

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

HELMUT WIELANDT

Sur la structure des groupes composés

Séminaire Dubreil. Algèbre et théorie des nombres, tome 17, n° 2 (1963-1964), exp. n° 17,
p. 1-10

http://www.numdam.org/item?id=SD_1963-1964__17_2_A5_0

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1963-1964, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR LA STRUCTURE DES GROUPES COMPOSÉS

par Helmut WIELANDT

1. Introduction.

Un groupe G , différent du groupe unité $\{1\}$, est dit composé s'il possède un sous-groupe normal propre $G_1 \neq \{1\}$: $G \triangleright G_1 \supset \{1\}$; dans le cas contraire on dit que G est simple.

Dans un groupe composé G , il existe des suites normales finies

$$1.1 \quad G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{n-1} \triangleright G_n \triangleright \dots \triangleright G_N = \{1\};$$

ce sont des suites de sous-groupes, strictement décroissantes, dans lesquelles chaque terme est un sous-groupe normal propre du précédent. Une suite normale 1.1, telle qu'il n'existe aucune suite normale distincte de 1.1 et plus fine que 1.1, est appelée une suite de composition de G ; dans ce cas, les groupes-quotients

$$1.2 \quad G^n = G_{n-1}/G_n \quad (n = 1, \dots, N),$$

sont simples et, d'après le théorème de Jordan-Hölder, ils sont parfaitement déterminés par G , à l'ordre des termes et à des isomorphismes près; on les appelle les facteurs de composition de G .

Si l'ordre $|G|$ d'un groupe $G \neq 1$ est fini, condition que nous supposons toujours vérifiée, sauf au paragraphe 3, ce groupe possède une suite de composition.

HÖLDER avait déjà établi le plan d'études suivant: Déterminer d'abord les groupes simples, puis construire les groupes composés, à l'aide de leurs facteurs de composition.

Sur l'état actuel de la première partie de ce programme, je ne dirai qu'un mot. Il y a deux types essentiellement différents de groupes simples. Les groupes G du premier type sont triviaux, en tant qu'ils ne possèdent pas de sous-groupes, autres que G et $\{1\}$; ce sont les groupes d'ordre premier. Quant aux groupes simples non triviaux, on sait, d'après BURNSIDE, que leur ordre contient, au moins, trois facteurs premiers différents, et, d'après un théorème récent de FEIT et THOMPSON, que leur ordre est pair. L'étude complète des groupes simples non triviaux n'est pas encore terminée, mais on travaille actuellement, de façon intensive, à ce problème fondamental de la théorie des groupes finis. A vrai dire, sa solution ne permettra

pas encore de regarder comme achevée la théorie des groupes finis. Car on se trouvera alors, dans l'étude des groupes composés, exactement au point où l'on était à l'origine de la théorie des groupes résolubles (dont les facteurs de composition sont tous triviaux), puisque la structure des groupes simples triviaux était connue d'avance ; et cependant, la théorie des groupes résolubles s'est développée en un domaine très ramifié qui continue à progresser d'une façon rapide. Après la détermination de tous les groupes simples finis, la théorie des groupes composés constituera donc encore un large cercle de problèmes. Elle devra en particulier obtenir, connaissant la structure des facteurs de composition G^n , des conclusions sur la structure du groupe G lui-même.

Le mot "structure" exige des éclaircissements. Nous traiterons seulement de la "structure de la famille des sous-groupes" d'un groupe. Le problème fondamental est le suivant : Déterminer tous les sous-groupes d'un groupe donné et les relations d'inclusion entre eux. Ce problème, à vrai dire, est si vaste que l'on doit se borner à des sous-groupes importants. Jusqu'à présent, en théorie des groupes finis, deux sortes de sous-groupes importants se sont révélées ; les uns sont les sous-groupes qui figurent dans une suite de composition du groupe donné ; les autres sont les sous-groupes dont l'ordre se distingue par des propriétés extrémales de nature arithmétique.

Nous parlerons, tout d'abord, de la structure normale des groupes, et ensuite de leur structure arithmétique.

2. Structure normale d'un groupe fini.

Nous dirons qu'un sous-groupe d'un groupe G est sous-normal s'il figure au moins dans une suite normale de G .

Un sous-groupe normal est, en particulier, sous-normal.

Nous noterons \underline{SG} l'ensemble des sous-groupes sous-normaux de G . L'ensemble \underline{SG} est un sous-treillis du treillis des sous-groupes de G ; c'est-à-dire que, si l'on désigne par $H \cap K$ l'intersection de deux sous-groupes H et K de G , et par $H \cup K$ le sous-groupe de G qu'ils engendrent, on a [8] :

2.1 Si T et $V \in \underline{SG}$, alors $T \cap V$ et $T \cup V \in \underline{SG}$.

Par structure normale du groupe G , on entend la structure du treillis \underline{SG} . Cette structure est d'autant plus claire que G a moins de facteurs de composition triviaux. S'il n'y en a pas, alors \underline{SG} est distributif :

2.2 Si G n'a pas de facteurs de composition triviaux, on a :

$$T \cap (U \cup V) = (T \cap U) \cup (T \cap V) \quad \text{pour } T, U \text{ et } V \in \underline{SG}.$$

Le treillis \underline{SG} est modulaire si et seulement si, quels que soient les sous-groupes sous-normaux T et U de G , on a

$$TU = UT.$$

Or, constatation surprenante, la permutabilité de deux sous-groupes sous-normaux est très fréquente ; c'est même presque la règle, [9] :

2.3 Soient $T, U \in \underline{SG}$. Ou bien $TU = UT$, ou bien il existe un nombre premier p et des sous-groupes normaux T_1 de T et U_1 de U tels que les indices $[T:T_1]$ et $[U:U_1]$ sont tous les deux égaux à p .

Des énoncés plus fins, dans cette direction, ont été trouvés par HAINZL [2].

Le théorème 2.3 laissait prévoir que le treillis \underline{SG} est, dans tous les cas, "presque modulaire". TAMASCHKE a réussi à exprimer cette notion en termes de treillis ([7], Satz 2.4). Il donne, de cette manière, des conditions nécessaires pour que, étant donné un treillis abstrait, il existe un treillis sous-normal \underline{SG} qui lui soit isomorphe ; on ne connaît pas encore de conditions, à la fois nécessaires et suffisantes, pour qu'il en soit ainsi.

3. Sous-groupes sous-normaux des groupes infinis.

On démontre facilement que l'intersection d'une famille de sous-groupes sous-normaux d'un groupe infini G est encore un sous-groupe sous-normal, dès qu'il existe un nombre N tel que tous les membres de la famille apparaissent dans des suites normales de G de longueur $\leq N$. En particulier, l'intersection $T \cap U$ de deux sous-groupes T et U sous-normaux est toujours sous-normale. Si l'ensemble ordonné \underline{SG} vérifie la condition maximale, le groupe engendré par une famille arbitraire de sous-groupes sous-normaux de G est encore sous-normal [8]. Mais, si \underline{SG} ne vérifie pas la condition maximale, le groupe $T \cup U$, engendré par deux sous-groupes sous-normaux T et U , n'est pas nécessairement sous-normal, ainsi que l'a montré ZASSENHAUS en 1958 ([11], Appendix D, Exercise 23). Ces derniers temps, ROSEBLADE et ROBINSON ont étudié des conditions sous lesquelles la sous-normalité de T et de U entraîne celle de $T \cup U$. Je mentionne, ici, un théorème de ROSEBLADE [6] :

3.1 Les sous-groupes sous-normaux T d'un groupe G pour lesquels l'ensemble ordonné \underline{ST} vérifie la condition minimale, forment un sous-treillis du treillis des sous-groupes.

Pour que \underline{SG} soit un treillis, il suffit donc aussi que \underline{SG} vérifie la condition

minimale.

On ne connaît pas encore de conditions de chaîne plus faibles que la condition maximale et que la condition minimale et qui entraîne encore que \underline{SG} est un sous-treillis du treillis de tous les sous-groupes.

Un autre résultat remarquable est dû à BAER [1] :

3.2 Dans tout groupe G , les éléments qui engendrent un sous-groupe cyclique sous-normal forment un sous-groupe caractéristique.

A un autre point de vue, les sous-groupes sous-normaux des groupes infinis se comportent de façon étonnamment "normale". Par exemple, le résultat connu qui s'énonce : "Si deux sous-groupes normaux ont pour intersection le sous-groupe unité, tout élément de l'un commute avec tout élément de l'autre", s'étend, de la manière suivante, aux sous-groupes sous-normaux :

3.3 Soient T et $U \in \underline{SG}$. Si $T \cap U = \{1\}$, ou bien chaque élément de T commute avec chaque élément de U , ou bien il existe un nombre premier p et des groupes

$$T_1 \triangleleft T_0 \in \underline{ST} \quad \text{et} \quad U_1 \triangleleft U_0 \in \underline{SU}$$

tels que

$$p = (T_0:T_1) = (U_0:U_1) .$$

Ce théorème pourrait avoir quelque utilité pour généraliser aux groupes infinis les théorèmes 2.2 et 2.3.

Signalons enfin une question intéressante, de nature générale : Existe-t-il, dans tout groupe $G \neq \{1\}$, deux sous-groupes sous-normaux G_1 et G_0 tels que $G_1 \triangleleft G_0$ et que G_0/G_1 soit simple ?

Revenons maintenant à l'étude des groupes finis.

4. Structure arithmétique.

La structure arithmétique d'un groupe G est décrite par des théorèmes sur les propriétés des sous-groupes de G , relatives à des nombres premiers donnés. Le théorème classique de ce type est dû à SYLOW (1871) :

4.1 Soit p^a la plus grande puissance de p qui divise $|G|$; alors, G possède des sous-groupes G_p tels que

$$(i) |G_p| = p^a ;$$

(ii) Si H est un sous-groupe de G dont l'ordre est une puissance de p , il existe un élément $g \in G$ tel que $H \subseteq g^{-1} G_p g$.

P. HALL a montré, en 1937, que ce théorème, moyennant des hypothèses convenables, peut s'étendre à la considération simultanée de plusieurs nombres premiers. Soit P un ensemble de nombres premiers. Pour chaque nombre naturel m , on désigne par m_p le plus grand diviseur de m dont tous les facteurs premiers appartiennent à P . Alors, le théorème de Hall [3], s'énonce de la manière suivante :

4.2 Si G est un groupe résoluble, G possède au moins un sous-groupe G_p possédant les deux propriétés suivantes :

$$(i) |G_p| = |G|_p ;$$

(ii) Si H est un sous-groupe de G tel que tous les facteurs premiers de $|H|$ appartiennent à P , il existe un élément $g \in G$ tel que $H \subseteq g^{-1} G_p g$.

Les tentatives pour étendre ce résultat à des groupes non résolubles ont donné lieu à une vaste théorie, que nous résumons brièvement au paragraphe suivant.

5. Groupes de Hall.

Soient P un ensemble de nombres premiers et G un groupe fini. On appelle P -groupe de Hall de G un sous-groupe de G , d'ordre $|G|_p$. On désigne par HPG l'ensemble des P -groupes de Hall de G .

D'après 4.2, si G est résoluble, l'ensemble HPG n'est pas vide.

Pour un groupe G non résoluble, le théorème 4.2 n'est pas valable ; l'ensemble HPG peut être vide (ce qui a lieu, par exemple, lorsque G est le groupe alterné de degré 5 et lorsque $P = \{3,5\}$) ; si HPG n'est pas vide, la condition 4.2(ii) peut ne pas être vérifiée (c'est le cas, pour le groupe alterné de degré 5, lorsque $P = \{2,3\}$).

Mais, à un autre point de vue, les groupes de Hall sont très agréables : ils se comportent bien vis-à-vis de la structure normale de G .

On a, de façon précise, le théorème suivant [10] :

5.1. (i) Si $A \in \text{HPG}$ et si $T \in \text{SG}$, alors $A \cap T \in \text{HPT}$;

(ii) Si A est un élément fixe de HPG et si T décrit SG, alors $A \cap T \in \text{SA}$ et l'application $T \rightarrow A \cap T$ de SG dans SA est un homomorphisme de treillis ; c'est-à-dire que

$$1^\circ A \cap (T_1 \cap T_2) = (A \cap T_1) \cap (A \cap T_2)$$

$$2^\circ A \cap (T_1 \cup T_2) = (A \cap T_1) \cup (A \cap T_2)$$

quels que soient T_1 et $T_2 \in \underline{SG}$; bien entendu, seule la relation 2° n'est pas triviale, et utilise le fait que A appartient à \underline{HPG} (rappelons aussi que $T_1 \cup T_2$ est le sous-groupe de G engendré par T_1 et T_2).

Relativement au problème de l'existence des groupes de Hall dans les groupes composés, on connaît d'après ČUNIHIN et, surtout, d'après P. HALL [5], une série de théorèmes du type suivant :

"Si chaque facteur de composition G^n contient un P-groupe de Hall qui possède une certaine propriété E , alors G contient un P-groupe de Hall qui possède une autre propriété E'' ".

Malheureusement, dans ces théorèmes, la propriété E' est toujours plus faible que la propriété E . Et cette théorie paraît laisser encore plus à désirer lorsqu'on se propose de sortir du domaine des groupes résolubles et de faire une étude tout à fait générale.

HALL avait démontré, en 1937, qu'il existe, pour chaque groupe non résoluble G , au moins un ensemble de nombres premiers P tels que \underline{HPG} est vide [4]. Par rapport à un tel ensemble P , les théorèmes précédemment énoncés ne permettent de connaître aucune propriété de G . Pour créer une théorie réellement générale, on doit donc remplacer les groupes de Hall par une autre classe de sous-groupes doués de propriétés arithmétiques, classe qui ne soit jamais vide. C'est ce qu'on peut faire d'une façon qui s'applique aussi aux groupes infinis.

6. P-sous-groupes maximaux.

La grande importance des théorèmes de Sylow, 4.1, et de Hall, 4.2, provient du fait que, sous certaines hypothèses, ils procurent une vue générale sur l'ensemble \underline{PG} des P-sous-groupes de G , un P-sous-groupe étant un sous-groupe dont l'ordre n'est divisible que par des nombres premiers appartenant à P . Obtenir une telle vue générale pour un groupe G quelconque est un but essentiel de la structure arithmétique.

Naturellement, on doit, ici aussi, se restreindre encore à l'étude des P-sous-groupes importants. Quels sont ceux-ci résulte du théorème de Lagrange d'après lequel l'ordre d'un sous-groupe divise l'ordre du groupe. Par suite, tout sous-groupe d'un P-sous-groupe de G est lui-même un P-sous-groupe de G . Si l'on connaît

l'ensemble \underline{MPG} des P-sous-groupes maximaux de G , on en déduit tous les P-sous-groupes de G .

Le problème se simplifie encore par la remarque suivante : Si $A \in \underline{MPG}$ et si $g \in G$, alors $g^{-1}Ag \in \underline{MPG}$. On en déduit que \underline{MPG} est la réunion d'une ou plusieurs classes de sous-groupes conjugués de G

$$\underline{MPG} = M_1 + M_2 + \dots + M_c \quad \text{où } c = c_P(G) \geq 1.$$

Lorsque le nombre de classes c est égal à 1, il suffit de connaître un seul P-sous-groupe maximal A de G pour obtenir tous les P-sous-groupes H de G comme sous-groupes d'un groupe conjugué de A .

Le théorème de Sylow entraîne

6.1 On a $c_P(G) = 1$ pour tous les groupes G , si et seulement si $|P| = 1$.

Les théorèmes de Hall ([3], [4]) s'énoncent de la manière suivante :

6.2 On a $c_P(G) = 1$ pour tous les ensembles de nombres premiers P , si et seulement si G est résoluble.

Ce dernier théorème indique une relation générale entre les nombres $c_P(G^n)$ de classes des facteurs de composition G^n de G et le nombre $c_P(G)$ de classes de G , pour un même ensemble P ; en effet, d'après le résultat de HALL, on a, si G est résoluble, $c_P(G^n) = 1$ pour chaque facteur de composition G^n et pour tous les P . Mais, jusqu'à présent, on sait seulement que les P-sous-groupes maximaux se comportent, vis-à-vis de la structure normale beaucoup moins bien que ne le font les groupes de Hall. Déjà le résultat 5.1 (i) ne s'étend pas; l'intersection d'un P-sous-groupe maximal de G avec un sous-groupe normal N de G n'est pas nécessairement un P-sous-groupe maximal de N (L'exemple le plus simple est celui du groupe $PGL(2,7)$ d'ordre 2.168, avec $P = \{2,3\}$). C'est probablement à cause de cet obstacle que, jusqu'à maintenant, rien n'a été publié pour constituer une théorie des P-sous-groupes maximaux. Après de longues recherches, je suis arrivé à en établir une. Elle repose sur les idées suivantes.

7. Projection.

Soient A un sous-groupe quelconque et $\{G_n\}$ une suite normale de G ; A définit, univoquement, dans chaque facteur G^n un sous-groupe (que nous appellerons projection de A dans G^n et que nous noterons $A \uparrow G^n$) de la manière suivante :

$$7.1 \quad A \uparrow G^n = \frac{(A \cap G_{n-1})G_n}{G_n} \quad (n = 1, 2, \dots, N).$$

Ce sous-groupe de G^n est formé des classes résiduelles de G_{n-1} modulo G_n qui contiennent au moins un élément de A .

En posant $|A \uparrow G^n| = [(A \cap G_{n-1}) : (A \cap G_n)]$, on a :

$$7.2 \quad |A| = \prod_n |A \uparrow G^n| .$$

Cette formule montre que les projections $A \uparrow G^n$ se prêtent à l'étude arithmétique du sous-groupe A . On constate facilement que :

7.3 (i) Le sous-groupe A appartient à \underline{PG} , si et seulement si $A \uparrow G^n$ appartient à \underline{PG}^n , quel que soit n ;

(ii) Le sous-groupe A appartient à \underline{HPG} si et seulement si $A \uparrow G^n$ appartient à \underline{HPG}^n quel que soit n ;

(iii) Si $A \uparrow G^n$ appartient à \underline{MPG}^n , quel que soit n , alors le sous-groupe A appartient à \underline{MPG} .

La réciproque de 7.3 (iii) n'est pas vraie en général, comme le prouve l'exemple du groupe $\text{PGL}(2,7)$.

Un problème se présente : Jusqu'à quel point un sous-groupe A de G est-il déterminé par ses projections dans les facteurs G^n d'une suite normale 1.1 donnée de G ? Si, pour deux sous-groupes A et B de G , on a

$$A \uparrow G^n = B \uparrow G^n \quad \text{quel que soit } n ,$$

alors on a, d'après 7.2, $|A| = |B|$. Mais, contrairement à ce qu'on pourrait croire, les sous-groupes A et B ne sont pas toujours isomorphes, comme le montrent des contre-exemples. Cependant, il existe un cas important dans lequel on a même une propriété plus forte. Définissons l'ensemble \underline{LPG} de sous-groupes de G de la manière suivante :

$$7.4 \quad A \in \underline{LPG} \iff \{A \in \underline{PG} ; A \trianglelefteq B \in \underline{PG} \text{ entraînent } A = B\} .$$

Alors, à l'aide du théorème de Feit et Thompson, on prouve le résultat suivant :

7.5 Si $A \uparrow G^n = B \uparrow G^n \in \underline{LPG}^n$ pour tous les n , il existe un élément s de $A \cup B$ tel que $A = s^{-1}Bs$.

Pour étudier à quelle condition deux P -sous-groupes maximaux A et B de G sont conjugués, ce théorème, à vrai dire, ne suffit pas car l'hypothèse $A \uparrow G^n \in \underline{LPG}^n$ ne sera pas satisfaite, en général.

En outre, la classe \underline{LPG} joue aussi un rôle important dans l'étude de l'existence

d'un sous-groupe A ayant des projections données :

7.6 Soit $\{G_n\}$ une suite normale de G dans laquelle chaque terme est un sous-groupe caractéristique du précédent. Pour chaque n , soit A^n un élément de LPG^n . Si chaque P -groupe d'automorphismes de G^n laisse la classe des sous-groupes conjugués de A^n dans G^n globalement fixe, alors G contient un sous-groupe A tel que $A \cap G^n = A^n$ quel que soit n .

8. Propriétés de conjugaison des P -sous-groupes maximaux.

Une remarque très récente dans cette question centrale de la théorie arithmétique est que la conjecture de Schreier permet d'avancer dans l'étude des groupes composés. Cette conjecture s'énonce de la manière suivante : "Soient F un groupe fini simple, $\text{Aut } F$ le groupe des automorphismes de F et $\text{Inn } F$ le groupe des automorphismes intérieurs de F ; alors, le groupe quotient $\text{Aut } F / \text{Inn } F$ est résoluble". Elle est vraie pour les groupes simples triviaux et bien vérifiée empiriquement pour les groupes simples non triviaux. Si on la suppose vérifiée par tous les groupes simples F qui sont facteurs de composition de sous-groupes de G , on peut énoncer le théorème suivant :

8.1 Si $A \in \text{MPG}$ et si $N \triangleleft G$, on a $A \cap N \in \text{LPN}$.

Puisque 1 n'appartient à LPN que si l'ordre de N ne possède pas de facteurs premiers appartenant à P , il résulte de 8.1 que l'on a $A \cap N \neq 1$ dès que $|N|_P \neq 1$ et $1 \neq A \in \text{MPG}$. En appliquant un raisonnement par induction, on démontre ainsi que :

8.2 Soient A et B deux P -sous-groupes maximaux de G qui ont mêmes projections dans chaque facteur non trivial d'une suite de composition de G . Alors, A et B sont conjugués dans le sous-groupe de G qu'ils engendrent.

Le théorème fondamental de Hall d'après lequel deux P -sous-groupes maximaux d'un groupe résoluble sont conjugués, est un cas particulier de 8.2, car dans un groupe résoluble, il n'y a pas de facteur de composition non trivial.

Si l'on remplace, dans les théorèmes 8.1 et 8.2, l'ensemble MPG des P -sous-groupes maximaux de G , par l'ensemble des P -sous-groupes résolubles maximaux, ces théorèmes sont valables sans recours à la conjecture de Schreier.

BIBLIOGRAPHIE

- [1] BAER (R.). - Nilgruppen, Math. Z., t. 62, 1955, p. 402-437.
 - [2] HAINZL (J.). - Über Seminormalität in Gruppen und Verbänden, Math. Z., t. 80, 1963, p. 358-362.
 - [3] HALL (P.). - A note on soluble groups, J. Lond. math. Soc., t. 3, 1928, p. 98-105.
 - [4] HALL (P.). - A characteristic property of soluble groups, J. Lond. math. Soc., t. 12, 1937, p. 198-200.
 - [5] HALL (P.). - Theorems like Sylow's, Proc. Lond. math. Soc., Series 3, t. 6, 1956, p. 286-304.
 - [6] ROSEBLADE (J. E.). - Two subnormal coalition classes, J. Lond. math. Soc. (à paraître).
 - [7] TAMASCHKE (O.). - Die Kongruenzrelationen im Verband der zugänglichen Subnormalteiler, Math. Z., t. 75, 1961, p. 115-126.
 - [8] WIELANDT (H.). - Eine Verallgemeinerung der invarianten Untergruppen, Math. Z., t. 45, 1939, p. 209-244.
 - [9] WIELANDT (H.). - Vertauschbare nachinvariante Untergruppen, Abh. math. Sem. Univ. Hamburg, t. 21, 1957, p. 55-62.
 - [10] WIELANDT (H.). - Sylowtürme in subnormalen Untergruppen, Math. Z., t. 73, 1960, p. 386-392.
 - [11] ZASSENHAUS (H.). The theory of groups, 2nd edition. - Göttingen, Vandenhoeck und Ruprecht ; New York, Chelsea, 1958.
-