Un théorème concernant le nombre total des bases d'un groupe d'ordre fini.

Autor(en): **Piccard, Sophie**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **21 (1948)**

PDF erstellt am: **29.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-18603

Un théorème concernant le nombre total des bases d'un groupe d'ordre fini

Par Sophie Piccard, Neuchâtel

Soit G un groupe d'ordre fini. Soit v un entier ≥ 1. Nous dirons que G est à base d'ordre v s'il existe au moins un système 1) $a_1, a_2, \ldots, a_v$ formé de v éléments indépendants[1]) de G, tel que tout élément de G s'obtient par composition finie des éléments 1), alors qu'aucun système formé de moins de v éléments de G ne jouit de cette propriété. Si G est à base d'ordre v, nous appellerons base de G tout système de v éléments indépendants de G qui engendrent le groupe G tout entier par composition finie. Soit $B = [a_1, a_2, \ldots, a_v]$ une base de G et soit a un élément quelconque de G. Posons $a a_i a^{-1} = a_i'$[2]). Alors $B' = [a_1', a_2', \ldots, a_v']$ est également une base de G. Nous dirons que B' est la transformée de B par a et nous écrirons $B' = aBa^{-1}$.

Soient $B_1 = [a_1, a_2, \ldots, a_v]$ et $B_2 = [b_1, b_2, \ldots, b_v]$ deux bases de G. Nous dirons que ces bases sont distinctes si un élément au moins de l'ensemble $\{a_1, a_2, \ldots, a_v\}$ ne fait pas partie de l'ensemble $\{b_1, b_2, \ldots, b_v\}$ et vice versa. Nous dirons que les bases B_1 et B_2 sont indépendantes si $B_1 \neq a B_2 a^{-1}$, quel que soit l'élément a de G.

Nous dirons que les bases $B_1, B_2, \ldots, B_m$ d'un groupe G constituent un système complet de bases indépendantes de G si elles sont indépendantes deux à deux et si, pour toute base B de G, il existe un indice i compris au sens large entre 1 et m et un élément a de G, tels que $B = a B_i a^{-1}$. Le nombre m des éléments qui constituent un système complet de bases indépendantes de G est un invariant du groupe G. Nous l'appellerons l'ordre d'un système complet de bases indépendantes de G.

Remarque 1. Soit G un groupe d'ordre fini N à base d'ordre v et soit $B = [a_1, a_2, \ldots, a_v]$ une base de G. Soit E l'ensemble des éléments de G qui transforment la base B en elle-même. Montrons que E est un groupe.

---

[1]) Dont aucun ne peut être obtenu par composition finie des autres.

[2]) Les éléments successifs de la composition sont à effectuer de droite à gauche.

En effet soient a et b deux éléments quelconques de E. On a donc $aBa^{-1} = B$ et $bBb^{-1} = B$, d'où $baBa^{-1}b^{-1} = bBb^{-1} = B$, ce qui prouve que $ba \in E$. Donc E est bien un groupe. Soit v l'ordre de E. On a $v \geq 1$, puisque E contient en tout cas l'élément unité de G. Comme E est un sous-groupe de G, n est un diviseur de N. Soit E_c le centre de G et soit μ l'ordre de E_c. Montrons qu'on a $v \leq v!\mu$. En effet, soit $i_1, i_2, \ldots, i_v$ une permutation quelconque des nombres $1, 2, \ldots, v$ et soit $E_{i_1 i_2 \ldots i_v}$ l'ensemble des éléments de E qui transforment a_1 en a_{i_1}, a_2 en $a_{i_2}, \ldots, a_v$ en a_{i_v}.

Si l'ensemble $E_{i_1 i_2 \ldots i_v}$ n'est pas vide, il comprend μ éléments. En effet, supposons que cet ensemble n'est pas vide et soit c un élément quelconque de $E_{i_1 i_2 \ldots i_v}$. On a donc $ca_h c^{-1} = a_{i_h}$, quel que soit $h = 1, 2, \ldots, v$, et, quel que soit l'élément d de E_c, on a $cda_h d^{-1}c^{-1} = ca_h c^{-1} = a_{i_h}$.

Donc $cd \in E_{i_1 i_2 \ldots i_v}$ et, comme les éléments $cd (d \in E_c)$ sont au nombre de μ, il s'ensuit que $\overline{\overline{E}}_{i_1 i_2 \ldots i_v} \geq \mu$ [3]). Soient maintenant c un élément fixe et c' un élément quelconque de $E_{i_1 i_2 \ldots i_v}$. Montrons qu'il existe un élément d de E_c, tel que $c' = cd$. En effet, comme c et c' appartiennent à $E_{i_1 i_2 \ldots i_v}$, en a $ca_h c^{-1} = a_{i_h}$ et $c'a_h c'^{-1} = a_{i_h}$, $h = 1, 2, \ldots, v$. Donc $ca_h c^{-1} = c'a_h c'^{-1}$. D'où $c^{-1}c'a_h c'^{-1}c = a_h$, $h = 1, 2, \ldots, v$. Donc $c^{-1}c'$ est permutable avec a_h, quel que soit $h = 1, 2, \ldots, v$. Et comme $B = [a_1, a_2, \ldots, a_v]$ est une base de G, il s'ensuit que $c^{-1}c'$ est permutable avec tous les éléments de G. Donc $c^{-1}c \in E_c$. Soit $c^{-1}c' = d$, $d \in E_c$. On a donc bien $c' = cd$, où $d \in E_c$. On voit donc bien que si l'ensemble $E_{i_1 i_2 \ldots i_v}$ n'est pas vide, $\overline{\overline{E}}_{i_1 i_2 \ldots i_v} = \mu$. Et comme $E = \Sigma E_{i_1 i_2 \ldots i_v}$, la sommation Σ s'étendant à toutes les permutations possibles $i_1, i_2, \ldots, i_v$ des nombres $1, 2, \ldots, v$, et que les ensembles $E_{i_1 i_2 \ldots i_v}$ sont disjoints deux à deux, il s'ensuit que l'ordre v de E vérifie bien l'inégalité $v \leq v!\mu$.

Proposition 1. Quel que soit le groupe G d'ordre fini N, il existe un entier n diviseur de N et tel que le nombre total des bases de G est un multiple de $\frac{N}{n}$.

Démonstration. — En effet, soit G un groupe d'ordre fini N à base d'ordre v, soit m l'ordre d'un système complet de bases indépendantes de G et soit $B_1, B_2, \ldots, B_m$ un système complet de bases indépendantes de G.

---

[3]) Le symbole $\overline{\overline{E}}$ désigne la puissance de l'ensemble E.

Soit E_i l'ensemble des éléments de G qui transforment la base B_i en elle-même et soit n_i l'ordre de E_i ($i = 1, 2, \ldots, m$). D'après la remarque 1, on a $1 \leq n_i \leq v!\mu$, où μ désigne l'ordre du centre de G, E_i est un groupe et n_i est un diviseur de N.

Soit i un nombre quelconque de la suite $1, 2, \ldots, m$. Montrons que le nombre total de transformées distinctes de la base B_i par les éléments de G est égal à $\frac{N}{n_i}$.

En effet, soit c un élément de E_i. On a $cB_ic^{-1} = B_i$, par définition de E_i. Soient maintenant d un élément quelconque de $G - E_i$ et soit $dB_id^{-1} = B_i'$. On a $B_i' \neq B_i$, puisque $d \bar{\in} E_i$ et, quel que soit l'élément c de E_i, on a $dcB_ic^{-1}d^{-1} = dB_id^{-1} = B_i'$. Donc les n_i éléments dc ($c \in E_i$) de $G - E_i$ transforment B_i en B_i'. Montrons maintenant que si un élément f de $G - E_i$ transforme B_i en B_i', il existe un élément c de E_i, tel que $f = dc$. En effet, par définition de f, on a $fB_if^{-1} = B_i'$. D'autre part, on a $dcB_ic^{-1}d^{-1} = B_i'$, quel que soit $c \in E_i$. Soit c_1 un élément fixe quelconque de E_i. On a donc $fB_if^{-1} = dc_1B_ic_1^{-1}d^{-1}$. On en déduit $f^{-1}dc_1B_ic_1^{-1}d^{-1}f = B_i$. Donc $f^{-1}dc_1 \in E_i$. Soit h l'élément de E_i, tel que $f^{-1}dc_1 = h$. On a donc $f = dc_1h^{-1}$ et, comme $c_1 \in E_i$, $h \in E_i$ et que E_i est un groupe, on a $h^{-1} \in E_i$ et $c_1h^{-1} \in E_i$. Soit $c_1h^{-1} = c$. On a donc bien $f = dc$, où $c \in E_i$. Ainsi n_i éléments et n_i seulement de $G - E_i$ transforment B_i en B_i'. On peut donc répartir les éléments de G en $\frac{N}{n_i}$ ensembles $G_1 = E_i$, $G_2, \ldots, G_{\frac{N}{n_i}}$, disjoints deux à deux, comprenant chacun n_i éléments et tels que tous les éléments de G_l transforment B_i en la même base $B_i^{(l)}$ de G, quel que soit $l = 1, 2, \ldots, \frac{N}{n_i}$ et les bases $B_i^{(1)} = B_i, B_i^{(2)}, \ldots, B_i^{\left(\frac{N}{n_i}\right)}$ sont toutes distinctes. Notre assertion est ainsi démontrée.

Et comme les bases $B_1, B_2, \ldots, B_m$ forment un système complet de bases indépendantes du groupe G, le nombre total π des bases de G est

$$\pi = \frac{N}{n_1} + \frac{N}{n_2} + \cdots + \frac{N}{n_m}. \tag{2}$$

Soit n le plus petit commun multiple des nombres $n_1, n_2, \ldots, n_i$ et soit $n = n_in_i'$, $i = 1, 2, \ldots, m$.

Comme $n_1, n_2, \ldots, n_m$ sont les diviseurs de N, il en est de même de n et on a, d'après 2),

$$\pi = (n_1' + n_2' + \cdots + n_m') \frac{N}{n} ,$$

ce qui démontre la proposition 1.

Remarque 2. Si le groupe G est abélien, quelle que soit la base B de G et quel que soit l'élément a de G, on a $aBa^{-1} = B$. Dans ce cas $n_1 = n_2 = \cdots = n_m = n = N$ et la proposition 1 ne donne aucune indication sur le nombre total π de bases de G.

D'autre part, si G est tel que toute base de G admet N transformées distinctes au moyen des éléments de G, on a $n_1 = n_2 = \cdots = n_m = n = 1$ et le nombre total des bases de G est un multiple de N. Tel est, par exemple, le cas du groupe G d'ordre 18 engendré par trois éléments a, b, c liés par les relations fondamentales $a^2 = b^2 = c^2 = 1$, $aba = bab$, $aca = cac$, $bcb = cbc$, $(abc)^2 = 1$ [4]).

Ce groupe est à base du troisième ordre et chacune de ses bases admet 18 transformées distinctes au moyen des éléments de G. Donc, d'après la proposition démontrée, le nombre total des bases de ce groupe doit être un multiple de 18. Et, en effet, ce nombre est $504 = 18 \times 28$.

Pour le groupe symétrique d'ordre $N = k!$, où k est un entier ≥ 3 $\left(\text{le groupe alterné d'ordre } N = \frac{k!}{2},\ k \geq 4\right)$ on a $n = 2$ et le nombre total des bases de ce groupe est un multiple de $\frac{k!}{2}\left(\frac{k!}{4}\right)$.

D'une façon générale, il résulte de la proposition 1 et de sa démonstration que le nombre total π de bases d'un groupe G d'ordre fini N vérifie les inégalités $\frac{mN}{v!\,\mu} \leq \pi \leq mN$.

Pour le groupe symétrique d'ordre $N \geq 6$, on a $v = 2$, $\mu = 1$ et il existe des bases de deux espèces : les unes admettent N transformées distinctes au moyen des éléments de G, les autres n'en admettent que $N/2$, de sorte que l'on a en tout cas les inégalités $\frac{mN}{2} < \pi < mN$.

Si G est abélien, en a $\mu = N$ et $\pi = m$.

(Reçu le 10 juin 1947.)

---

[4]) Il existe un groupe de substitutions caractérisé par ces relations.