LE SÉMINAIRE DE MATHÉMATIQUES 1933–1939

édition réalisée et annotée par
Michèle Audin

1. Année 1933-1934
Théorie des groupes et des algèbres

Paul Dubreil

Théorie des groupes

Séminaire de mathématiques (1933-1934), Exposé 1-A, 19 p.

<http://books.cedram.org/MALSM/SMA_1933-1934__1__A_0.pdf>

Séminaire de mathématiques 13 novembre 1933
Exposé 1-A, p. 1 à 19

THÉORIE DES GROUPES

par **Paul Dubreil**

Bibliographie. On pourra consulter[1]

Van der Waerden, Moderne Algebra, T.1, 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 considérerons 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 $E \cap E'$.[2]

1/2

I. Groupes ordinaires

1.– Définition. Nous dirons d'un ensemble E qu'il forme un *groupe* si les trois hypothèses suivantes sont réalisées[3] :

a) À 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[4] : $c = (a, b)$ ou $c = ab$. Cette loi de composition est supposée *associative*, c'est-à-dire que l'on a : $(ab)c = a(bc)$ quels que soient les trois éléments a, b, c de G.

b) Il existe dans G un élément[5] e tel que $ea = a$ quel que 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 $ae' = a$ quel que soit l'élément a de G.

c) À 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 a.

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
2/3 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,[6] 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 que aba^{-1} 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 chaque 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
3/4 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, quels que 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 [la possibilité][7] 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 0 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[8] :

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.* 4/5

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 correspondre 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 en commun ou elles sont identiques. Un élément quelconque de G appartient donc à une classe et à 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*[9] 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 groupe G' est tel que chaque classe à droite coïncide avec la classe à gauche correspondante : $aG' = G'a$ quel que soit a dans G ; on dit que G' est un *sous-groupe* 5/6
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.

(1) 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'.

6/7 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 $\overline{a}$ de $\overline{E}$

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

(3) On a : $\overline{ab} = \overline{a}\overline{b}$

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.[10]

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.[11]

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 $\overline{G}$. À 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
7/8 en un sous-groupe invariant de $\overline{G}$.

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

8.– Automorphismes. Soit E un ensemble à l'intérieur duquel est défini[e] 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 $\overline{x}$, le second de $\overline{x}$ à $\overline{\overline{x}}$; l'opération qui fait passer de x à $\overline{\overline{x}}$ est encore un automorphisme qui se déduit des 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 et
$x \to axa^{-1}$; ces automorphismes qui dépendent chacun de l'élément a choisi sont 8/9
appelés les automorphismes *intérieurs* du groupe. On appelle les autres des automorphismes *extérieurs*. On verra facilement que les automorphismes intérieurs forment un groupe I, 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 $\overline{G}$ un groupe homomorphe à un groupe G, l'ensemble E des éléments de G qui ont pour homologue dans $\overline{G}$ l'élément-unité est un sous-groupe invariant de G et $\overline{G}$ 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 $\overline{a}$ de $\overline{G}$ 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. 9/10

II. Groupes avec opérateurs

10.– Définitions. Soit G un groupe dont nous désignerons les éléments par des lettres romaines[12] $a, b, \dots$ et Ω un ensemble de transformations portant sur les éléments de G ; nous désignerons les transformations par des lettres grecques $\theta, \mathrm{H}, \dots$ et nous dirons que ce sont des *opérateurs* si :

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

b) Si l'on a quels que soient θ, a, b :

$$\theta(ab) = \theta a \cdot \theta b$$

c'est-à-dire si les transformations sur les éléments de G définies par 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

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

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).[13]

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
10/11 différents désignent des homomorphismes différents.

11.– Sous-groupes conservés. Groupe simple. On dit qu'un sous-groupe G' de G est *conservé* par les opérateurs du système 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 $a \in G'$ entraîne $\theta a \in G'$ quel que soit θ.

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

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

Étant 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, $\theta_a(x) = axa^{-1}$. Les
11/12 sous-groupes conservés 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.*

12.– Application aux anneaux. Idéaux. On appelle *anneau* un groupe abélien dans lequel est défini[e] 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 :

$$pq \cdot r = p \cdot qr \text{ et } r(a+b) = ra + rb$$

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 idéaux conservés par les opérateurs Γ_r et Δ_r sont dits des *idéaux des deux côtés.*[14]

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 12/13
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.

13.– Application aux modules. Soit G un groupe abélien, l'opération du groupe étant l'addition ; soit $\mathfrak{O}$ un anneau et supposons définie une multiplication (à gauche, par exemple) des éléments de G par les éléments de $\mathfrak{O}$ satisfaisant aux trois conditions suivantes :

a) $r(a+b) = ra + rb$ $a \in G$, $b \in G$, $r \in \mathfrak{O}$ qui montrent que les r définissent des opérateurs.

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

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

On dit que G est un $\mathfrak{O}$-module (à gauche) et on appelle sous-modules les *sous-groupes* de G conservés par les opérateurs.

14.– Homomorphismes 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

(1) C'est un homomorphisme au sens précédemment défini du mot $G \sim \overline{G}$ 13/14

(2) Si $\overline{\theta a} = \theta\overline{a}$ quel que soit l'opérateur θ du domaine considéré et l'élément a de G choisis.

Si la correspondance entre G et $\overline{G}$ 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 $\overline{G}$ deux groupes ayant le même système Ω d'opérateurs et un homomorphisme par rapport aux opérateurs qui fait passer de G à $\overline{G}$:

(1) *L'ensemble E des éléments de G qui ont pour homologue dans $\overline{G}$ l'élément unité est un sous-groupe invariant conservé.*

(2) *Il y a isomorphisme par rapport aux opérateurs entre $\overline{G}$ et le groupe facteur de G par rapport à E :*

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

Pour la démonstration, analogue à celle que nous avons indiquée pour les groupes
14/15 ordinaires, cf.V.d.W. I. p.135.

III. Théorèmes d'isomorphismes

15.– Remarque. Premier théorème. Les deux théorèmes que nous allons donner complètent le théorème fondamental de l'hmomorphisme. 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 $\overline{G}$ l'image de G dans un homomorphisme ; soit $\overline{A}$ un sous-groupe invariant de $\overline{G}$ et A l'ensemble des éléments de G qui ont pour homologues dans $\overline{G}$ des éléments de $\overline{A}$.

(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 $\overline{G}$ par rapport à $\overline{A}$*

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

Démonstration. Des isomorphismes $G \sim \overline{G} \sim \overline{G}/\overline{A}$ résulte que le groupe facteur $\overline{G}/\overline{A}$ est isomorphe à un certain 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 $\overline{G}/\overline{A}$ l'unité, c'est-à-dire qui ont pour homologues dans $\overline{G}$ les éléments de $\overline{A}$, c'est donc A.

Cas particulier. Si $\overline{G}$ est un groupe facteur de G, on a l'isomorphisme :[15]

$$G/N \Big/ A/N \simeq G/A$$

15/16

16.– Deuxième théorème. *Soient A et B deux sous-groupes d'un même groupe G, B étant un sous-groupe invariant.*

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

16/17

IV. Séries de composition

17.– Définitions. Soit G un groupe. On appelle *série normale*[16] une suite finie de sous-groupes de G telle que chacun d'eux soit sous-groupe invariant du précédent :

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_\ell = E \tag{S}$$

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

Une série normale

$$G = G_0 \supset G'_1 \supset G'_2 \supset \cdots \supset G'_{\ell'} = E \tag{S'}$$

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.* Quel que soit p, il n'existe alors aucun sous-groupe G' différent de G_{p-1} et G_p qui soit sous-groupe invariant de G_{p-1} et qui admette G_p comme sous-groupe invariant ; autrement dit, tous les facteurs d'une série de composition sont *simples.*

18.– 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.[17] 17/18

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.

19.– Isomorphisme de deux séries normales. Soient

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

et

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

18/19 deux séries normales du groupe G. On les dit isomorphes si :

(1) elles ont la même longueur $\ell = \ell'$

(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

$$G_{12} \supset G_6 \supset G_6 \supset E \text{ et } G_{12} \supset G_{12} \supset G_2 \supset E$$

sont isomorphes.

On verra facilement que si deux séries normales (S) et (S') sont isomorphes, à toute subdivision (S_1) 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) $$G \supset G_1 \supset G_2 \supset \cdots \supset G_r = E$$

(S') $$G \supset G'_1 \supset G'_2 \supset \cdots \supset G'_s = E$$

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'analyse 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 donner une démonstration générale qui repose sur un théorème de Schreier. 19/20

21.– Théorème de Schreier. *Soient*

(S) $$G \supset G_1 \supset G_2 \supset \cdots \supset G_r = E$$

(S') $$G \supset H_1 \supset H_2 \supset \cdots \supset H_s = E$$

deux séries normales d'un même groupe G, il existe deux séries

($\overline{\mathrm{S}}$) $$G \supset \cdots \supset G_1 \supset \cdots \supset G_2 \supset \cdots \supset \cdots \supset G_r = E$$

($\overline{\mathrm{S}}'$) $$G \supset \cdots \supset H_1 \supset \cdots \supset H_2 \supset \cdots \supset \cdots \supset H_s = E$$

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, $(\overline{S})$ et $(\overline{S}')$ les deux séries isomorphes qu'on en déduit par le théorème de Schreier. $(\overline{S})$ ne diffère de (S) que par des répétitions auxquelles correspondent des répétitions dans $(\overline{S}')$, 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 un théorème important :

Si un groupe admet une série de composition, il passe au moins une telle série par un sous-groupe invariant quelconque donné. 20/21

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

E.Noether, Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, Math. Ann. T.96, 1926, p.67,prg.10

La démonstration y est donnée pour les 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 décomposition, 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
21/22 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 le groupe G un sous-groupe d'ordre p^s quelque soit le nombre s $(0 \leqslant s \leqslant r)$

Nous renvoyons pour la démonstration et pour celle des théorèmes suivants au mémoire de Sylow (Math. Ann. Bd 5 S.594) ou à l'ouvrage de Speiser : Theorie der Gruppen von endlicher Ordnung (p.42).

25.– Groupes de Sylow. On appelle groupes de Sylow les sous-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 p 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
22/23 sous-groupe de G que l'on appelle 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 près.*

23/24

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

On montrera 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

$$g = ab$$

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

$$ab = a'b' \text{ entraîne } a = a' \quad b = b'$$

(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 $G = A \cdot B$ ayant le sens rappelé plus haut).

Si G est abélien et si l'opération du groupe est l'addition on dit G *somme directe* 24/25
de A et B et on écrit :

$$G = A + B$$

quand aucune confusion n'est possible.

29.– Généralisation. On généralise la notion du produit direct au cas de plusieurs facteurs en procédant 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 suivantes $(\mathcal{A})$ sont remplies :

(1) Tout A est un sous-groupe invariant de G

(2) $G = A_1 \cdot A_2 \cdot \cdots \cdot A_n$

(3) $(A_1 \cdots A_{p-1}) \cap A_p = E$ 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 $a_1, a_2, \ldots, a_n$ appartenant à $A_1, A_2, \ldots, A_n$ respectivement : $y = a_1 a_2 \cdots a_n$ et un élément quelconque d'un sous-groupe A_p est permutable avec un élément quelconque d'un autre sous-groupe $A_{p'}$:

$$a_p a_{p'} = a_{p'} a_p \qquad (p' \neq p).$$

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

$$A_p \cap B_p = E$$

25/26 et d'après le théorème d'isomorphie : $G/A_p \simeq B_p$, $G/B_p \simeq A_p$

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 $\overline{A}$ et $\overline{B}$ d'un groupe G', ce groupe G' admet un sous-groupe $\overline{G}$ isomorphe à G et qui est le produit direct de $\overline{A}$ et $\overline{B}$.

$$A \simeq \overline{A} \quad B \simeq \overline{B} \text{ entraîne } A \times B \simeq \overline{A} \times \overline{B}$$

(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 :

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

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

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

(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 par chacun de ses facteurs.

32.– Groupes complètement réductibles. On dit[18] qu'un groupe est complètement réductible s'il est le produit direct d'un nombre fini de groupes *simples* :

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

26/27 les groupes

$$\begin{aligned} G &= A_1 \times A_2 \times \cdots \times A_n \\ G_1 &= A_1 \times A_2 \times \cdots \times A_{n-1} \\ &\cdots \\ G_{n-1} &= A_1 \\ G_n &= E \end{aligned}$$

forment alors une suite de composition de longueur n dont les facteurs sont isomorphes à $A_n, A_{n-1}, \ldots, A_1$

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

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

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_p*

(3) *H est complètement réductible*

Démonstration. On a $G = A_1 A_2 \cdots A_n$ d'où

$$G = HA_1A_2 \cdots A_n \qquad (1)$$

Considérons le produit ordinaire $H_1 = HA_1$. 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_1. 27/28
Dans le premier cas on a $H_1 = H \times A_1$. Dans le second $H_1 = H$. De même, le produit H_1A_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 :

$$G = H \times A_{i_1} \times A_{i_2} \times \cdots \times A_{i_r}$$

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

$$G = H \times B \qquad H \simeq G/B \simeq A_{j_1} \times \cdots \times A_{j_s}$$

$A_{j_1}, \ldots, A_{j_s}$ étant les facteurs 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.

Notes

1. Les articles et livres cités dans cette bibliographie sont [vdW30], [Noe29], [Spe27] (en citant l'édition la plus récente, à l'époque, du livre de Speiser dont la première édition date de 1923).

Les chapitres 2 et 6 du livre [vdW30] sont respectivement intitulés *Gruppen* et *Fortsetzung des Gruppentheorie*. D'autres références sont citées dans l'exposé, le traité d'analyse de Picard [Pic28], un autre article d'Emmy Noether [Noe26] et un article de Sylow [Syl72].

2. Quelques remarques sur ces notations :

— comme il a été dit dans le chapitre 2, $\in$ coexiste avec ε, $\wedge$ avec $\cap$... Voici les notations utilisées dans les exemplaires de l'IRMA, de l'IHP, et le choix fait ici :

Strasbourg	Institut H.P.	ce texte
$\in$	ε	$\in$
$\wedge$	$\cap$	$\cap$
$\supset$	$>$	$\supset$

— la notation $\subseteq$ introduite ici n'est pas utilisée dans l'exposé
— à la fin de l'exposé, la lettre majuscule E désignera aussi l'élément neutre d'un groupe.
3. Cette définition est clairement pré-Bourbachique : un ensemble ne forme pas un groupe. Notons aussi que l'ensemble E s'appelle G dans les lignes suivantes.

Van der Waerden [vdW30] précise que E doit être non vide (mais que ceci est impliqué par l'existence d'un élément neutre (b), voir la note 8). L'unicité de e semble acquise, ainsi que celle de a^{-1}, confirmée par l'article défini.
4. La première de ces notations n'est pas utilisée dans l'exposé.
5. La plupart des notations aujourd'hui habituelles en théorie des groupes viennent de l'allemand et du livre de van der Waerden. Ici le e, voyelle assurément neutre en français, est la première lettre du mot *Einheit*, unité.
6. La ponctuation des exposés est aléatoire. Nous ne l'indiquons pas systématiquement
7. La correction indiquée ici entre crochets figure sur l'exemplaire de l'IHP (rajoutée à la main).
8. Cette fois, il faut supposer que G' n'est pas vide...
9. Le mot allemand *Index* sera traduit par *indice*, utilisé dans les exposés suivants.
10. En termes modernes, (1) dit que $a \mapsto \overline{a}$ est une application, (2) qu'elle est surjective (et (3) qu'elle respecte les lois de composition). La terminologie utilisée aujourd'hui (injective, surjective, bijective), aussi naturelle et claire semble-t-elle être, date de 1954. Auparavant (je cite un message de J-P. Serre du 3 septembre 2011) :

> Un morphisme $f : X \to Y$ était dit « biunivoque » s'il était injectif ; on disait alors que c'est un « isomorphisme dans ». On disait que f était « sur » (aucun rapport avec les « pommes sures » de Rimbaud [(1)]) s'il était surjectif. La meilleure vertu que pouvait avoir f, c'était d'être un « isomorphisme sur ». Le plus étonnant de ces termes était « biunivoque ». Il provenait d'une terminologie encore plus ancienne où certaines fonctions étaient « univoques », i.e. ne prenaient qu'une seule valeur, i.e. étaient des « fonctions » au sens actuel. Par exemple, la racine carrée était vue comme une fonction, avec le petit défaut qu'elle n'était pas univoque. [...] Le tournant a été pris par Bourbaki, à un congrès à Celles-sur-Plaine, en 1954, où nous avons décidé d'introduire la trilogie « injectif, surjectif, bijectif ». Un des premiers articles utilisant cette audacieuse innovation est FAC (cf. note de bas de page no 1) [(2)]. Je me souviens très bien de nos discussions à ce sujet : il était clair pour nous que c'était une bonne idée, mais nous nous demandions si les autres mathématiciens suivraient. Deux ou trois ans plus tard, c'était fait ; je ne crois pas qu'aucune autre innovation de Bourbaki ait eu un succès aussi universel.

1. Il s'agit bien sûr de [Rim72, *Le bateau ivre*].
2. Il s'agit bien sûr de [Ser55].

11. Les adjectifs mériédrique et holoédrique, qui appartiennent au lexique de la chimie (les rapports entre la cristallographie et la théorie des groupes sont anciens) figurent dans le *Traité des substitutions* [Jor70] de Jordan. Nous verrons (dans l'exposé 4-G) que, en mars 1937 encore, Élie Cartan les utilisait.
12. En LaTeX, les romaines sont italiques...
13. On aurait aujourd'hui un groupe Ω (le système d'opérateurs) opérant sur (l'ensemble) G, qui par ailleurs est un groupe.
14. « Idéaux des deux côtés », traduction brutale de l'allemand *zweiseitigen Idealen*, laissera rapidement la place aux moins brutaux « idéaux bilatères » dans les exposés suivants.
15. Ici N est un sous-groupe invariant et on applique le résultat à $\overline{G} = G/N$ et $\overline{A} = A/N$ (pour A invariant contenant N).
16. « Série » traduit *Reihe*, on dit plutôt aujourd'hui « suite » de décomposition. À partir d'ici, E désigne ce que nous appellerions $\{e\}$, le sous-groupe trivial.
17. Ces notations sont légèrement incohérentes, puisque les inclusions vont dans le sens inverse. D'autre part, l'exemple donné par van der Waerden $\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset V_4 \supset E$ est plus intéressant et pertinent.

Ce qui nous amène à constater qu'il y a fort peu d'exemples, dans cet exposé et dans le séminaire de cette année-là en général.
18. Il n'y a pas de paragraphe 31.

Des archives du séminaire...

Compte-rendu de la séance du 13 Novembre 1933

1. Outre les élèves et anciens élèves de l'ENS, M.Julia a autorisé MM. Wachs, Monteiro, Diamond, Aronszajn, Krasner, Wasow, à assister aux séances.

Dès 15h. régnait à l'Institut Henri Poincaré une animation inaccoutumée, en particulier à la Bibliothèque. À 16h.30 arrive[nt] M.Hadamard, puis M.Cartan qui assistent à la séance.

2. Ouverture à 16h.30. M.Julia se loue d'avoir un aussi nombreux public et lit le programme de l'année.

On fixe, après quelques observations les dates des séances aux lundis : 13 Nov. 27 Nov. 11 Déc. 8 Janv. 22 Janv. 12 Fév. 26 Fév. 12 Mars 9 Av. 25 Av. (3) 8 Mai, 25 Mai, c'est-à-dire que les deux lundis réglementaires du 25 Déc. et du 26 Mars les séances sont supprimées ; et qu'elles auront lieu tout de même le lundi gras et le lundi de Quasimodo (4). L'année sera finie le 1er Juin.

En cas d'indisponibilité du conférencier prévu, les auditeurs habitant la province seront avisés directement, les autres le seront par voie d'affiche à l'Institut Henri Poincaré.

3. C'est le 23 avril 1934 qui était un lundi. Magnier va reproduire l'erreur dans la circulaire suivante.

4. Pâques était, en 1934, le 1er avril. Le lundi de Quasimodo, deuxième lundi après Pâques, était donc le 9 avril. Le lundi gras était le 12 février. Ces dates furent rapidement modifiées, et en particulier il n'y eut pas d'exposé le lundi gras. Voir les archives à la fin de l'exposé 1-E.

3. La parole est donnée à DUBREIL qui, en une heure, expose la Théorie des Groupes.

4. À la fin de l'exposé, M.Hadamard pose une question sur les Groupes de Sylow. Une réponse satisfaisante lui est donnée.

5. M.Julia remercie l'Orateur d'avoir compris la façon dont ces exposés devaient être faits : ils doivent servir de canevas pour un travail personnel et non être une exposition détaillée qui d'ailleurs serait impossible faute de temps. Il prévient que les exposés suivants seront aussi rapides et nourris.

6. Thé, aimablement servis par Mmes DUBREIL et CHEVALLEY. Les conversation s'engagent. On annonce que le deuxième exposé sera fait par Chevalley ou Marty et non par Weil. Arrivée (mieux vaut tard que jamais) de Coulomb. La séance est levée à 18h.15 (5).

Séminaire de mathématiques
Avis

[manuscrit] 19 Nov. 1933

1. Les auditeurs sont priés de donner leurs nom et adresse à MAGNIER ; ceux qui habitent la province et veulent être prévenus en cas de changement de programme sont particulièrement visés.

2. La cotisation – 50 Frs – est payable le lundi 25 Novembre (6) à Magnier.

3. Le 2ème exposé (Modules) sera fait par M.MARTY et non par M.WEIL.

4. Extrait du Compte-rendu de la première séance : les *douze* séances auront lieu les 13 & 25 Nov., 11 Déc., 8 & 22 Janv. 12& 26 Fév. 12 Mars 9 & 25 Avril, 8 & 22 Mai soit tous les deuxièmes et quatrièmes lundis du mois du 1er Novembre au 1er Juin les jours *officiels* de congé étant seuls exclus (7).

Références

[Jor70] C. Jordan – *Traité des substitutions et des équations algébriques*, Gauthier-Villars, 1870.

[Noe26] E. Noether – « Abstrakter Aufbau der Idealtheorie in algebraischen Zahl und Funktionenkörpern. », *Math. Ann.* **96** (1926), p. 26–61 (German).

[Noe29] ———, « Hyperkomplexe Größen und Darstellungstheorie. », *Math. Z.* **30** (1929), p. 641–692.

---

5. Deux pages ronéotées. Archives de l'IHP.

6. C'est du lundi 27 novembre qu'il est question. Pas plus que le 25 avril 1934, le 25 novembre 1933 n'était un lundi.

7. Une page ronéotée. Archives de l'IHP.

[Pic28] E. Picard – *Traité d'analyse. T. III. 3 éd.*, Paris : Gauthier-Villars. IX, 1928.

[Rim72] A. Rimbaud – *Poésies,* in *Œuvres complètes*, Bibliothèque de la Pléiade, Gallimard, Paris, 1972.

[Ser55] J.-P. Serre – « Faisceaux algébriques cohérents », *Ann. of Math. (2)* **61** (1955), p. 197–278.

[Spe27] A. Speiser – *Die Theorie der Gruppen von endlicher Ordnung*, Grundlehren der mathematischen Wissenschaften, Springer-Verlag, Berlin, 1927, 2. Auflag.

[Syl72] L. Sylow – « Théorèmes sur les groupes de substitutions », *Math. Ann.* **5** (1872), p. 584–594.

[vdW30] B. van der Waerden – *Moderne Algebra*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, Springer, 1930.