SOCIÉTÉ MATHÉMATIQUE SUISSE

Frühjahrssitzung in Bern, 30. 5. 65

Herr Prof. Dr. R. Brauer (Harvard University) hält einen Vortrag über „Einige neuere Entwicklungen in der Theorie der endlichen Gruppen (Bericht)".

Jahresversammlung in Genf, 25. 9. 65

An der Jahresversammlung werden neun wissenschaftliche Mitteilungen vorgelegt, die untenstehend entweder durch Titel oder durch Auszug angeführt sind:

Sophie PICCARD (Neuchâtel): Les groupes libres et quasi-libres modulo n. Des théorèmes d'existence.

Jules CHUARD (Lausanne): Réseaux cubiques tracés sur une sphère.

André AMMANN (Yverdon): Fibrations cycliques d'un espace fibré circulaire cycliquement partitionné.

Cécile TANNER (Londres): L'algèbre de Thomas Harriot (1560-1621).

M. A. KNUS (Zürich): Algèbres graduées et algèbres filtrées.

Urs STAMMBACH (Zürich): Homologische Methoden in der Gruppentheorie.

François SIGRIST (Zürich): Obstruction et transgression.

Georges LERESCHE (Neuchâtel): Algèbres d'opérateurs non bornés sur l'espace d'Hilbert.

Jean-Claude HOLY (Genève): Sur l'ensemble des valeurs stationnaires d'une application différentiable.

Herr Prof. H. Debrunner (Bern) hielt einen Hauptvortrag über „Aspekte der Knotentheorie".

Sophie PICCARD (Neuchâtel): *Les groupes libres modulo n. Les groupes quasi libres modulo n. Théorèmes d'existence.*

Le présent travail se place dans le cadre de l'étude générale suivante:

1. Rechercher les caractères qui peuvent être communs à toutes les relations reliant un ensemble de générateurs d'un groupe multiplicatif.
2. Etant donné un ensemble de propriétés qui peuvent être communes à toutes les relations reliant les éléments d'un ensemble de générateurs d'un groupe multiplicatif, étudier la classe de groupes dont chacun possède au moins un ensemble de générateurs, tel que toute relation qui les lie possède les propriétés données. Six classes de groupes ont été découvertes et étudiées par cette voie: ce sont les groupes libres, quasi libres, pseudo-libres et les groupes libres, quasi libres et pseudo-libres modulo n, où n est un entier $\geqq 2$ donné.

Un groupe multiplicatif G est appelé *libre modulo n* s'il possède au moins un ensemble A de générateurs — dits libres modulo n — qui ne sont liés que par des relations triviales modulo n, c'est-à-dire par des relations de la forme $f(a_1, \ldots, a_k) = 1$ où 1 est l'élément neutre de G et f est une composition finie des éléments du sous-ensemble $A^* = \{a_1, \ldots, a_k\}$ de A, totalement réductible modulo n (rappelons que la réduction modulo n d'un produit de puissances entières d'éléments de A^* consiste à effectuer alternativement et aussi longtemps que possible l'une ou l'autre des deux opérations élémentaires suivantes: 1. Réduction, par le seul jeu des axiomes de groupe multiplicatif, du produit considéré à la forme 1) $a_{u_1}^{v_1} \ldots a_{u_l}^{v_l}$, où $a_{u_s} \in A^*$, $s = 1, \ldots, l$, $a_{u_s} \neq a_{u_{s+1}}$, $s = 1, \ldots, l-1$, et où v_s est un entier non nul quel que soit $s = 1, \ldots, l$. 2. Réduction, dans un produit de la forme 1), de tous les exposants modulo n. Après un nombre fini d'opérations de ce genre, on tombe soit sur un reste qui est $= 1$, auquel cas le produit considéré est dit *totalement réductible modulo n*, soit sur un reste de la forme 1) où $l \geqq 1$ et où $v_1, \ldots, v_l$ sont des entiers compris entre 1 et n—1. Les groupes libres modulo n ont été découverts en 1964. Ils constituent une vaste classe de groupes, dont les groupes libres ne sont qu'un cas très particulier.

Un groupe multiplicatif G est dit *quasi libre modulo n* s'il possède au moins un ensemble de générateurs quasi libres modulo n qui ne sont liés que par des relations *quasi triviales modulo n*, c'est-à-dire par des relations de la forme $f(a_1, \ldots, a_k) = 1$, où f est une composition finie d'éléments de A, de degré $\equiv 0 \pmod{n}$ par rapport à chacun d'eux.

Soit G un groupe quasi libre modulo n et soit A un ensemble donné de générateurs quasi libres modulo n de G. Tout élément de A

est soit d'ordre infini, soit d'ordre fini multiple de n. Tout élément de G possède un degré fixe modulo n par rapport à tout élément de A et on peut répartir les éléments de G en classes d'équivalence $M^{(n)}$, en prenant dans une classe $M^{(n)}$ deux éléments de G dans le cas et ce cas seulement où ils sont du même degré modulo n par rapport à tout élément de A.

On peut munir l'ensemble des classes $M^{(n)}$ d'une structure de groupe abélien en appelant produit de deux telles classes ${}_1M^{(n)}$ et ${}_2M^{(n)}$ l'ensemble des éléments ab de G, tels que $a \in {}_1M^{(n)}$ et $b \in {}_2M^{(n)}$. Avec cette loi de composition, l'ensemble $\Gamma^{(n)}$ des classes $M^{(n)}$ est un groupe abélien associé à G. Quel que soit le sous-groupe γ de $\Gamma^{(n)}$, la réunion des classes $M^{(n)}$ qui constitue les éléments de γ est un sous-groupe invariant de G. Les classes $M^{(n)}$ ont un caractère intrinsèque, indépendant de l'ensemble de générateurs A à partir duquel elles ont été définies. Tout groupe quasi libre modulo n est *fondamental* et tout ensemble A de générateurs quasi libres modulo n de G est un ensemble irréductible de générateurs de G.

Un groupe libre modulo n non cyclique n'est pas abélien.

Tout groupe libre modulo n est quasi libre modulo n et par suite il jouit de toutes les propriétés d'un groupe quasi libre modulo n. Mais tout groupe quasi libre n'est pas libre modulo n.

Soit maintenant G un groupe libre modulo n et soit A un ensemble de générateurs libres modulo n de ce groupe.

Tout élément de G possède un reste fixe r modulo n et on peut répartir les éléments de G en classes C_r en prenant dans une même classe C deux éléments de G dans le cas et dans ce cas seulement où ils ont le même reste r modulo n. Les classes C_r munies de la même loi de composition que les classes $M^{(n)}$ forment un groupe G_c qui n'est, en général, pas abélien, mais qui jouit de cette propriété que quel que soit le sous-groupe g_c de G_c, la réunion des classes C_r qui forment le groupe g_c est un sous-groupe de G. L'élément neutre du groupe G_c est la classe C_1 formée de tous les éléments de G qui sont représentés par des compositions finies d'éléments de A totalement réductibles modulo n. C_1 est un sous-groupe invariant de G. Le groupe G_c est indépendant de A. Deux éléments a et b de G sont dits *symétriques modulo n*, si leur produit $ab = c \in C_1$. Un sous-groupe g de G est dit *invariant modulo n* si $agb = g$ quel que soit le couple a, b d'éléments de G symétriques modulo n. C_1 et G lui-même sont des sous-groupes invariants modulo n de G. Il en est de même de la réunion des classes C qui forment un sous-groupe de n. Mais $\{ 1 \}$ ne l'est en général pas. L'ensemble des sous-groupes invariants modulo n d'un groupe libre modulo n forme un treillis avec les deux lois de treillis: intersection et union. On appelle *automorphisme modulo n du groupe G* toute application $\mathscr{A}^{(n)}$ de G sur lui-même qui détermine un isomorphisme du groupe G/C_1. Dans tout automorphisme modulo n, la classe C_1 est appliquée

sur elle-même de façon binumivoque et au produit de deux éléments de G correspond toujours le produit de leurs images multiplié par un élément de C_1. Quel que soit le couple a, b d'éléments, symétriques modulo n de G, l'application $\mathscr{A}_i^{(n)}$ qui fait passer de tout élément d de G à adb est un automorphisme modulo n dit *automorphisme intérieur modulo n*. L'ensemble de tous les automorphismes modulo n d'un groupe libre modulo n est un groupe dont l'ensemble de tous les automorphismes intérieurs modulo n est un sous-groupe. Tout automorphisme de G est aussi un automorphisme modulo n et tout automorphisme intérieur est aussi un automorphisme intérieur modulo n.

On appelle endomorphisme modulo n de G une application $\mathscr{E}^{(n)}$ de G dans G qui détermine un endomorphisme du groupe G/C_1. Dans tout endomorphisme mod n la classe C_1 est appliquée sur elle-même.

Un sous-groupe g de G est dit *caractéristique modulo n* s'il est transformé en lui-même par tous les automorphismes modulo n de G. En particulier, C_1 et G sont de tels sous-groupes de G. Un automorphisme modulo n ne transforme pas nécessairement un ensemble de générateurs libres modulo n en un ensemble du même type: l'ensemble des images peut même ne pas engendrer G. Un groupe G libre modulo n est dit élémentaire s'il possède au moins un ensemble $A \cup B$ de générateurs liés par les seules relations caractéristiques $b^n = 1$, quel que soit b G B. Si $B = \emptyset$, G est libre et tout groupe libre est un groupe libre modulo n élémentaire. Un groupe libre modulo n élémentaire est le produit libre des groupes cycliques engendrés par les éléments de l'ensemble $A \cup B$. Il est indépendant de la nature de ses éléments et tout groupe libre modulo n est entièrement caractérisé par un couple ordonné $\mathfrak{m}$ $\mathfrak{n}$ qui sont les cardinaux des ensembles A et B. Pour tout couple ordonné $\mathfrak{m}$, $\mathfrak{n}$ de nombres cardinaux, il existe un groupe libre modulo n élémentaire dont ils sont les caractéristiques. Si n est premier, tout sous-groupe d'un groupe libre mod. n élémentaire est aussi libre mod. n et élémentaire. Mais il existe une infinité de groupes libres modulo n non élémentaires et qui ne sont pas les produits libres des groupes cycliques engendrés par les éléments d'un ensemble quelconque A de générateurs libres modulo n. Tel est, par exemple, le groupe $G(a, b)$ libre modulo 2 de transformations des entiers qui est engendré par les deux cycles infinis $a = (\ldots -3, -2, -1, 0, 1, 2, 3, \ldots)$ et $b = (\ldots, 3, 4, 1, 2, -1, -2, -3, -4, \ldots)$ qui sont deux générateurs libres modulo 2 de $g(a, b)$ liés par une infinité de relations non triviales, parmi lesquelles $(a^{2h} b^{2h})^{h+1} = 1$, quel que soit l'entier h. Ce dernier groupe possède des sous-groupes non fondamentaux, donc non libres modulo n, par exemple le sous-groupe γ de toutes les substitutions d'un nombre fini quelconque d'entiers quelconques. Il existe un groupe libre modulo n engendré par deux générateurs a et b, libres modulo 2 et qui sont liés par la seule relation caractéristique $a^2 b^2 = 1$. Pour tout nombre cardinal $\mathfrak{m}$, il existe un groupe G

libre modulo n, engendré par un ensemble A de générateurs libres modulo n, de puissance $\mathfrak{m}$. Il existe également, pour tout nombre cardinal $\mathfrak{m}$, un groupe G quasi libre modulo n engendré par un ensemble A de puissance $\mathfrak{m}$ de générateurs quasi libres modulo n, quel que soit l'entier de $n \geqq 2$.

D'un ensemble donné A de générateurs libres modulo n d'un groupe G libre modulo n on peut déduire de nouveaux ensembles de générateurs libres modulo n par application répétée des deux opérations suivantes:

1. Remplacement d'un élément a de l'ensemble considéré par a^m, où m est un entier, de la suite $1, 2, \ldots, ln - 1$, premier avec ln si a est d'ordre fini ln (l = entier $\geqq 1$), ou bien $m = -1$, si a est, d'ordre infini.
2. Remplacement d'un élément quelconque a de l'ensemble de générateurs considéré par son produit, à droite, à gauche ou des deux côtés à la fois, par une composition finie totalement réductible modulo n d'éléments autres que a de l'ensemble considéré de générateurs.

Soient a et b deux éléments quelconques d'un groupe G libre modulo n, soit a^* un élément de G symétrique de a modulo n et soit b^* un élément symétrique de b modulo n. Le produit aba^*b^* est appelé un *commutateur* de a et b modulo n. Il existe en général plusieurs commutateurs modulo n de deux éléments a et b de G. Le sous-groupe de G engendré par l'ensemble des commutateurs modulo n de couples d'éléments de G est un sous-groupe invariant modulo n de G, appelé le *sous-groupe commutateur modulo n* de G.

Une succession finie de groupes $G_0, G_1, \ldots, G_u$, telle que $G_0 = G$, $G_u = C_1$, $G_0 \supset G_1 \supset \supset G_u$ et où Gs est un sous-groupe maximum invariant modulo n de G_{s-1}, $s = 1, \ldots u$, est appelée *série de composition modulo n de G*. Un groupe libre modulo n ne possède pas toujours une telle série de composition.

Tout groupe libre modulo n élémentaire non cyclique possède une infinité de sous-groupes libres. Le centre d'un groupe libre modulo n élémentaire non cyclique se réduit à 1, mais un groupe libre modulo n non élémentaire peut posséder des éléments centraux $= 1$.

Tout groupe G libre modulo n est un *produit libre* des groupes cycliques engendrés par les éléments de n'importe quel ensemble de générateurs libres modulo n de G.

J. Chuard (Lausanne): *Réseaux cubiques tracés sur une sphère. Le greffage.*

Un réseau tracé sur une sphère transforme la surface de celle-ci en un polyèdre. Les arêtes des polyèdres que nous examinons forment un réseau cubique. Il s'en suit qu'à chaque sommet aboutissent 3 arêtes. Les faces du polyèdre sont simplement connexes. Le polyèdre a α_0 sommets, α_1 arêtes et α_2 faces. Nous introduisons un nombre μ qui fixe la classe du polyèdre. Le théorème d'Euler permet d'écrire les égalités

$$\mu = \alpha_2 - 1 \qquad \mu - 1 = \frac{\alpha_1}{3} = \frac{\alpha_0}{2} \cdot$$

Le réseau cubique considéré est réductible, en vertu du théorème de Petersen, cela de diverses manières, en un réseau quadratique (réseau R) et un réseau linéaire (réseau L). Le réseau R est formé de α_0 arêtes tandis que le réseau L n'en compte que $\frac{1}{2}\,\alpha_0$. Les réseaux R ainsi obtenus peuvent être répartis en 3 types: type I, le réseau ne comporte qu'un seul contour fermé; type II, il y en a 2 ou plusieurs qui comptent tous un nombre pair d'arêtes; type III, certains de ces contours fermés ont un nombre impair d'arêtes (ils sont d'ailleurs en nombres pairs).

Le polyèdre de la Planche 1 appartient à la classe $\mu = 4$. Il renferme 4 réseaux R (par suite 4 réseaux L). Il va nous permettre d'exposer en quoi consiste la méthode du *greffage*.

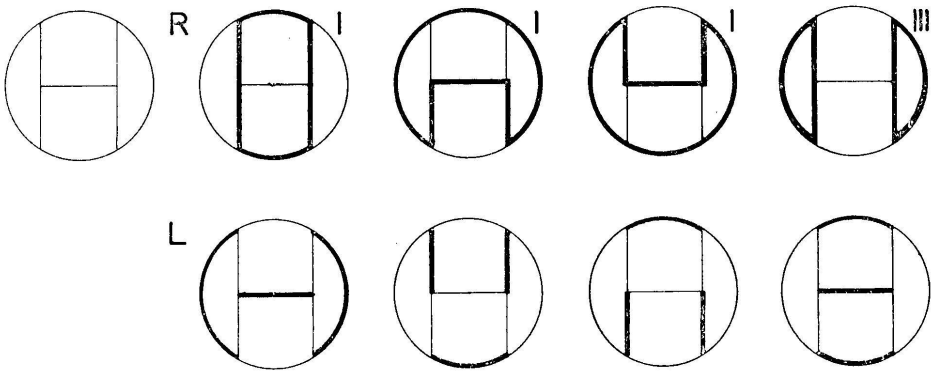

Planche 1

Sur une des arêtes du polyèdre, n'importe laquelle, on marque 2 points que l'on considère comme 2 nouveaux sommets. On réunit ces sommets par une nouvelle arête. On forme ainsi un nouveau polyèdre, de classe $\mu = 5$, dont on recherche les réseaux R. On constate que si l'arête sur laquelle s'est opéré le greffage est sur un

réseau R de la classe $\mu = 4$, on obtient 2 réseaux R sur le polyèdre de la classe $\mu = 5$, sinon on n'en obtient qu'un seul. C'est ce que fait voir la Planche 2. Ce dernier polyèdre renferme donc 6 réseaux R.

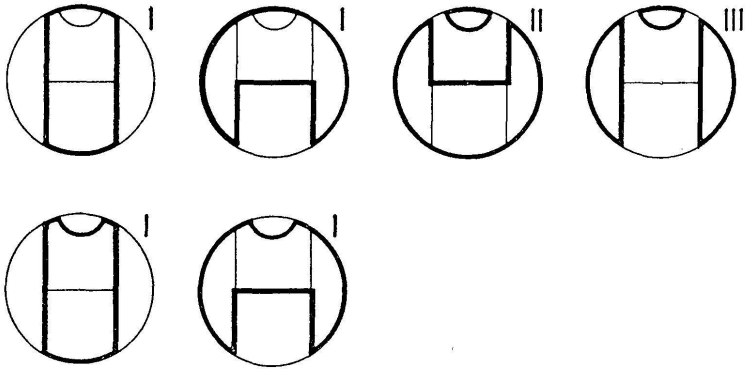

PLANCHE 2

Un second greffage conduit à un polyèdre de la classe $\mu = 6$. Les caractères relevés ci-dessus, dans le passage du polyèdre de la classe $\mu = 4$ à celui du polyèdre de la classe $\mu = 5$, se retrouvent ici intégralement. Il convient de noter que la Planche 1 présente 4 réseaux R dont 3 sont du type I et 1 du type III. La Planche 2 en présente 6 dont 4 sont du type I, 1 du type II et 1 du type III. La Planche 3 en présente 9 dont 4 sont du type I, 4 du type II et 1 du type III.

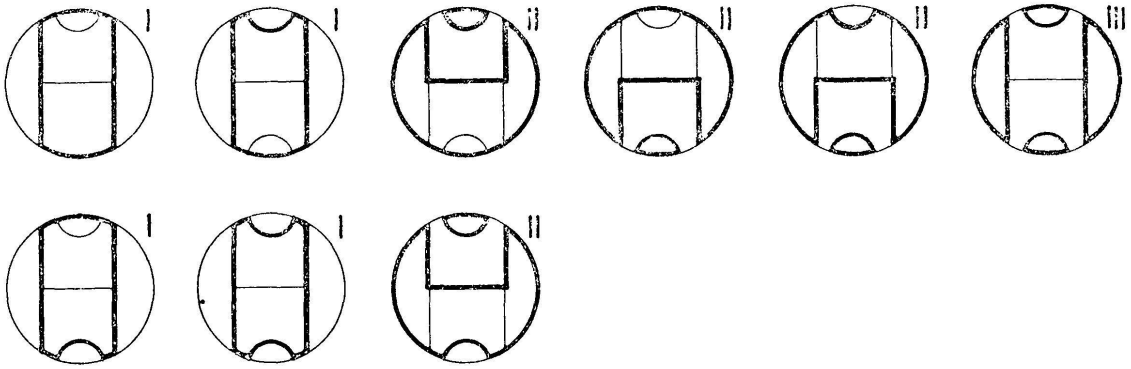

PLANCHE 3

Lorsque l'on passe à la troisième opération de greffage, une remarque s'impose. Jusqu'ici nous avons utilisé des arêtes qui faisaient partie du même réseau R: Planche 1. Si la troisième arête appartient encore à ce réseau R, il n'y a aucune raison de ne pas rencontrer encore des réseaux R du type I. Le nouveau polyèdre est de la classe $\mu = 7$. Celui de la Fig. 1: Planche 4 compte 8 réseaux R du type I, 6 du type II et 1 du type III.

Si, par contre, l'arête utilisée appartient au réseau L correspondant, les réseaux R du type I ont tous disparu, les 4 figures de gauche de la Planche 3 en donnent la raison. C'est ainsi qu'en Fig. 2: Planche 4 on dénombre 12 réseaux R du type II et 1 du type III, tandis que la Fig. 3 conduit à 12 réseaux R du type II et 2 du type III.

En utilisant la deuxième figure de la Planche 1, on constate que la Fig. 4: Planche 4 renferme des réseaux R du type I, tandis que la Fig. 5 n'en a pas.

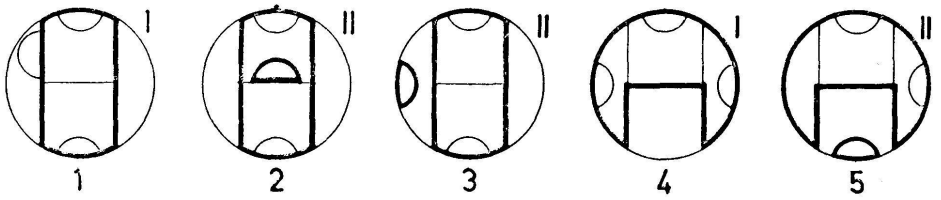

PLANCHE 4

Le greffage ainsi effectué n'est pas un but, mais un moyen qui permet de justifier l'inexistence de réseaux R du type I dans un réseau cubique donné. Ce qui est important ce n'est pas la présence de faces limitées par 2 arêtes seulement, mais plutôt celle de faces ayant en commun 2 arêtes distinctes. C'est ce que l'on évite en se plaçant dans le « cas difficile » de Errera.

Voici quelques exemples de réseaux cubiques dans lesquels le troisième greffage a été effectué sur une arête d'un réseau L.

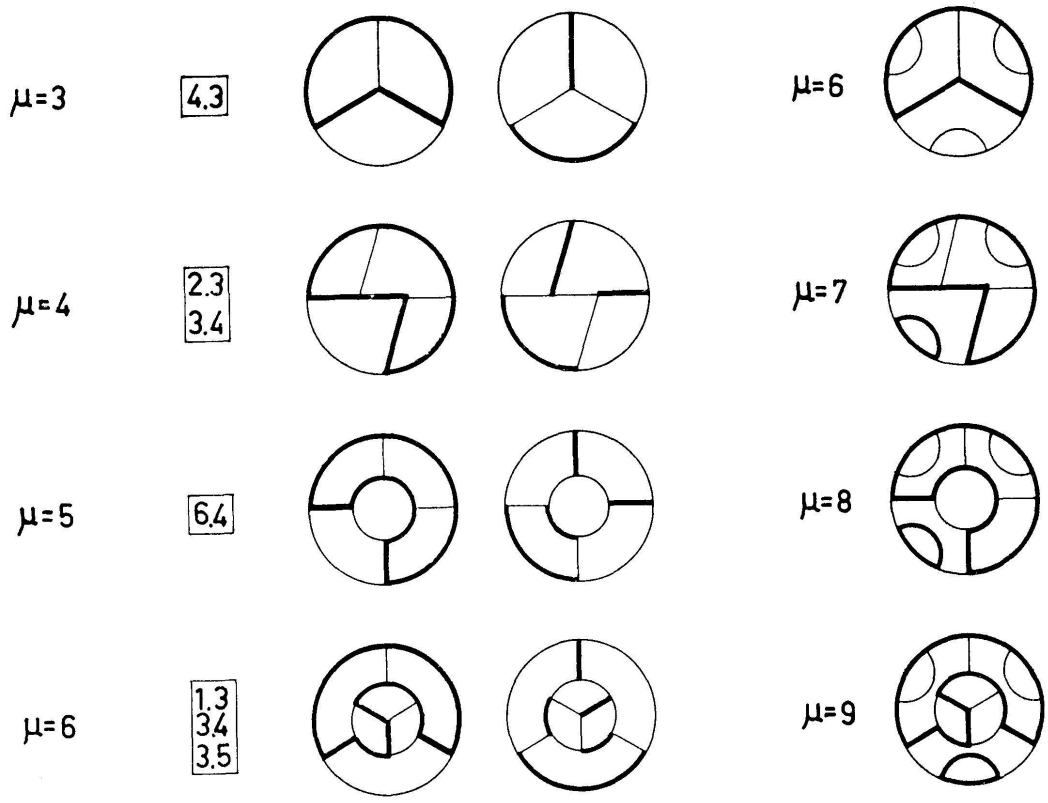

PLANCHE 5