Une nouvelle preuve du théorème de Wilson généralisé

G. A. Miller

En utilisant plusieurs théorèmes élémentaires portant sur les groupes de substitution, il est possible de donner une preuve très simple du théorème de Wilson en théorie des nombres. Cette preuve n'utilise rien de la théorie en ce qui concerne le nombre de racines d'une congruence. En fait, l'idée de congruence n'est pas utilisée du tout si ce n'est que le concept qui intervient est celui de périodicité. On commence par développer les théorèmes portant sur les groupes de substitution qui seront utilisés.

1. Énoncé du théorème. Produit de tous les opérateurs dans un groupe commutatif. Le théorème de Wilson porte sur les $\varphi(g)$ nombres premiers à un entier g et inférieurs à g, et affirme que leur produit est congru, *modulo* g, à -1 dans trois cas, quand $g = p^a, 2p^a$, ou 4, et dans tous les autres cas, leur produit est congru à $+1$. (Ici, p désigne un nombre premier impair, et a un nombre entier positif quelconque). Maintenant, ces $\varphi(g)$ nombres combinés par multiplication et leurs produits pris *modulo* g forment un groupe d'une certaine sorte particulière, le groupe des isomorphismes d'un groupe cyclique dans lui-même. L'ordre du groupe cyclique est g, et le groupe des isomorphismes est nécessairement abélien. De plus amples détails ont été expliqués dans un numéro récent des Annals (Seconde série, Vol. 2, p. 77). On s'attend donc à trouver en théorie des groupes un équivalent du théorème de Wilson en théorie des nombres, si on examine les groupes abéliens, et en particulier les groupes d'isomorphismes de groupes cycliques.

Tous les opérateurs dont l'ordre excède 2 dans n'importe quel groupe peuvent être arrangés de telle façon que leur produit continu est l'identité. Cela peut être fait, par exemple, en associant chaque opérateur avec son inverse. Comme dans un groupe abélien (A), dans lequel tout produit est indépendant de l'ordre de ses facteurs, il en découle que *le produit continu de tous les opérateurs dont l'ordre excède 2 dans A est l'identité.*

Si le groupe A ne contient aucun opérateur d'ordre 2, alors le produit de tous ses opérateurs est l'identité. Il reste à examiner séparément les opérateurs d'ordre 2 quand de tels opérateurs sont contenus dans le groupe.

Tous les opérateurs d'ordre 2 dans A engendrent un groupe (A_1) d'ordre 2^a, qui a a générateurs indépendants d'ordre 2. Si s_1 désigne n'importe lequel d'entre eux, alors A_1 est le produit direct du groupe $(1, s_1)$ et du sous-groupe d'ordre 2^{a-1} engendré par les gérérateurs indépendants restant. Il découle de cela que s_1 est un facteur de la moitié des opérateurs de A_1 et que par conséquent, il n'apparaît pas dans le produit continué de tous les opérateurs de A_1 à chaque fois que $a > 1$. Puisque n'importe quel opérateur d'ordre 2 aurait pu être pris à la place de s_1, on a le théorème : *Si un groupe abélien contient plus qu'un opérateur d'ordre 2, le produit continué de tous ses opérateurs est l'identité ; s'il ne contient qu'un seul tel opérateur, cet opérateur est le produit continué de tous ses opérateurs.*

Annals of mathematics, vol. 4, n° 4, Juillet 1903.
Traduction : Denise Vella-Chemla, septembre 2024.

2. Ordre d'un groupe cyclique dont le groupe d'isomorphismes contient seulement un opérateur d'ordre 2. On commence par prouver que l'ordre d'un tel groupe cyclique est de l'une des trois formes p^a, $2p^a$, ou 4. Soit M n'importe quel groupe de substitution métacyclique d'ordre $p(p-1)$ et de degré p. Le sous-groupe (M_1) qui est composé de toutes les substitutions de M qui omettent une lettre donnée est régulier et de degré $p-1$, puisque chacune de ses substitutions transforme chaque substitution d'ordre p dans M en une puissance d'elle-même. Comme M_1 est un groupe d'isomorphismes d'un groupe cyclique, il est abélien [*] . S'il contient plus d'une substitution d'ordre 2, M devrait contenir plus de p telles substitutions, puisque deux conjugués selon M ne peuvent appartenir en même temps à M_1 et chaque substitution d'ordre 2 dans M a p conjugués selon M.

Supposons, alors, que M puisse contenir plus que p substitutions d'ordre 2. Chacune d'elles devrait faire intervenir $(p-1)/2$ transpositions, et, comme il y a seulement $p(p-1)/2$ transpositions distinctes de p lettres, deux substitutions d'ordre 2 devraient avoir une transposition en commun. Leur produit devrait, par conséquent, être de degré moindre que $p-1$. Comme ceci est contraire au fait que M_1 est régulier de degré $p-1$, il s'ensuit que *le groupe d'isomorphismes d'un groupe cyclique d'ordre p contient seulement un opérateur d'ordre 2.*

Le groupe d'isomorphismes du groupe cyclique d'ordre p^a, $a>1$, est le produit direct du groupe cyclique d'ordre p^{a-1} et du groupe d'isomorphismes du groupe d'ordre p [†]. De cela, il découle que le groupe d'isomorphismes du groupe cyclique d'ordre p^a (et par conséquent également du groupe cyclique d'ordre $2p^a$) contient seulement un opérateur d'ordre 2. Il a été démontré sans utiliser la théorie des congruences que le groupe des isomorphismes du groupe cyclique d'ordre 2^a contient juste 3 opérateurs d'ordre 2 à chaque fois que $a>2$; quand $a=2$, ce groupe d'isomorphismes est d'ordre 2 de façon évidente. C'est-à-dire que, *si le groupe d'isomorphismes d'un groupe cyclique d'ordre 2^a contient seulement un opérateur d'ordre 2, alors a doit être égal à 2.*

Puisque le groupe des isomorphismes (G_1) du groupe cyclique (G) d'ordre $g=2^{a_0}p_1^{a_1}p_2^{a_2}\dots p_m^{a_m}$ est le produit direct [‡] des groupes d'isomorphismes des groupes cycliques d'ordres 2^{a_0}, $p_1^{a_1}$, $p_2^{a_2}$,$\dots$,$p_m^{a_m}$ et puisque chacun de ces groupes d'isomorphismes est d'ordre pair (excepté celui d'ordre 2^{a_0} quand $a_0=1$), il en résulte que G_1 doit faire intervenir plus d'un opérateur d'ordre 2 avec l'exception des trois cas lorsque son ordre est p^a, $2p^a$, ou 4 ou lorsque p est un nombre premier impair quelconque. C'est-à-dire que, *si le groupe d'isomorphismes d'un groupe cyclique contient seulement un opérateur d'ordre 2, l'ordre du groupe cyclique doit être l'un des trois nombres $4, p^a, 2p^a$, où p est un nombre premier impair quelconque.*

3. Conclusion. Comme stipulé dans l'introduction, le groupe G_1 des paragraphes précédents est représentable par les $\varphi(g)$ nombres inférieurs à g et premiers à g, quand on les combine par multiplication, les produits étant remplacés par leur plus petit résidu *modulo* g. Pour compléter maintenant la preuve du théorème de Wilson généralisé, il est seulement nécessaire de remarquer que dans les trois cas exceptionnels spécifiés dans le §1, l'unique opérateur d'ordre deux correspond

[*] *Transactions of the American Mathematical Society*, vol. 1 (1900), p. 397. De la théorie des racines primitives, il découle directement que M_1 est le groupe cyclique d'ordre $p-1$, mais la présente preuve est indépendante de cette théorie.

[†] *Bulletin of the American Mathematical Society*, vol. 7, 1901, p. 350.

[‡] *Transactions of the American Mathematical Society*, vol. 1, 1900, p. 396, Théorème II.

respectivement aux nombres $p^a - 1, 2p^a - 1$, et 3, i.e. les nombres congrus dans leurs systèmes respectifs à -1, alors que l'identité correspond à $+1$. Avec ces faits à l'esprit, il est évident que les théorèmes démontrés aux §§ 1, 2 constituent précisément un énoncé, dans le langage de la théorie des groupes, du théorème de Wilson.

Université de Stanford, Décembre 1902.