SÉMINAIRE DE MATHÉMATIQUES

PAUL DUBREIL

Théorie des groupes

Séminaire de Mathématiques (Julia), tome 1 (1933-1934), exp. n° 1, p. 1-28

<http://www.numdam.org/item?id=SMJ_1933-1934__1__A1_0>

Exemplaire n°4

Ne peut quitter la salle de lecture

SEMINAIRE DE MATHEMATIQUES

Première année 1933-1934

Théorie des Groupes et des Algèbres

4. Théorie des Groupes

Exposé fait par M. Paul DUBREUIL le 13 Novembre 1933

BIBLIOGRAPHIE

On pourra consulter :

Van der Waerden, Moderne Algebra , T.I , chap. 2 et 6

E.Noether, Hyperkomplexe Grössen und Darstellungstheorie
Math. Zeit. 30 p.641

Speiser , Theorie der Gruppen von endlicher Ordnung

Nous ne faisons aucune hypothèse sur la façon dont ont été définis les ensembles que nous considèrerons ni sur la nature de leurs éléments (nombres, points, transformations géométriques, fonctions, ensembles d'autres éléments, etc ...) . Nous désignerons en général un ensemble par une majuscule, et ses éléments par des minuscules. Quand un élément a appartient à un ensemble E, nous le noterons : $a \in E$

Quand un ensemble E' se compose d'éléments appartenant tous à un autre ensemble E, nous dirons E' sous-ensemble de E et nous écrirons $E' \subseteq E$

Nous appellerons intersection de deux ensembles E, E' l'ensemble de leurs éléments communs et nous noterons cette intersection : $E \wedge E'$

I.- Groupes ordinaires

I.- Définition

Nous dirons d'un ensemble E qu'il forme un groupe si les trois hypothèses suivantes sont réalisées :

a) A tout couple de deux éléments a, b, de G correspond suivant une loi déterminée appelée loi de composition un troisième élément c de G que nous désignerons par l'une ou l'autre des deux notations : c = (a,b) ou c = ab . Cette loi de composition est supposée associative c'est-à-dire que l'on a : (ab)c = a(bc) quelque soient les trois éléments a,b,c de G.

b) Il existe dans G un élément e tel que ea = a quelque soit l'élément a de G ; on appelle e une unité à gauche de G. Cette hypothèse (b) peut être remplacée par celle (b') de l'existence d'une unité à droite de G, c'est-à-dire d'un élément e' tel que ae' = a quelque soit l'élément a de G.

c) A tout élément a de G on peut faire correspondre un élément a^{-1} de G tel que $a^{-1}a = e$; a est dit l'inverse à gauche de G.

Si l'hypothèse (b) a été remplacée par l'hypothèse (b'), la troisième hypothèse (c) doit être remplacée par celle de l'existence pour tout élément a d'un inverse à droite a^{-1} tel que $aa^{-1} = e'$.

2.- Remarques

a) on dit souvent de la loi de composition qu'elle définit une "opération" à l'intérieur du groupe G : la notion de loi de composition pour les éléments d'un groupe est en effet une

généralisation de la notion d'opération pour les nombres de l'arithmétique .

b) Nous avons supposé seulement de l'opération du groupe qu'elle était associative . Il peut arriver qu'elle soit commutative, c'est-à-dire que c ne dépende que des deux facteurs a et b dans G ; le groupe est dit alors abélien . Si aucune confusion n'est possible avec une autre opération préalablement définie, on peut employer pour la loi de composition, la notation de l'addition et écrire : c = a+b . On n'emploiera d'ailleurs cette notation que dans le cas abélien .
Si deux éléments a et b d'un groupe jouissent de cette propriété que ab = ba on les dit permutables.
On dit de aba^{-1} qu'il est le transformé de b par a
On voit que si deux éléments sont permutables chacun d'eux est identique à son transformé par l'autre .

c) Enfin, il peut arriver que G soit un sous-ensemble d'un ensemble E à l'intérieur duquel est définie l'opération considérée . La première hypothèse exprime que ab appartient à G toutes les fois que a et b lui appartiennent déjà .
Il peut arriver aussi que dans E aient été définies plusieurs opérations ; il importera alors toujours de préciser par rapport à laquelle de ces opérations G doit être considéré comme un groupe .

3. Conséquences de la définition

On démontre que tout inverse à gauche est aussi un inverse

à droite ; que l'unité à gauche est aussi une unité à droite et que les divisions à droite et à gauche sont toujours possibles et d'une seule manière, c'est-à-dire que, quelque soient a et b les équations ax = b et ya = b ont toujours une solution et une seule .

On démontre que les hypothèses (b) et (c) [ou (b') et (c')] peuvent être remplacées par l'hypothèse de la possibilité et de l'unicité des divisions . On démontre même que si le groupe G est fini, c'est-à-dire n'a qu'un nombre fini d'éléments, il suffit de supposer l'~~unicité~~ possibilité de la division . Le nombre des éléments s'appelle l'ordre du groupe .

Dans le cas où G est abélien et où on emploie la notation additive, on désigne par O l'élément unité .

4.- Sous-groupe

On dit qu'un sous-ensemble G' de G est un sous-groupe s'il forme lui-même un groupe par rapport à l'opération définie dans G.

On voit immédiatement que pour que G' soit un sous-groupe il faut et il suffit que :

a) ab appartienne à G' si a et b appartiennent eux-mêmes à G'

b) a^{-1} appartienne à G' si a appartient à G' .

On peut exprimer encore ceci en disant : la condition nécessaire et suffisante pour que G' soit un sous-groupe de G est que G' contienne ab^{-1} s'il contient a et b .

On peut remarquer que G' contient nécessairement l'unité; il peut arriver que G' soit abélien alors que G ne l'est pas .

5.- Décomposition d'un groupe en classes par rapport à un sous-groupe . Sous-groupe invariant.- Groupe facteur .

Soit G un groupe, G' un sous-groupe de G .

Considérons un élément a de G et faisons-lui ocrrespondre l'ensemble des éléments ag' de G, g' étant un élément quelconque de G' ; nous appellerons cet ensemble une classe (gauche) de G relative à G' et nous la noterons aG' . Elle contient a et on voit aisément qu'étant données deux classes aG',bG', de deux choses l'une : ou elles n'ont aucun élément commun ou elles sont identiques . Un élément quelconque de G appartient donc à une classe et une seule et on peut dire que G' décompose G en classes.

S'il arrive que le nombre de classes soit fini, on appelle ce nombre l'index de G' dans G et on le note(G/G'); en particulier, si G est fini et d'ordre n , et si n' désigne l'ordre de G' on a la relation : (G/G') = n/n', on voit ainsi que l'ordre d'un sous-groupe d'un groupe fini est un diviseur de l'ordre du groupe .

On définit d'une manière analogue les classes à droite G'a de G relatives à G' . Si le sous-groupe G' est tel que chaque classe à droite coincide avec la classe à gauche correspondante : aG' = G'a quelque soit a dans G ; on dit que G' est

un sous-groupe invariant de G

Cette définition équivaut à la suivante : le transformé d' un élément d'un sous-groupe invariant G' par un élément quelconque de G appartient encore à G'.

Si G' est un sous-groupe quelconque, les transformés de ses éléments g' par un élément g de G : $g''= gg'g^{-1}$ forment un sous-groupe que l'on note $G''=gG'g^{-1}$ en général différent de G' , et que l'on dit conjugué de G'.

Exemples de sous-groupes invariants

I°) les sous-groupes d'un groupe abélien sont tous des sous-groupes invariants .

2°) Les éléments d'un groupe G permutables avec tous les autres éléments de G forment un sous-groupe invariant appelé centre de G.

Considérons un groupe G et un sous-groupe invariant G' de G Considérons l'ensemble des classes de G par rapport à G'; soient aG', bG' , deux d'entre elles, on verra facilement que la classe abG' ne dépend pas des deux éléments a,b, pris dans chacune d' elles; on définit donc ainsi une loi de composition faisant correspondre à deux classes aG', bG', la classe abG' ; on verra facilement que les conditions de définition d'un groupe sont satisfaites, et que par suite les classes relatives à un sous-groupe invariant forment elles-mêmes un groupe . On appelle ce groupe, groupe facteur et on le note G/G'.

La correspondance qui existe entre les éléments a de G et

la classe aG' à laquelle ils appartiennent est un cas particulier de l'homomorphisme que nous allons étudier .

6.- Homomorphisme

Soient E, $\overline{E}$ deux ensembles à l'intérieur de chacun desquels est définie une loi de composition ; on dit qu'une correspondance entre les éléments de E et de $\overline{E}$ est un homomorphisme si:

1°) à tout élément de E correspond un seul élément $\bar{a}$ de $\overline{E}$

2°) Tout élément $\bar{a}$ de $\overline{E}$ est l'homologue d'au moins un élément de E.

3°) On a : $\overline{ab} = \bar{a}\,\bar{b}$

Autrement dit un homomorphisme est une application de E sur $\overline{E}$ univoque dans le sens de E vers $\overline{E}$, dans laquelle tous les éléments de $\overline{E}$ sont obtenus et qui respecte la loi de composition

On dit encore que $\overline{E}$ est homomorphe à E et on écrit : $E \sim \overline{E}$. On appelle aussi parfois un homomorphisme un isomorphisme mériédrique .

Théorème : Si un ensemble $\overline{G}$ est homomorphe à un groupe G, cet ensemble est un groupe ; son élément unité est l'homologue de l'élément unité de G ; à deux éléments inverses de G correspondent deux éléments inverses de $\overline{G}$. A un sous-groupe G' de G correspond un sous-groupe $\overline{G'}$ de $\overline{G}$.

La démonstration est immédiate ; on remarquera en outre que $\overline{G}$ peut être abélien sans que G le soit , de même qu'un sous-groupe quelconque de G peut être transformé en un sous-groupe invariant

de $\bar{G}$.

7.- Isomorphisme

Soit $\bar{E}$ un ensemble homomorphe à E ; s'il arrive que la correspondance entre les éléments de E et $\bar{E}$ soit biunivoque, on dit que c'est un isomorphisme (ou encore isomorphisme holoèdrique) et on dit les deux ensembles isomorphes l'un à l'autre . On note cette relation par : $E \simeq \bar{E}$ ou $E \cong \bar{E}$.

8.- Automorphismes

Soit E un ensemble à l'intérieur duquel est défini une loi de composition ; s'il existe une correspondance biunivoque entre les éléments de E respectant la loi de composition, cette correspondance est un isomorphisme faisant correspondre E à lui-même ; on l'appelle un automorphisme .

Considérons deux automorphismes d'un ensemble . Le premier fait passer de x à $\bar{x}$, le second de $\bar{x}$ à $\bar{\bar{x}}$; l'opération qui fait passer de x à $\bar{\bar{x}}$ est encore un automorphisme qui se déduit donc deux deux autres par une loi de composition . On verra facilement que cette loi satisfait aux conditions de définition d'un groupe . Autrement dit, les automorphismes d'un ensemble forment un groupe .

Parmi les automorphismes d'un groupe G, il faut considérer particulièrement ceux qui font passer d'un élément x à son transformé par un élément choisi d'avance a: $x \to axa^{-1}$; ces automor-

phismes qui dépendent chacun de l'élément s choisi sont appelés les automorphismes intérieurs du groupe . On appelle les autres des automorphismes extérieurs . On verra facilement que les automorphismes intérieurs forment un groupeI , sous-groupe du groupe de tous les automorphismes . On verra aussi que I est homomorphe au groupe G et (en cherchant quand deux automorphismes intérieurs définis par des éléments distincts sont les mêmes) que le groupe des automorphismes intérieurs est isomorphe au groupe facteur du centre de G . On remarquera enfin que le centre est l'ensemble des éléments qui définissent l'automorphisme intérieur-unité .

9.- Théorème fondamental de l'homomorphisme

Soit $\bar{G}$ un groupe homomorphe à un groupe G, l'ensemble E des éléments de G qui ont pour homologue dans $\bar{G}$ l'élément-unité est un sous-groupe invariant de G et $\bar{G}$ est isomorphe au groupe facteur G/E.

On vérifie d'abord que E est un sous-groupe invariant de G On remarque d'autre part qu'un élément $\bar{a}$ de $\bar{G}$ est l'homologue non seulement de a mais de tous les éléments de la classe aE.

L'intérêt de ce théorème (et des précédents, qui n'en sont au fond, que des applications particulières) est qu'il exprime qu'un groupe G n'a pas,à des isomorphismes près, d'autres images homomorphes que ses groupes-facteurs.

II.- Groupes avec opérateurs

IO.- Définitions

Soit G un groupe dont nous désignerons les éléments par des lettres romaines, a, b,..... et Ω un ensemble de transformations portant sur les éléments de G ; nous désignerons les transformations par des lettres grecques ϑ, H ..... et nous dirons que ce sont des opérateurs si :

a) A tout symbole ϑ de Ω et à tout élément a de G correspond un élément de G que nous noterons ϑa

b) Si l'on a, quelque soient ϑ, a, b :

$$\vartheta (ab) = \vartheta a . \vartheta b$$

c'est à dire si les transformations sur les éléments de G définissepar les opérateurs sont distributives par rapport à l'opération du groupe ; si le groupe était abélien et si l'opération du groupe était écrite sous forme additive, on aurait :

$$\vartheta (a + b) = \vartheta a + \vartheta b$$

On peut encore dire sous une forme plus brève que ϑ est un opérateur s'il représente un homomorphisme de G sur un sous-ensemble de G (qui peut être G lui-même).

G s'appelle un groupe avec opérateurs . L'ensemble Ω est dit un système ou domaine d'opérateurs. On dit qu'un système d'opérateurs est absolu si deux opérateurs différents désignent

des homomorphismes différents .

II.- Sous-groupes conservés . Groupe simple .

On dit qu'un sous-groupe G' de G est conservé par les opérateurs du syatème Ω si le transformé d'un élément quelconque du sous-groupe G' par un opérateur quelconque de Ω appartient encore à ce sous-groupe ; autrement dit, si : $s \in G'$ entraine $\Theta s \in G'$ quelque soit Θ .

Dans l'étude des groupes avec opérateurs seuls sont intéressants les sou-groupes conservés, aussi sous-entendrons -nous souvent le mot "conservé".

Si deux sous-groupes sont conservés, leur intersection est un sous-groupe également conservé .

Etant donné deux-sous-groupes A et B d'un même groupe G dont l'un est un sous-groupe invariant, on appelle produit de ces deux sous-groupes l'ensemble C des éléments $c = ab$ tels que $a \in A$, $b \in B$. On verra aisément que C est un sous-groupe . On verra aussi que si A et B sont deux sous-groupes conservés dont l'un au moins est invariant, leur produit est un sous-groupe conservé .

On dit qu'un groupe avec opérateurs est simple s'il n'admet pas de sous-groupe invariant conservé .

Un exemple d'opérateurs nous est donné par les automorphismes intérieurs : ϑ_a est l'isomorphisme qui fait passer de x à axa^{-1} ; autrement dit, $\vartheta_a x = axa^{-1}$. Les sous-groupes conser-

vés quand Ω est le domaine des automorphismes intérieurs sont les sous-groupes invariants .

Si on prend pour opérateurs tous les automorphismes du groupe, les sous-groupes conservés sont appelés les sous-groupes caractéristiques du groupe .

I2.- Application aux anneaux. Idéaux.

On appelle anneau un groupe abélien dans lequel est défini une seconde opération associative , distributive par rapport à l'opération du groupe . Nous noterons l'opération du groupe sous la forme additive et la seconde opération sous la forme de la multiplication . On a donc :

$pq.r = p.qr$ et $r(a+b) = ra + rb$

La multiplication n'est pas supposée commutative.

Dans un anneau chaque élément r définit deux opérateurs : Γ_r qui fait passer de x à rx , et Δ_r qui fait passer de x à xr ; autrement dit;

$\Gamma_r x = rx$ $\qquad$ $\Delta_r x = xr$

Les sous-groupes conservés par les opérateurs Γ_r sont dits des idéaux à gauche, les sous-groupes conservés par les opérateurs Δ_r sont dits des idéaux à droite. Enfin les sous-groupes conservés par les opérateurs Γ_r et Δ_r sont dits des idéaux des deux côtés .

Si en enlevant de l'anneau l'élément 0, il reste un groupe par rapport à la multiplication, on dit que l'anneau

est un corps . Dans un corps il n'y a que deux idéaux . Celui qui se compose du seul élément 0 et celui qui est identique à l'anneau lui-même ; c'est le cas de l'anneau des nombres rationnels ; ce n'est pas celui de l'anneau des nombres entiers .

I3. -Application aux modules.

Soit G un groupe abélien, l'opération du groupe étant l'addition ; soit un anneau et supposons définie une multiplication (à gauche par exemple) des éléments de G par les éléments de Ω satisfaisant aux trois conditions suivantes :

a) $r(a+b) = ra + rb$ $\quad a \in b$, $b \in G$, $r \in \Omega$

qui montre que les r définissent des opérateurs .

b) $(rs)\, a = r\,(sa)$

c) $(r+s)\, a = ra + sa$

On dit alors que G est un Ω module(à gauche) et on appelle sous-modules, les sous-groupes de G conservés par les opérateurs .

I4.- Homomorphisme par rapport aux opérateurs

Soient G et $\overline{G}$ deux groupes possédant le même système d'opérateurs ; supposons G l'image de $\overline{G}$ dans une correspondance Nous dirons que celle-ci est un homomorphisme par rapport aux opérateurs , si :

I°) C'est un homomorphisme au sens précédemment défini du mot

$G \curvearrowright \overline{G}$

2°) si $\overline{\Theta a} = \Theta \bar{a}$ quelque soit l'opérateur Θ du domaine considéré et l'élément a de G choisis.

Si la correspondance entre G et $\bar{G}$ est biunivoque, on dit que c'est un isomorphisme par rapport aux opérateurs. Comme dans l'étude des groupes avec opérateurs, seuls sont intéressants les homomorphismes et isomorphismes par rapport aux opérateurs nous sous-entendrons souvent "par rapport aux opérateurs".

On peut étendre aux groupes avec opérateurs et à leurs homomorphismes les propriétés vues pour les groupes ordinaires ; en particulier le théorème fondamental de l'homomorphisme devient

Soient G et $\bar{G}$ deux groupes ayant le même système Ω d'opérateurs et un homomorphisme par rapport aux opérateurs qui fait passer de G à $\bar{G}$

I°- l'ensemble E des éléments de G qui ont pour homologue dans $\bar{G}$ l'élément unité est un sous-groupe invariant conservé

2°- Il y a isomorphisme par rapport aux opérateurs entre $\bar{G}$ et le groupe facteur de G par rapport à E :

$$\bar{G} \simeq G/E$$

Pour la démonstration ; analogue à celle que nous avons indiquée pour les groupes ordinaires, cf. V.d.W. I. P.I35 .

III.- Théorèmes d'isomorphismes

15.- Remarque . Premier Théorème .

Les deux théorèmes que nous allons donner complètent le théorème fondamental de l'homomorphisme . Ils sont valables pour les groupes avec opérateurs, à la condition de sous-entendre les locutions "par rapport aux opérateurs", quand on parle d'homomorphisme ou d'isomorphisme et "conservé" quand on parle de sous-groupe .

Soit $\bar{G}$ l'image de G dans un ~~iso~~homomorphisme ; soit $\bar{A}$ un sous-groupe invariant de $\bar{G}$ et A l'ensemble des éléments de $\bar{G}$ qui ont pour homologues dans $\bar{G}$ des éléments de $\bar{A}$.

1°- A est un sous-groupe invariant de G

2°- Il y a isomorphisme entre le groupe facteur de G par rapport à A et le groupe facteur de $\bar{G}$ par rapport à $\bar{A}$:

$$G/A \simeq \bar{G}/\bar{A}$$

Démonstration : Des isomorphismes $G \sim \bar{G} \sim \bar{G}/\bar{A}$ résulte que le groupe facteur $\bar{G}/\bar{A}$ est isomorphe à un certain facteux groupe-facteur G/N de G . Le sous-groupe invariant N est constitué par l'ensemble des éléments de G qui ont pour homologue dans le groupe facteur $\bar{G}/\bar{A}$ l'unité, c'est à dire qui ont pour homologue dans $\bar{G}$ les éléments de $\bar{A}$, c'est donc A .

Cas particulier : Si $\bar{G}$ est un groupe facteur de G, on a l'isomorphisme :

$$G/N \,/\, A/N \simeq G/A$$

I6- Deuxième Théorème

Soient A et B deux sous-groupes d'un même groupe G , B étant un sous-groupe invariant

I°- Le sous-groupe intersection de A et B : $A \cap B$, est un sous-groupe invariant de A .

2°- On a l'isomorphisme :

$$AB/B \simeq A/(A \cap B)$$

Démonstration :

L'homomorphisme $G \frown G/B$ fait correspondre aux éléments a de A les classes aB ; on a donc l'homomorphisme $A \frown AB/B$ et il existe un sous-groupe invariant N de A tel que l'on ait l'isomorphisme $A/N \simeq AB/B$. N est l'ensemble des éléments de A auxquels correspondent l'unité dans AB/B . Ce sont donc ceux qui appartiennent aussi à B et on a : $N = A \cap B$.

IV.- Séries de composition

I7.- Définitions

Soit G un groupe . On appelle série normale une suite finie de sous-groupes de G, telle que chacun d'eux soit sous-groupe invariant du précédent :

(S) $G = G_0 \supset G_1 \supset G_2 \ldots\ldots \supset G_\ell = E$

On appelle l la longueur de la série . Les groupes facteurs G_{h-1}/G_h sont les facteurs de la série. La série peut présenter des répétitions : $G_h = G_{h+1}$

Une série normale

(S') $G = G_0 \supset G'_1 \supset G'_2 \ldots\ldots \supset G'_{\ell'} = E$

est dite subdivision de la série S si les termes de (S') contiennent tous les termes de (S) et éventuellement d'autres .

Une série normale sans répétition telle que toute subdivision ait au moins une répétition, s'appelle une série de composition . Quelque soit p , il n'existe alors aucun sous-groupe G' différent de G_{h-1} et G_h qui soit sous-groupe invariant de G_{h-1} et qui admette G_h comme sous-groupe invariant ; autrement dit, tous les facteurs d'une série de composition sont simples

I8.- Exemples

Le groupe des racines douzièmes de l'unité G_{12} admet comme sous-groupe l'ensemble des racines sixièmes G_6 ; l'ensemble des racines quatrièmes G_4 l'ensemble des racines cubiques G_3 , l'

ensemble des racines carrées G_2 et enfin l'unité .

On voit facilement que la série

$$G_{12} \supset G_4 \supset G_4 \supset E$$

est une série normale, les facteurs G_{12}/G_4 G_4/G_4 G_4/E étant respectivement isomorphes à G_3 E et G_4 , mais que ce n'est pas une série de composition . On verra enfin que G admet les trois séries :

$$G_{12} \supset G_6 \supset G_3 \supset E$$
$$G_{12} \supset G_6 \supset G_2 \supset E$$
$$G_{12} \supset G_4 \supset G_2 \supset E$$

comme séries de composition .

Il y a des groupes qui n'ont pas de séries de composition par exemple,le groupe abélien des nombres entiers (positifs ou négatifs) où l'opération du groupe est l'addition : soit , en effet, $G_{\ell-1}$ le dernier sous-groupe $\neq E$ d'une série normale On voit facilement que G_ℓ se compose des multiples d'un entier m ; il admet un sous-groupe à savoir le sous-groupe des multiples de l'entier 2m .

Savoir si un groupe admet une série de composition et comparer celles-ci s'il en admet plusieurs est donc la question essentielle .

I9.- Isomorphisme de deux séries normales

Soient (S) $G \supset G_1 \supset G_2 \supset \dots\dots \supset G_\ell = E$

et (S') $G \supset G'_1 \supset G'_2 \supset \dots\dots \supset G'_{\ell'} = E$

deux séries normales du groupe G . On les dit isomorphes si :

I°) elles ont la même longueur $l = l'$

2°) il existe une correspondance biunivoque entre les facteurs de la première série et ceux de la seconde de telle sorte que deux facteurs homologues soient isomorphes .

Par exemple les deux séries normales

$G_{12} \rhd G_6 \rhd G_6 \rhd E$ et $G_{12} \rhd G_{12} \rhd G_2 \rhd E$

sont isomorphes .

On verra facilement que si deux séries normales (S) et (S') sont isomorphes, à toute subdivision S, de S, correspond une subdivision S'_1 de S' isomorphe à S_1.

20.- Théorème de Jordan-Hölder

Si un groupe G admet deux séries de composition différentes (S) $G \rhd G_1 \rhd \ldots\ldots \rhd G_r = E$

$G \rhd G'_1 \rhd \ldots\ldots \rhd G'_s = E$

elles sont isomorphes (donc r=s)

Ce théorème est d'une très grande importance dans la théorie de Galois (Voir par exemple Picard ,Traité d'Anslyse , t.III chap.XVII) . Jordan a, le premier, comparé ces deux séries et trouvé qu'elles avaient la même longueur , Hölder, ultérieurement, a montré l'isomorphisme des groupes-facteurs . Tous les deux supposaient le groupe fini .

Nous allons d'abord donner une démonstration générale qui repose sur un théorème de Schreier .

21.- Théorème de Schreier.

Soient

(S) $G > G_1 > G_2 \ldots\ldots\ldots > G_r = E$

(S') $G > H_1 > H_2 \ldots\ldots\ldots H_s = E$

deux séries normales d'un même groupe G . Il existe deux séries

$(\bar{S})$ $G > \ldots G_1 > \ldots G_2 > \ldots\ldots\ldots > G_r = E$

$(\bar{S}')$ $G > \ldots H_1 > \ldots H_2 > \ldots\ldots\ldots > H_s = E$

qui sont respectivement des subdivisions de S et de S' et sont isomorphes entre elles .

Le théorème est évident pour s=1 , r quelconque , ainsi que pour r=1 , s quelconque .

Il se démontre par récurrence sur r et s et application des théorèmes d'isomorphisme (Voir Van der Waerden, I p.139).

Le théorème de Jordan-Hölder en résulte immédiatement : Soient S et S' les deux séries de composition du groupe G, $\bar{S}$ et $\bar{S}'$ les deux séries isomorphes qu'on en déduit par le théorème de Schreier . $\bar{S}$ ne diffère de S que par des répétitions auxquelles correspondent des répétitions dans $\bar{S}'$ en les supprimant de part et d'autre, on a encore deux séries isomorphes : or ce sont S et S' .

On tire aussi du théorème de Schreier ce théorème important :

Si un groupe admet une série de composition, il passe au moins une telle série par un sous-groupe invariant quelconque

donné .

Voir aussi pour une démonstration du théorème de Jordan-Hölder pour des groupes non nécessairement finis :

E.Noether. Abstrakter Aufban der Idealthéorie in algébraischen Zahl . und Funktionenkörpen. Math. Ann. T 96. 1926. p.67. prg.10

La démonstration y est donnée pour des modules , mais l' hypothèse de la commutativité n'y intervient pas .

23.- Cas des groupes finis

Il résulte de la définition que tout groupe fini admet une série de composition

Appelons, en effet, sous-groupe invariant maximum de G, un sous-groupe invariant tel qu'il n'existe pas de sous-groupe invariant de G qui le contienne . On voit qu'un groupe peut avoir plusieurs sous-groupes invariants maxima et que chacun d'eux peut commencer une série de composition, qu'on obtient en mettant après chaque sous-groupe un de ses sous groupes invariants maxima (l'ordre des sous-groupes successifs, va en effet en décroissant)

Le théorème de Jordan-Hölder en résulte au moyen d'un raisonnement par récurrence sur le nombre des facteurs premiers figurant dans l'ordre du groupe .

Définition : On dit qu'un groupe est résoluble quand les groupes facteurs sont tous d'ordre premier . On voit aisément que tout sous-groupe d'un groupe résoluble est lui-même résoluble.

24.- Théorème de Sylow

Cauchy a montré que quand un nombre premier p divise l'ordre d'un groupe , il y a dans le groupe un élément a d'ordre p (c'est à dire tel que $a^{p} = E$ et que $a^{p'} \neq E$ pour tout p' tel que $0 < p' < p$)

Sylow a étendu ce résultat en montrant que :

Si p^{r} est la plus grande puissance de p divisant l'ordre du groupe G, il existe dans G un sous-groupe d'ordre p^{s} , quelque soit le nombre s ($0 \leq s \leq r$)

Nous renvoyons pour la démonstration et pour celle des théorèmes suivants au mémoire de Sylow (Math.Ann. Bd 5 S.584) ou à l'ouvrage de Speiser : Théorie der Gruppen von endlicher Ordnung (p.42) .

25.Groupes de Sylow.

On appelle sous-groupes de Sylow les groupes dont nous venons d'affirmer l'existence et qui ont pour ordre p^{r}

Théorème :

Tout sous-groupe de G dont l'ordre est une puissance de p p^{s} est contenu dans un groupe de Sylow .

Théorème :

Deux groupes de Sylow correspondant au même nombre premier sont conjugués (voir prg.5 la définition)

Définition : soit C un ensemble d'éléments d'un groupe G, l'ensemble des éléments x de G permutables avec l'ensemble C , c'est à dire tels que $xCx^{-1} = C$ forme un sous-groupe de G que l'on ap-

pelle le normalisateur de C

Théorème :

Le nombre des différents groupes de Sylow d'ordre p est égal à l'index du normalisateur de l'un quelconque d'entre eux Ce nombre est congru à un (module p).

V.- Produits directs .
Groupes complètement réductibles

26.- Définitions

On dit que le groupe G est le produit direct de A et B si les trois conditions ($\mathcal{A}$) sont vérifiées :

1) A et B sont des sous-groupes invariants de G.

2) AB = G , le produit étant entendu au sens ordinaire (c'est à dire que AB représente l'ensemble des produits des éléments de A par les éléments de B)

3) $A \wedge B = E$, c'est à dire que A et B n'ont pas d'autre élément commun que l'unité .

On montre que ces trois conditions ($\mathcal{A}$) et l'ensemble des trois conditions ($\mathcal{B}$) suivantes sont équivalentes :

1) Tout élément g de G est le produit d'un élément a de A par un élément b de B $\quad g = ab$

2) Un élément de G n'est susceptible que d'une seule représentation de ce genre :

$ab = a'b'$ entraine $a=a' \quad b=b'$

3) Tout élément de A est permutable avec tout élément de B

$ab = ba$

Si G est le produit direct de A et B on écrira : $G = A \times B$ (la notation G = AB ou G = A.B ayant le sens rappelé plus haut).

Si G est abélien et si l'opération du groupe est l'addi-

tion, on dit G, somme directe de A et B et on écrit :

$$G = A + B$$

quand aucune confusion n'est possible .

29- Généralisation

On généralise la notion de produit direct au cas de plusieurs facteurs en opérant par induction complète :

Nous dirons que le groupe G est le produit direct des sous-groupes $A_1, A_2 \ldots A_n$, si les conditions ($\mathcal{A}$) suivantes sont remplies :

1) Tout A_i est un sous-groupe invariant de G
2) $G = A_1 . A_2 . \ldots . A_n$
3) $(A_1 \ldots A_{p-1}) \cap A_p = E$ pour $p=2, \ldots n$

et on verra de même que ces conditions sont équivalentes aux suivantes ($\mathcal{B}$) :

1) Tout élément g de G peut se représenter d'une manière unique comme le produit de n facteurs $s_1, s_2, \ldots s_n$ appartenant à $A_1, A_2, \ldots A_n$ respectivement : $y = s_1 s_2 \ldots s_n$
et un élément quelconque d'un sous-groupe A_p est permutable avec un élément quelconque d'un autre sous-groupe $A_{p'}$:

$$s_p s_{p'} = s_{p'} s_p \quad (p' \neq p)$$

On voit que dans le produit direct $G = A_1 \times A_2 \times \ldots \times A_n$ l'ordre des facteurs est indifférent, donc que chaque facteur A_p n'a aucun élément commun avec $B_p = A_1 . A_2 \ldots A_{p-1} . A_{p+1} \ldots A_n$ sauf E .

$$A_p \cap B_p = E$$

et d'après le théorème d'isomorphie : $G/A_r \simeq B_r$ $G/B_r \simeq A_r$

30.- Propriétés des produits directs

1) Si le groupe G est le produit direct de deux sous-groupes A et B respectivement isomorphes à deux sous-groupes $\bar{A}$ et $\bar{B}$ d'un groupe G' , ce groupe G' admet un sous-groupe $\bar{G}$ isomorphe à G et qui est le produit direct de $\bar{A}$ et $\bar{B}$.

$A \simeq \bar{A}$ $B \simeq \bar{B}$ entraine $A \times B \simeq \bar{A} \times \bar{B}$

2) Si G est le produit direct de A et B et si G admet un sous-groupe G' admettant lui-même A comme sous-groupe :

$G = A \times B$ $G \supset G' \supset A$

G' est le produit direct de A et d'un autre sous-groupe (à savoir l'intersection de G' et de B)

$G' = A \times B'$ ($B' = G' \cap B$)

3) Si G est le produit direct de deux facteurs A et B admettant des séries de composition de longueurs respectives m et n , G admet une série de composition de longueur m + n passant pas chacun de ces facteurs .

32.- Groupes complètement réductibles

On dit qu'un groupe est complètement réductible s'il est le produit direct d'un nombre fini de groupes simples :

$G = A_1 \times A_2 \ldots\ldots \times A_n$

les groupes $G = A_1 \times A_2 \ldots\ldots A_n$

$G_1 = A_1 \times A_2 \ldots\ldots A_{n-1}$

.....

$$G_{n-1} = A_1$$

$$G_n = E$$

forment alors une suite de composition de longueur n dont les facteurs sont isomorphes à

$$A_n \quad A_{n-1} \ldots\ldots A_1$$

Il résulte immédiatement du théorème de Jordan-Hölder que le nombre des facteurs et les facteurs eux-mêmes sont déterminés par G à une isomorphie près .

On voit aussi que tout groupe isomorphe à un groupe complètement réductible est complètement réductible .

33.- Décomposition d'un groupe complètement réductible

Nous avons le théorème fondamental suivant :

Si G est un groupe complètement réductible

$$G = A_1 \times A_2 \ldots\ldots A_n$$

et si H est un sous-groupe invariant de G :

1) H est facteur direct de G, c'est à dire qu'on peut lui associer un sous-groupe B tel que G soit le produit direct de H et B : $G = H \times B$

2) Le sous-groupe B est lui-même produit direct de certains des groupes A_ν

3) H est complètement réductible

Démonstration :

On a : $G = A_1 A_2 \ldots\ldots A_n$

d'où (1) $G = H A_1 A_2 \ldots A_n$

Considérons le produit ordinaire $H_1 = H A_1$

Le sous-groupe invariant $H \cap A_1$ étant sous-groupe invariant de A_1

qui est simple , ne peut être égal qu'à l'unité E ou à A

Dans le premier cas on a :

$$H_1 = H \times A_1$$

dans le second :

$$H_1 = H$$

De même , le produit $H_1 A_2$ est égal à $H_1 \times A_2$ ou à H_1 , suivant que $H_1 \cap A_2 = E$ ou $H_1 \cap A_2 = A_2$. En continuant le raisonnement de proche en proche , nous voyons qu'en supprimant éventuellement au second membre de (1) certains des facteurs A nous pouvons mettre G sous la forme d'un produit direct :

$$G = H \times A_{i_1} \times A_{i_2} \times \ldots\ldots \times A_{i_2}$$

Si l'on pose $B = A_{i_1} \times A_{i_2} \times \ldots\ldots A_{i_2}$,

on a $G = H \times B$ $H \simeq G/B \simeq A_{j_1} \times \ldots\ldots \times A_{j_s}$

$A_{j_1} \ldots\ldots A_{j_s}$ étant les facteurs A de la représentation (1) qui ne figurent pas dans B .

Les modules de base finie et les systèmes hypercomplexes sont des groupes réductibles (par rapport à l'addition) ; leur décomposition en somme directe jouera un rôle fondamental dans leur étude .
