

|                     |   |
|---------------------|---|
| <b>Zeitschrift:</b> | Commentarii Mathematici Helvetici   |
| <b>Herausgeber:</b> | Schweizerische Mathematische Gesellschaft   |
| <b>Band:</b>        | 21 (1948)   |
| <br>                |   |
| <b>Artikel:</b>     | Un théorème concernant le nombre total des bases d'un groupe d'ordre fini.            |
| <b>Autor:</b>       | Piccard, Sophie   |
| <b>DOI:</b>         | <a href="https://doi.org/10.5169/seals-18603">https://doi.org/10.5169/seals-18603</a> |

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 16.02.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

# 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  $\geq 1$ . Nous dirons que  $G$  est à base d'ordre  $v$  s'il existe au moins un système 1)  $a_1, a_2, \dots, a_v$  formé de  $v$  éléments indépendants<sup>1)</sup> 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  $B = [a_1, a_2, \dots, a_v]$  une base de  $G$  et soit  $a$  un élément quelconque de  $G$ . Posons  $aa_i a^{-1} = a'_i$ <sup>2)</sup>. Alors  $B' = [a'_1, a'_2, \dots, a'_v]$  est également une base de  $G$ . Nous dirons que  $B'$  est la transformée de  $B$  par  $a$  et nous écrirons  $B' = aB a^{-1}$ .

Soient  $B_1 = [a_1, a_2, \dots, a_v]$  et  $B_2 = [b_1, b_2, \dots, b_v]$  deux bases de  $G$ . Nous dirons que ces bases sont distinctes si un élément au moins de l'ensemble  $\{a_1, a_2, \dots, a_v\}$  ne fait pas partie de l'ensemble  $\{b_1, b_2, \dots, b_v\}$  et vice versa. Nous dirons que les bases  $B_1$  et  $B_2$  sont indépendantes si  $B_1 \neq aB_2a^{-1}$ , quel que soit l'élément  $a$  de  $G$ .

Nous dirons que les bases  $B_1, B_2, \dots, B_m$  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  $B = aB_ia^{-1}$ . 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  $B = [a_1, a_2, \dots, a_v]$  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  $\nu$  l'ordre de  $E$ . On a  $\nu \geq 1$ , 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  $\mu$  l'ordre de  $E_c$ . Montrons qu'on a  $\nu \leq \nu! \mu$ . En effet, soit  $i_1, i_2, \dots, i_\nu$  une permutation quelconque des nombres  $1, 2, \dots, \nu$  et soit  $E_{i_1 i_2 \dots i_\nu}$  l'ensemble des éléments de  $E$  qui transforment  $a_1$  en  $a_{i_1}$ ,  $a_2$  en  $a_{i_2}, \dots, a_\nu$  en  $a_{i_\nu}$ .

Si l'ensemble  $E_{i_1 i_2 \dots i_\nu}$  n'est pas vide, il comprend  $\mu$  éléments. En effet, supposons que cet ensemble n'est pas vide et soit  $c$  un élément quelconque de  $E_{i_1 i_2 \dots i_\nu}$ . On a donc  $ca_h c^{-1} = a_{i_h}$ , quel que soit  $h = 1, 2, \dots, \nu$ , 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  $cd \in E_{i_1 i_2 \dots i_\nu}$  et, comme les éléments  $cd$  ( $d \in E_c$ ) sont au nombre de  $\mu$ , il s'ensuit que  $\bar{\bar{E}}_{i_1 i_2 \dots i_\nu} \geq \mu$ <sup>3)</sup>. Soient maintenant  $c$  un élément fixe et  $c'$  un élément quelconque de  $E_{i_1 i_2 \dots i_\nu}$ . Montrons qu'il existe un élément  $d$  de  $E_c$ , tel que  $c' = cd$ . En effet, comme  $c$  et  $c'$  appartiennent à  $E_{i_1 i_2 \dots i_\nu}$ , on a  $ca_h c^{-1} = a_{i_h}$  et  $c'a_h c'^{-1} = a_{i_h}$ ,  $h = 1, 2, \dots, \nu$ . Donc  $ca_h c^{-1} = c'a_h c'^{-1}$ . D'où  $c^{-1}c'a_h c'^{-1}c = a_h$ ,  $h = 1, 2, \dots, \nu$ . Donc  $c^{-1}c'$  est permutable avec  $a_h$ , quel que soit  $h = 1, 2, \dots, \nu$ . Et comme  $B = [a_1, a_2, \dots, a_\nu]$  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  $E_{i_1 i_2 \dots i_\nu}$  n'est pas vide,  $\bar{\bar{E}}_{i_1 i_2 \dots i_\nu} = \mu$ . Et comme  $E = \sum E_{i_1 i_2 \dots i_\nu}$ , la sommation  $\sum$  s'étendant à toutes les permutations possibles  $i_1, i_2, \dots, i_\nu$  des nombres  $1, 2, \dots, \nu$ , et que les ensembles  $E_{i_1 i_2 \dots i_\nu}$  sont disjoints deux à deux, il s'ensuit que l'ordre  $\nu$  de  $E$  vérifie bien l'inégalité  $\nu \leq \nu! \mu$ .

*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  $\nu$ , soit  $m$  l'ordre d'un système complet de bases indépendantes de  $G$  et soit  $B_1, B_2, \dots, B_m$  un système complet de bases indépendantes de  $G$ .

---

<sup>3)</sup> Le symbole  $\bar{\bar{E}}$  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  $E_i$  ( $i = 1, 2, \dots, m$ ). D'après la remarque 1, on a  $1 \leq n_i \leq v! \mu$ , où  $\mu$  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  $1, 2, \dots, m$ . 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  $cB_i c^{-1} = B_i$ , par définition de  $E_i$ . Soient maintenant  $d$  un élément quelconque de  $G - E_i$  et soit  $dB_i d^{-1} = B'_i$ . On a  $B'_i \neq B_i$ , puisque  $d \notin E_i$  et, quel que soit l'élément  $c$  de  $E_i$ , on a  $dcB_i c^{-1}d^{-1} = dB_i d^{-1} = B'_i$ . 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  $fB_i f^{-1} = B'_i$ . D'autre part, on a  $dcB_i c^{-1}d^{-1} = B'_i$ , quel que soit  $c \in E_i$ . Soit  $c_1$  un élément fixe quelconque de  $E_i$ . On a donc  $fB_i f^{-1} = dc_1 B_i c_1^{-1}d^{-1}$ . On en déduit  $f^{-1}dc_1 B_i c_1^{-1}d^{-1}f = B_i$ . 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  $f = dc_1 h^{-1}$  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  $c_1 h^{-1} \in E_i$ . Soit  $c_1 h^{-1} = c$ . 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  $G_1 = E_i$ ,  $G_2, \dots, G_{\frac{N}{n_i}}$ , 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  $l = 1, 2, \dots, \frac{N}{n_i}$  et les bases  $B_i^{(1)} = B_i$ ,  $B_i^{(2)}, \dots, B_i^{(\frac{N}{n_i})}$  sont toutes distinctes. Notre assertion est ainsi démontrée.

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

$$n = \frac{N}{n_1} + \frac{N}{n_2} + \dots + \frac{N}{n_m} . \quad (2)$$

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

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

$$n = (n'_1 + n'_2 + \cdots + n'_m) \frac{N}{n} ,$$

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  $n$  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  $a^2 = b^2 = c^2 = 1, aba = bab, aca = cac, bcb = cbc, (abc)^2 = 1$ <sup>4)</sup>.

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  $\geq 3$  (le groupe alterné d'ordre  $N = \frac{k!}{2}, k \geq 4$ ) 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  $n$  de bases d'un groupe  $G$  d'ordre fini  $N$  vérifie les inégalités  $\frac{mN}{v!\mu} \leq n \leq mN$ .

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  $\frac{mN}{2} < n < mN$ .

Si  $G$  est abélien, on a  $\mu = N$  et  $n = m$ .

(Reçu le 10 juin 1947.)

---

<sup>4)</sup> Il existe un groupe de substitutions caractérisé par ces relations.