STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1951 - 006

Rapport sur un manuscrit de Sophie Piccard intitulé:

Structure des groupes imprimitifs, suites associées, classes de substitutions, sous-groupes distingués, nombre minimum d'éléments générateurs.

W. Peremans

1951

Rapport Z.W. 1951-006

Rapport sur un manuscrit de Sophie Piccard intitulé: Structure des groupes imprimitifs, suites associées, classes de substitutions, sous-grpupes distingués, nombre minimum d'éléments générateurs.

par W.Peremans.

Si G est un groupe imprimitif de substitutions des nombres 1,2,...,n et $E_1,E_2,\ldots,E_m$ sont des systèmes d'imprimitivité, on obtient un nouveau groupe transitif de substitutions des nombres 1,2,...,m ($1 < m < n$) en prenant toute substitution $\begin{pmatrix} 1 & 2 & \ldots & m \\ i_1 & i_2 & \ldots & i_m \end{pmatrix}$ à laquelle correspond au moins une substitution du groupe G qui transforme E_j en E_{i_j}, quel que soit $j = 1,2,\ldots,m$. Le groupe G est homomorphe à ce groupe. Ce groupe est appelé le premier groupe associé de G. Si ce groupe est de nouveau imprimitif, on peut répéter ce procédé et obtenir ainsi une suite de groupes, dont le dernier est primitif. Cette suite est appelée la suite complète associée au groupe G relative aux systèmes d'imprimitivité, qui sont choisis dans chaque groupe de la suite pour construire le groupe suivant de la suite. A une substitution S de G correspond une substitution dans chaque groupe de la suite complète associée au groupe G et ainsi S donne lieu à une suite complète de substitutions associée à la substitution S relative à la suite donnée associée au groupe G. Des suites complètes de groupes et de substitutions on peut extraire des suites partielles. A chaque suite partielle de groupes on fait correspondre une décomposition du groupe G en deux classes C_1 et C_2. Une substitution S de G fait partie de la classe C_1 si le nombre des substitutions impaires dans la suite partielle de substitutions associée à S relative à la suite partielle donnée est pair et de la classe C_2, si ce nombre est impair. La classe C_2 peut être vide, mais la classe C_1 contient toujours la substitution identique. L'auteur démontre que, si C_2 n'est pas vide, C_1 et C_2 ont le même nombre d'éléments et C_1 est un sous-groupe distingué de G. Ainsi on obtient une décomposition de G tout à fait

analogue à la décomposition du groupe symétrique en substitutions paires et impaires!

Si la longueur de la suite complète considérée est m, on obtient ainsi 2^m-1 paires de classes, qui ne sont pas nécessairement toutes distinctes. L'auteur démontre même (dans sa proposition 2) que, quel que soit l'entier $m \geqslant 2$, il existe un groupe G qui a une suite complète de longueur m telle que toutes les $2(2^m-1)$ classes sont distinctes. Dans ce cas nous appelons le groupe G complet par rapport à la suite complète donnée. Par conséquent G possède au moins 2^m-1 sous-groupes distingués distincts dont chacun comprend la moitié des substitutions de G. Le groupe construit par l'auteur est de degré 2^m et d'ordre 2^{2^m-1}; il est engendré par m substitutions génératrices. L'auteur demontre (dans sa proposition 3) qu'un groupe ayant les propriétés exigées dans la proposition 2 ne peut pas être engendré par un système de substitutions génératrices d'un nombre moindre que m. Finalement l'auteur donne pour chaque entier $n \geqslant 2$ un exemple d'un groupe imprimitif auquel on peut associer des suites complètes de longueur m quel que soit l'entier $m \geqslant 2$ et $\leqslant n$.

Je me permets de faire les remarques suivantes au sujet du manuscrit.

L'auteur emploie p_i pour indiquer des nombres qui ne sont pas premiers. N'est-il pas préférable de réserver la lettre p pour les nombres premiers?

L'auteur emploie le terme "isomorphe" dans le sens de méroédriquement isomorphe. Je sais que l'emploi des mots isomorphe et homomorphe n'est pas fixé; cependant je crois que l'emploi d'homomorphe pour merо édriquement isomorphe et d'isomorphe pour holoédriquement isomorphe est à présent assez généralement convenu.

Il serait peut-être préférable de faire précéder les lignes 5 à 7 de la page 5 des lignes 8 à 10, vu que l'énoncé des lignes 8 à 10 reste vrai indépendamment de la restriction faite aux lignes 5 à 7.

Pour le corollaire 1 (page 5) je propose une démonstration simplifiée comme suit:

Soit $\mathfrak{G}_2 = \{1, a\}$ un groupe à deux éléments ($a^2 = 1$). On fait correspondre à un élément $S^{(')}$ de G_1 l'élément 1; si $S^{(')} \in C_1^{i_1 i_2 \ldots i_t}$ et l'élément a, si $S^{(')} \in C_2^{i_1 i_2 \ldots i_t}$. Selon la proposition 1 cette corres-

pondance est un homomorphisme qui est, $C_2^{i_1 i_2 \ldots i_t}$ n'étant pas vide, sur γ_2. Il s'ensuit directement que $C_1^{i_1 i_2 \ldots i_t}$ est un sous-groupe distingué de G_1, dont le nombre des éléments est la moitié du nombre des éléments de G_1.

Les lignes 12 à 10 au bas de la page 6 me semblent être incorrectes. Je crois qu'il faut lire:
Quel que soit l'entier $j = 2,3,\ldots,m$ le groupe G_j a pour système d'éléments générateurs les $m - j + 1$ substitutions: $S_i^{(j)} = (1 \quad 1+2^{i-1} \quad 1+2.2^{i-1} \ldots 1+(2^{m-j-i+2}-1)2^{i-1})$, $i = 1,2,\ldots,m-j+1$.

La possibilité $r > u$ (page 8) est exclue d'avance, car elle impliquerait $i_{t-r+1} = j_{u-r+1}$, ce qui dans ce cas serait vide de sens. Les cas à distinguer doivent être a) $r \geqslant u$ et b) $r < u$ (la définition de r étant lue de manière que $i_{t-r} \neq j_{u-r}$ si un des indices est $\leqslant 0$). Alors la ligne 17 en haut se change comme suit:
a) $r \geqslant u$. On a alors nécessairement $t > u$, $r = u$, $i_{t-h} = j_{u-h}$, $h = 0,1,\ldots,u-1$.

La même remarque peut être faite page 9.

Les lignes 4 et 3 au bas de la page 8 seraient peut-être mieux formulées de la manière suivante:
$C_1^{j_1 j_2 \ldots j_u}$, si r est impair, et la substitution $S^{(')}_{m-j_{u-r+2}}$ fait partie de la classe $C_1^{j_1 j_2 \ldots j_u}$.
En effet il n'est pas certain que $S^{(')}_{m-j_{u-r-1}+1}$ ait du sens, par exemple si $r = u - 1$.

A la ligne 15 au bas de la page 10, il faut lire $m - i$ au lieu de $m - i - 1$.

A titre de curiosité on pourrait peut-être insérer dans la remarque 1 (page 10) l'observation que 2^{2^m-1} est la puissance la plus élevée de 2 qui soit un sousmultiple de $(2^m)!$ et par conséquent que le groupe en question est le groupe le plus grand de degré 2^m, dont l'ordre soit une puissance de 2.

Aux lignes 5 et s.s. de la page 12 la lettre h est introduite, mais cette lettre avait déja été employée dans la même démonstration avec une autre signification. Je propose de la remplacer par k.

Partant de la constatation que la théorie classique des équations linéaires (avec déterminants) garde sa va-

lidité dans un corps commutatif arbitraire, qui est dans le cas présent le corps à deux éléments, on pourrait supprimer de la démonstration de la proposition 3 la partie qui se trouve à la page 12. L'auteur d'ailleurs dans sa remarque 2 y a fait allusion. Il est vrai que l'auteur a prouvé qu'il y a pour les équations au bas de la page 11 une solution exacte en nombres entiers, dont au moins un est impair, tandis que la mise en application du corps à deux éléments ne donne qu'une solution des équations entendues comme congruences mod 2. Pour la démonstration de la proposition cette dernière solution est suffisante.

Page 14 la forme explicite de ${}_iE'_h$ n'est pas donnée. Je propose d'insérer:

${}_iE'_h = \{h, h+2^i, h+2.2^i, \ldots, h+(2^{n-i}-1)2^i\}$, $h = 1,2,\ldots,2^i$.

Je ne comprends pas pourquoi l'auteur a, comparativement à la démonstration de la proposition 3, interverti les indices de a^i_j dans la remarque 2.

Je dois avouer que je n'ai pas compris la portée de la remarque 3 (page 14). Je ne vois pas pourquoi il est nécessaire de donner un exemple explicite d'un groupe auquel on peut associer des suites complètes d'une longueur qui est un entier arbitraire compris au sens large entre 2 et un entier n donné. En effet je crois être à même de démontrer qu'à chaque groupe, auquel on peut associer des suites complètes de longueur n, on peut associer également des suites complètes d'une longueur arbitraire, comprise au sens large entre 2 et n. Afin de démontrer ceci, je commence par rappeler la preuve faite par l'auteur de l'homomorphisme entre un groupe et son premier groupe associé. Ainsi l'imprimitivité implique l'existence d'un certain homomorphisme. Cette relation est réversible ainsi que je l'exprime dans la proposition suivante:

Proposition: Soit G un groupe transitif de substitutions des nombres $1,2,\ldots,n$ et H un groupe de substitutions des nombres $1,2,\ldots,k$ $(1 < k < n)$. S'il y a une transformation $\varphi(i)$ qui transforme les nombres $i = 1,\ldots,n$ en les nombres $\varphi(i) = 1,\ldots,k$ et une transformation $\phi(S)$ qui transforme les substitutions S de G en les substitutions $\phi(S)$ de H telles que $\phi(S)\,\varphi(i) = \varphi(Si)$, quelle que soit la substitution S du groupe G et quel que soit $i = 1,\ldots,n$, le groupe H est transitif, la transformation ϕ est un homomorphisme et, quand on décompose les nombres $1,\ldots,n$ en classes en prenant i et j dans la même classe si $\varphi(i) = \varphi(j)$, ces classes sont des systèmes d'imprimitivité de G et H est le premier groupe associé à G rela-

tif à ces systèmes d'imprimitivité.

Démonstration: Si λ et μ sont des entiers, $1 \leqslant \lambda \leqslant k, 1 \leqslant \mu \leqslant k$, il y a des entiers i et j ($1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n$) tels que $\varphi(i) = \lambda$, $\varphi(j) = \mu$. Comme G est transitif, il existe une substitution S du groupe G telle que $S(i) = j$. Alors $\Phi(S)\lambda = \Phi(S)\varphi(i) = \varphi(Si) = \varphi(j) = \mu$, donc H est transitif. Comme $\Phi(ST)\varphi(i) = \varphi(STi) = \Phi(S)\varphi(Ti) = \Phi(S)\Phi(T)\varphi(i)$, Φ est un homomorphisme. Si $\varphi(i) = \varphi(j)$, $\varphi(Si) = \Phi(S)\varphi(i) = \Phi(S)\varphi(j) = \varphi(Sj)$. Puisque $k > 1$, il y a des nombres i et j tels que $\varphi(i) \neq \varphi(j)$; puisque $k < n$, il y a des nombres i et j tels que $i \neq j$ et $\varphi(i) = \varphi(j)$. Ceci prouve que les classes formées conformément à l'énoncé de la proposition sont des systèmes d'imprimitivité de G. Ceci dit il est évident que H est le premier groupe associé à G relatif à ces systèmes d'imprimitivité, c.q.f.d.

Il est évident qu'inversement chaque groupe imprimitif et son premier groupe associé peuvent être obtenus par la méthode de la proposition ci-dessus.

Si nous prenons un troisième groupe K de substitutions des nombres $1,\ldots,l$ ($1 < l < k$) de telle manière qu'il existe une transformation $\psi(j)$ qui transforme les nombres $1,\ldots,k$ en les nombres $\psi(j) = 1,\ldots,l$ et une transformation $\Psi(T)$ qui transforme les substitutions T de H en les substitutions $\Psi(T)$ de K telles que $\Psi(T)\psi(j) = \psi(Tj)$, le groupe K est le second groupe associé à G relatif aux systèmes d'imprimitivité trouvés au moyen de la proposition ci-dessus. Cependant la transformation $\Psi(\varphi(i))$ est une transformation des nombres $1,\ldots,n$ sur les nombres $1,\ldots,l$ et $\Psi(\Phi(S))$ une transformation des substitutions de G sur les substitutions de K, telles que $\Psi(\Phi(S))\psi(\varphi(i)) = \psi(\Phi(S)\varphi(i)) = \psi(\varphi(Si))$ et la proposition ci-dessus nous fait voir que G peut être décomposé en systèmes d'imprimitivité tels que K est le premier groupe associé à G par rapport à ces systèmes d'imprimitivité.

Ainsi nous avons démontré que la longueur d'une suite complète peut être diminuée d'une unité et par conséquent qu'à chaque groupe imprimitif auquel peut être associée une suite complète de longueur n, on peut associer une suite d'une longueur arbitraire comprise au sens large entre 2 et n.

Signalons en passant que ceci démontre aussi la proposition de C.Jordan mentionnée au bas de la page 2 du manuscrit.