i.

Soit G d'ordre p^α et de base $a_1, \ldots, a_r$, a_i étant d'ordre p^{α_i}. Il n'y a aucun e_h primitif si h n'est pas un des invariants basiques. Soit donc $h = p^{\alpha_n}$, et supposons $\alpha_m < \alpha_{m+1} = \ldots = \alpha_n < \alpha_{n+1}$. Soient

$$A_m = \{a_1, \ldots, a_m\}, \qquad \text{et} \qquad B_m = \{a_{m+1}, \ldots, a_r\};$$

tout e_h de B_m est primitif; et tout e_h primitif est produit d'un $e_{(h)}$ de A_m par un e_h de B_m.

CHAPITRE IV.

GROUPES D'ORDRE p^m.

36. Un groupe d'ordre p^m sera dit un p-groupe. En faisant $n = 1$ dans le corollaire II du théorème de Frobenius (29), on voit que tout p-groupe G a une série de composition dont tout groupe facteur est d'ordre p. Tout diviseur d'indice p (maximum), qui est par suite normal, contient des éléments $\neq 1$ normaux dans G [18, n° 60]. G a donc un premier central $C_1 > 1$. De même $G \mid C_1$ a un central $C_2 \mid C_1$ ($C_2 > C_1$). Et ainsi de suite. G est donc spécial (29). Tout g_p de C_1 est évidemment normal dans G, et, inversement, tout g_p *normal de* G *est dans* C_1. Tout g_{p^2} est abélien. Tout diviseur d'indice p^2 contient le commutant.

Si G est métabélien et a un commutant cyclique, le nombre des générateurs basiques de même ordre de $G \mid C_1$ est toujours pair.

Si un diviseur maximum est abélien, il contient tous les centraux

successifs. Si le commutant de G est d'ordre p^n, la spécialité de G est $\leqq n+1$. Soit $f(n) = m - \frac{n(n-1)}{2}$. Si $f(n+1)$ est $\geqq 0$, un $g_{p^m}G$ a toujours un diviseur normal d'ordre $p^{f(n)}$ dont le central contient un g_{p^n} *normal dans* G.

Un $g_{p^m}G$ ayant un seul g_{p^n} est cyclique, sauf si, à la fois, $p=2$, $n=1$, $m \geqq 3$, auquel cas G est cyclique ou dicyclique. Plus généralement (24), un g_N ayant, quel que soit m, exactement m $e_{(m)}$ est cyclique.

37. Le p. g. c. d. D des diviseurs d'indice p d'un p-groupe est dit *diviseur principal.* Tout diviseur contenant D est dit *majeur.* Le groupe quotient G | D est abélien principal. Un diviseur M de G est majeur toujours et seulement s'il est normal dans G et si G | M est abélien principal.

Soit p^d l'indice de D dans G. et $a_1, \ldots, a_d$ un système de restes de G mod D. Ce système forme une base de G, dite *base minimun*. Toute base de G contient au moins d éléments, et, parmi ses éléments tous ceux d'une certaine base minimum.

Deux bases minimum $(a_1, \ldots, a_d)$ et $(b_1, \ldots, b_d)$ sont dites *équivalentes* quand il existe un automorphisme de G qui fait correspondre a_i et b_i $(i = 1, \ldots, d)$.

Toutes les bases minima équivalentes entre elles sont dites former une *classe*. Le nombre des bases minima distinctes de chaque classe est égal à l'ordre du groupe des automorphismes.

Dans un p-groupe non cyclique d'ordre impair, le nombre des diviseurs d'un même ordre est $\equiv$ à $1+p \mod p^2$; le nombre des diviseurs cycliques d'un même ordre est $\equiv$ à $0 \mod p$.

Le nombre total des diviseurs d'indice p^a d'un p-groupe $(0 \leqq a \leqq d)$ est $\equiv \mod p^{d-a}$ au nombre des g_{p^a} d'un g_{p^d} abélien principal. Le nombre des diviseurs non majeurs d'indice p^a est $\equiv 0 \mod p^{d-a+1}$ [8].

38. Soient a et b deux éléments d'un p-groupe G, et K le commutant de $\{a, b\}$. Si, quels que soient les éléments a et b et l'entier h, il existe, dans K, des éléments $k_1, k_2, \ldots$, tels que

$$(ab)^{p^h} = a^{p^h} b^{p^h} k_1^{p^h} k_2^{p^h} \ldots,$$

G sera dit *régulier*.

Si, quels que soient les éléments a et b, $\{a, b\}$ est de spécia-

lité $<p-1$, G est régulier. Tout p-groupe de spécialité $<p-1$, ou d'ordre $\leqq p^p$, est régulier. Si donc n est fixe et p arbitraire, les seuls groupes où p est $>n$ sont nécessairement réguliers.

Si a et b sont deux éléments quelconques d'un p-groupe régulier G, il existe un élément c tel que $a^{p^h}b^{p^h}=c^{p^h}$. L'ordre de ab ne peut pas dépasser les ordres de a et de b. Les $e_{(p^k)}$ de G forment un groupe $\mathfrak{E}_h$; les x^{p^h} (x parcourant G) forment un groupe P_h [8].

39. Soit p^m l'ordre maximum des éléments d'un p-groupe régulier G. Pour $h=1, \ldots, m$, les deux groupes quotients $P_{h-1}\,|\,P_h$ et $E_h\,|\,E_{h-1}$ sont de même ordre j_h. On a $j=j_1\geqq j_2\geqq\ldots\geqq j_m$. Pour $k=1, \ldots, j$, on désigne par m_k le nombre des $j_h\geqq k$. On a

$$m=m_1\geqq m_2\geqq\ldots\geqq m_j.$$

Réciproquement, j_a est le nombre des m_b qui sont $\geqq a$.

Chacune des sommes $m_1+\ldots+m_j$ et $j_1+\ldots+j_m$ est égale à l'exposant de p dans l'ordre de G.

Tout p-groupe régulier G *admet au moins une base monogène* $a_1, \ldots, a_j$, a_i *étant d'ordre* p^{m_i}. *Toute base monogène de* G *contient* j *éléments, dont le* $i^{ième}$ *est d'ordre* p^{m_i} [8].

Soit $1, C_1, \ldots, C_n=G$ la série spéciale d'un p-groupe. Si $C_i\,|\,C_{i-1}$ est de type $(a_i, b_i, \ldots, k_i)$ (33), on dira que G a pour *figure*

$$\Pi_1^n(a_i, b_i, \ldots, k_i),$$

considéré comme un produit symbolique.

Pour former tous les groupes d'ordre p_n (n donné), on déterminera les figures possibles d'après les nos 28, 29 et 36. A chaque figure correspond une forme générale d'équations, où certains exposants restent indéterminés. Il y a autant de types distincts que de systèmes d'exposants irréductibles les uns aux autres par changements de générateurs.

Ainsi on sait déterminer les groupes de figure

$$(\alpha)(\beta_{11}, \ldots, \beta_{1,\circ n_1}, \ldots, \beta_{k1}, \ldots, \beta_{k,\circ n_k}),$$

les β_{ih} ($h=1, \ldots, n_h$) étant égaux.

On a de même déterminé tous les groupes d'ordre p^n pour $n=3, 4, 5$ [18, nos 152 159] et $n=6$ [12].

CHAPITRE V.

AUTOMORPHISMES.

40. Soit $G = \Sigma x$, et fx l'élément correspondant à x dans un automorphisme (8) de G. On peut considérer cette correspondance comme définissant une substitution que nous représenterons par (x, fx). D'après la définition de l'automorphisme, on a $fxy = fxfy$. Il en résulte que les automorphismes de G forment un groupe $\mathcal{J}$ que l'on peut appeler *l'aggrédient* de G.

Les automorphismes $(x, g^{-1}xg)$, g étant dans G, sont dits *cogrédients* ou *internes*. Les autres, s'il en existe, sont dits *externes*.

Les automorphismes internes forment un groupe $\mathcal{C}$ appelé *cogrédient*, évidemment isomorphe à $G|C$, C étant le central de G, et normal dans $\mathcal{J}$.

41. Soit $\mathfrak{S}$ le symétrique dont les symboles sont les éléments x de G, c'est-à-dire l'ensemble de toutes les substitutions possibles sur les x. A tout élément g de G correspond une substitution (x, xg). L'ensemble de ces substitutions forme un groupe $\mathcal{G} \equiv G$, (x, xg) correspondant à g (1). Il en est de même du groupe $\mathcal{G}'$ des substitutions (x, gx). Chacun des groupes $\mathcal{G}$ et $\mathcal{G}'$ est l'ensemble des substitutions de $\mathfrak{S}$ permutables à toutes celles de l'autre. On dit alors que chacun de ces deux groupes est l'*adjoint* de l'autre.

On a $\{\mathcal{G}, \mathcal{J}\} = \{\mathcal{G}', \mathcal{J}\}$. Ce groupe, qui sera désigné par $\mathcal{K}$, est dit l'*holomorphe* de $\mathcal{G}$, et $\mathcal{K}$ est le normalisant de $\mathcal{G}$ et $\mathcal{G}'$ dans $\mathfrak{S}$. On a donc aussi $\mathcal{K} = \mathcal{G}\mathcal{J} = \mathcal{G}'\mathcal{J}$. On obtient tous les automorphismes de $\mathcal{G}$ en le transformant par les éléments de $\mathcal{K}$. On voit aisément que le p. g. c. d. de $\mathcal{G}\mathcal{G}'$ et $\mathcal{J}$ est $\mathcal{C}$, et que l'on a

$$\mathcal{G}\mathcal{G}' = \mathcal{G}\mathcal{C} = \mathcal{G}'\mathcal{C} \qquad \text{et} \qquad \mathcal{K} \mid \mathcal{G}\mathcal{G}' = \mathcal{J} \mid \mathcal{C}.$$

Tout groupe abstrait K contenant normalement G et isomorphe à $\mathcal{K}$ pourra être dit holomorphe de G. Le groupe K contiendra un diviseur $J \equiv \mathcal{J}$. Le groupe J pourra être dit l'aggrédient de G.

---

(1) Nous identifierons souvent, dans le langage, les groupes G et $\mathcal{G}$.

Les automorphismes de G qui conservent les classes d'éléments conjugués (12) de G forment un diviseur normal de $\mathcal{J}$. L'ordre de ce diviseur ne contient que des facteurs premiers divisant l'ordre de G. Si tous les diviseurs H_i d'un même type de G forment une seule classe, et si aucun automorphisme interne de G ne conserve chacun des H_i, il n'existe aucun automorphisme externe conservant chacun des H_i [3].

42. Un diviseur de G est caractéristique (21) toujours et seulement s'il est normal dans $\mathcal{K}$. La partie contenue dans $\mathcal{C}$ de toute série principale de $\mathcal{K}$ contenant $\mathcal{G}$ sera dite *série caractéristique* de G.

Le groupe G est dit *complet* lorsqu'il n'a pas d'automorphisme externe et que son central se réduit à 1.

Tout groupe complet se sépare (13) de tout groupe qui le contient normalement.

Lorsque C est égal à 1 et $\mathcal{C}$ caractéristique dans $\mathcal{J}$, $\mathcal{J}$ est complet.

Le même procédé de démonstration fournit le théorème plus général : Si $G = \Sigma x$ est caractéristique dans son holomorphe K, si, P étant une partie de K à laquelle aucun élément de G n'est permutable, les $x^{-1}Px$ forment un système caractéristique de K, et si aucun élément de K n'est permutable à tous les $x^{-1}Px$, G est complet.

Si H est normal dans G, l'ordre d'un automorphisme de G qui fournit l'automorphisme-unité de H et de G | H divise l'ordre de H.

Le même procédé de démonstration permet d'énoncer la proposition plus générale : Si H est normal dans $A < G$, si j est un automorphisme de G fournissant l'automorphisme-unité de H et de A | H, si j^m est la première puissance de j fournissant l'automorphisme-unité de A, m divise les ordres de j et de H.

Si G est un produit direct de groupes G_i, le produit direct P des aggrédients J_i des G_i divise normalement J. Si, de plus, les G_i sont caractéristiques dans G, on a $P = J$. Ce cas se présente pour un groupe abélien quelconque, produit direct de ses groupes sylowiens.

Soit [3, p. 239; 20, p. 70] G un groupe abstrait isomorphe de deux manières avec un groupe de substitutions $\mathcal{G}$. Soient H et H′ deux diviseurs de G correspondant, dans ces deux isomorphismes, à un diviseur de $\mathcal{G}$ fixant un symbole. Il existe toujours un automorphisme de G dans lequel H et H′ se correspondent. Cet automorphisme est

interne ou externe, suivant que, dans G, H et H′ sont conjugués ou non.

43. Soient : G un groupe résoluble (27_a) d'ordre $g = \Pi_1^r p_i^{\alpha_i}$; $S_1, \ldots, S_r$ (S_i d'ordre $p_i^{\alpha_i}$) r groupes de Sylow deux à deux permutables, appartenant à un même système de Sylow $\mathfrak{S}(27_a)$; $\mathfrak{A}_i$, d'ordre a_i, l'aggrédient de S_i. *Le diviseur de l'aggrédient* $\mathfrak{J}$ *de* G *qui laisse invariant le système* $\mathfrak{S}$ *est isomorphe à un diviseur du produit direct* $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$. Il en résulte que, *si m est le nombre de systèmes de Sylow distincts de* G, *l'ordre de* $\mathfrak{J}$ *divise le produit* $ma_1 \ldots a_r$, *et par suite* $g\psi(g)$, *où*

$$\psi(g) = \Pi_1^r \psi(p_i^{\alpha_i}), \qquad \psi(p^\alpha) = (p^\alpha - 1)(p^\alpha - p) \ldots (p^\alpha - p^{\alpha-1}).$$

Si l'ordre d'un automorphisme j de $\mathfrak{G}$ *est premier à l'ordre de* $\mathfrak{G}$, *j laisse invariant au moins un système de Sylow de* $\mathfrak{G}$ [27].

44. L'aggrédient d'un groupe abélien principal d'ordre p^r est isomorphe au groupe des substitutions linéaires $|x_i \quad \Sigma_1^r a_{ik} x_k|\,(i = 1, \ldots, r)$ dont les coefficients parcourent tous les nombres entiers mod$p$ tels que le déterminant $|a_{ik}|$ soit $\not\equiv 0 \bmod p$. Ce groupe sera désigné par $L(r, p)$ [18].

L'aggrédient J d'un groupe abélien d'ordre p^{ar} et de type $(a, a, \ldots, a)$ possède une série de a diviseurs normaux $H_1, H_2, \ldots, H_{a-1}, 1$, dont chacun est contenu dans le précédent, ayant les propriétés suivantes : le groupe-quotient $J|H_1$ est isomorphe à $L(r, p)$; les $H_i|H_{i+1}$ $(i = 1, \ldots)$ sont abéliens principaux d'ordre p^r.

Soient G un p-groupe abélien ayant n_h générateurs basiques d'ordres p^h $(h = 1, \ldots, r)$, S_h le système de ces n_h générateurs, P_h le groupe formé (35) des éléments de G qui sont les p^h-ièmes puissances d'éléments de G, A_h le diviseur de J qui conserve tous les éléments de P_h. Tout A_h est normal dans J. Tout groupe quotient $A_h|A_{h-1}$ contient normalement un diviseur abélien principal d'ordre

$$p^{(n_h + \ldots + n_r)(n_{h+1} + \ldots + n_r)},$$

et d'indice

$$\psi(n_h)\, p^{n_h(n_{h+1} + \ldots + n_r)},$$

$\psi(n_h)$ désignant l'ordre de $L(n_h, p)$ [23].

Tous les automorphismes d'un groupe abélien figurent parmi les

transformations obtenues de la manière suivante : soient H et H′ deux groupes réciproques (34) dans G; choisissons arbitrairement une des correspondances isomorphiques existant entre H′ et G | H, h' de H′ répondant à Hx de G | H. Chacun des éléments g de G appartenant à un même complexe Hx sera remplacé par gh' [23].

Si G est un g_p cyclique $\{g\}$, son aggrédient est le g_{p-1} cyclique engendré par la substitution $|g \quad g^a|$, a étant une des racines primitives de p. Son holomorphe est $\{s, g\}$, s étant un élément vérifiant

$$s^{p-1} = 1, \qquad s^{-1}gs = g^a.$$

Dans le symétrique S de degré $n \neq 6$ (c'est-à-dire opérant sur n symboles), les n diviseurs fixant un symbole forment un système conjugué qui contient tous les diviseurs de ce type. Aucun élément de S n'est permutable à chacun de ces diviseurs. D'après ce qu'on a vu à la fin du n° 41, tout automorphisme de S permute entre eux ces n diviseurs. D'ailleurs S n'a aucun élément normal. Il est donc complet [23].

Pour $n = 6$, le symétrique, considéré comme groupe abstrait G, est isomorphe de deux manières à un même groupe abstrait S de degré 6. Les deux diviseurs de G correspondant respectivement à un diviseur de S fixant un symbole ne sont pas conjugués dans G. Donc (42) G admet un automorphisme externe. Il n'est donc pas complet. Il a une classe et une seule d'automorphismes externes [23]. Son aggrédient est donc d'ordre 1440 [3].

INDEX BIBLIOGRAPHIQUE.

1. Baer. — Einfuhrung des Scharbegriffs (*Crelle*, t. 160, 1929, p. 199).
2. Birckoff. — Diviseurs d'un Groupe abélien (*P. L. M. S.*, t. 38, 1934, p. 389).
3. Burnside. — *Theory of Groups of finite Order* (2e édition).
4. Burnstin et Mayer. — Distributive Gruppen von endlicher Ordnung (*Crelle*, t. 160, 1929, p. 111).
5. Dickson. — Definition of a Group and Field by independent Postulates. Semi-Groups and general Isomorphism between infinite Groups (*Transactions of Am. Math. Soc.*, t. 6, 1905, p. 198).
6. Dornte. — Untersuchungen uber einen verallgemeinerten Gruppenbegriff (*Math. Zeitschr.*, t. 29, 1929, p. 1).
7. Garver. — Note concerning Group Postulates (*Bull. A. M. S.*, t. 40, 1934, p. 698); Postulates for special Types of Groups (*Ibid.*, t. 42, 1936, p. 125).
8. Hall. — Contribution to the Theory of Groups of prime-power Orders (*Proc. Lond. Math. Soc.*, 2e sér., vol. 36, p. 29); On a Theorem of Frobenius (*Ibid.*, t. 40, 1935, p. 469).
9. Levi. — Intergruppen freien Gruppen (*Math. Zeit.*, t. 32, 1930, p. 315).
10. Magnus. — Diskontinuierliche Gruppen mit definierenden Relationen (*Crelle*, t. 163, p. 141).
11. Nielsen. — Isomorphismengruppe der freien Gruppen (*Math. Ann.*, t. 91, 1924, p. 175).
12. Potron. — *Les groupes d'ordre p^6* (Thèse, 1904).
13. Prufer. — Theorie der abelschen Gruppen (*Math. Zeit.*, t. 20, 1924, p. 165).
14. Remak. — Neuer Beweis eines Satzes uber spezielle endliche Gruppen (*Crelle*, t. 142, 1913, p. 54).
15. Remak. — Minimale invariante Untergruppen in der Theorie der endlichen Gruppen (*Crelle*, t. 162, 1930, p. 1).
16. Remak. — Darstellung der endlichen Gruppen als Untergruppen direkter Producten (*Crelle*, t. 163, 1930, p. 1).
17. Schmidt. — Sur les Produits directs (*Bull. Soc. Math. de France*, t. 41, 1913, p. 161).
18. De Séguier. — *Éléments de la Théorie des Groupes abstraits* (1904).
19. De Séguier. — Représentation du Symétrique et de l'Alterné (*Journ. de Math.*, 1910, p. 402).
20. De Séguier. — *Éléments de la Théorie des Groupes de Substitutions* (1912).
21. De Séguier. — Les Produits directs et la Structure de leurs Diviseurs maximums (*Bull. Soc. Math. de France*, t. 41, 1913, p. 164).

22. De Séguier. — Sur les Diviseurs des Produits directs abéliens finis (*Bull. Sc. Math.*, t. 50, 1926).

23. Speiser. — *Theorie der Gruppen von endlicher Ordnung* (2e édit., 1927).

24. Suskewitsch. — Gruppen ohne eindeutige Umkerhrbarkeit (*Math. Ann.*, t. 99, 1929, p. 30).

25. Grun. — Beitrage zur Grüppentheorie (*Crelle*, t. 174, 1935, p. 1).

26. Remak. — Zerlegung endlichen Gruppen in direkte unzerlegbare Factoren (*Crelle*, t. 139, 1911, p. 293).

27. Hall. — A note on soluble Groups (*Journ. of Lond. Math. Soc.*, vol. 3, 1928, p. 98); A characteristic property of soluble Groups (*Ibid.*, vol 12, 1937, p. 198 et 201); On the Sylow-Systems of a soluble Group; On the System Normalizers of a soluble Group (*Proc. of Lond. Math. Soc.*, vol. 43, 1937, p. 316 et 507).

Note. — Le renvoi à 18 est toujours sous-entendu, lorsqu'aucune référence spéciale n'est indiquée pour la démonstration d'un théorème énoncé.

INDEX DES TERMES.

TABLE DES MATIÈRES.