

# BULLETIN DE LA S. M. F.

J. PEROTT

## Sur les groupes de Galois

*Bulletin de la S. M. F.*, tome 21 (1893), p. 61-65.

[http://www.numdam.org/item?id=BSMF\\_1893\\_\\_21\\_\\_61\\_1](http://www.numdam.org/item?id=BSMF_1893__21__61_1)

© Bulletin de la S. M. F., 1893, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>), implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

*Sur les groupes de Galois*; par M. JOSEPH PEROTT.

Je n'ai nullement l'intention de donner une théorie complète de ces groupes qui ont fait l'objet de nombreux travaux : je me propose seulement de montrer comment il est possible d'engendrer chacun des trois groupes de Galois au moyen de trois opérations appartenant à l'exposant deux ou *réciproques*, comme les appelle Listing. Pour cela, j'aurai besoin de deux lemmes que je vais établir tout d'abord.

LEMME I. — *Deux opérations réciproques commutatives non identiques, faisant partie d'un groupe associatif quelconque, engendrent un sous-groupe d'ordre quatre.*

En effet, soient  $a$  et  $b$  les deux opérations en question; toute opération exécutée à l'aide de  $a$  et  $b$  revient, en vertu de leur commutativité, à une puissance de  $a$  combinée avec une puissance de  $b$ . Or, en réduisant les exposants de ces puissances à leur moindre valeur positive (mod 2), on n'obtient que quatre expressions distinctes :

$$a^1 b^1, \quad a^1 b^2, \quad a^2 b^1, \quad a^2 b^2.$$

Comme ces quatre expressions donnent des résultats différents, — autrement les opérations  $a$  et  $b$  seraient identiques —, le lemme est démontré.

Ajoutons que, dans ce cas,  $ab$  appartient à l'exposant deux. Inversement, si  $a$  et  $b$  sont deux opérations réciproques faisant partie d'un groupe associatif et que  $ab$  appartienne à l'exposant deux, les opérations  $a$  et  $b$  sont commutatives. En effet, l'opération  $ba$ , qui est l'inverse de  $ab$ , est alors égale à  $ab$ .

LEMME II. — *Deux opérations réciproques non commutatives  $a$  et  $b$ , faisant partie d'un groupe associatif quelconque, engendrent un sous-groupe dont l'ordre est le double de l'exposant toujours supérieur à deux auquel  $ab$  appartient.*

En effet, soit  $t$  l'exposant auquel  $ab$  appartient; on aura

$$b = a(ab), \quad ba = (ab)^{t-1}.$$

Les opérations  $a$  et  $b$  étant réciproques, il est inutile de les employer autrement qu'alternativement et, par suite, toute opération exécutée au moyen d'un nombre pair d'opérations  $a$  et  $b$  reviendra à une puissance de  $ab$ , puisque  $ba$ , comme on vient de le voir, est une puissance de  $ab$ . Une opération exécutée au moyen d'un nombre impair d'opérations  $a$  et  $b$  revient, soit à

$$a(ba)^u = a(ab)^{tu-u},$$

soit à

$$b(ab)^v = a(ab)^{v+1}.$$

Cela étant ainsi, si l'on réduit les exposants de  $ab$  à leur moindre valeur positive (mod  $t$ ), toute opération exécutée au moyen de  $a$  et de  $b$  reviendra soit à un terme de la suite

$$ab, (ab)^2, (ab)^3, \dots, (ab)^t,$$

soit à un terme de la suite

$$a(ab), a(ab)^2, a(ab)^3, \dots, a(ab)^t.$$

L'opération  $ab$  appartenant à l'exposant  $t$ , chaque suite n'aura que des termes différents entre eux. Disons plus : aucun terme de la seconde suite ne peut être égal à un terme de la première.

En effet, dans ce cas, on aurait

$$a(ab)^u = (ab)^v,$$

et, par suite, soit

$$a = (ab)^{v-u},$$

soit

$$a = (ab)^{v-u+t}$$

suivant que  $v$  est plus grand ou plus petit que  $u$ .

De sorte que tant  $a$  que  $b$  se réduiraient à des puissances de  $ab$ , ce qui entraînerait la commutativité

$$ab = ba,$$

contrairement à la supposition que les opérations  $a$  et  $b$  ne sont pas commutatives. L'ordre du sous-groupe engendré par  $a$  et  $b$  est donc bien  $2t$ .

### I. — LE GROUPE DE GALOIS A 60 ÉLÉMENTS.

Pour ce groupe, le plus simple des trois, nous allons nous servir de considérations géométriques.

On sait que c'est Hamilton <sup>(1)</sup> qui a eu le premier l'idée d'appliquer l'icosaèdre (ou le dodécaèdre) à l'étude du groupe qui nous occupe en ce moment.

Cela étant ainsi, chaque côté de direction donnée de la *fig.* 97 dans Lucas représente un élément du groupe de Galois à 60 éléments, et il y a lieu de considérer les opérations suivantes <sup>(2)</sup> (nous supprimons celles qui sont inutiles) :

1° L'opération  $\iota$  qui *renverse* (ou retourne bout pour bout) une ligne de la figure.

2° L'opération  $\lambda$  qui change une ligne considérée comme un côté d'un pentagone en le côté suivant, en marchant toujours à *main droite*.

3° L'opération  $\omega$  qui change une *arête* du dodécaèdre pentagonal en l'*arête opposée* de ce solide.

Hamilton montre que les opérations  $\lambda$  et  $\iota$ , de périodes 5 et 2 respectivement, suffisent à elles seules pour engendrer le groupe.

J'introduis encore une opération  $\chi$  qui consiste à changer une *arête* du dodécaèdre en l'*arête opposée*, à changer de direction et à faire un pas à droite comme pour l'opération  $\lambda$ , le tout considéré comme une seule et unique opération. L'opération  $\chi$  sera réci-

---

<sup>(1)</sup> *Memorandum respecting a new System of Roots of Unity* (*Philosophical Magazine*, p. 446; 1856), trad. dans Lucas, *Récréations mathématiques*, vol. II, p. 326, où l'on trouvera aussi, à la page suivante, la traduction d'un autre extrait d'Hamilton sur le même sujet.

<sup>(2)</sup> LUCAS, *Ouvrage cité*, page 237.

proque et, comme on aura

$$\lambda = \omega \iota \chi,$$

il est clair que les trois opérations réciproques  $\iota$ ,  $\chi$  et  $\omega$  suffiront pour engendrer le groupe de Galois à elles seules.

## II. — LE GROUPE DE GALOIS A 168 ÉLÉMENTS.

Ce groupe peut être défini à l'aide des permutations des quantités

$$\infty, 0, 1, 2, 3, 4, 5, 6$$

qu'on obtient en leur faisant subir toutes les transformations qui changent  $\omega$  en

$$\frac{\alpha\omega + \beta}{\gamma\omega + \delta} \pmod{7},$$

où  $\alpha, \beta, \gamma, \delta$  sont des nombres entiers pris suivant le module 7 et satisfaisant à la congruence

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{7}.$$

Cela étant ainsi, je considère trois opérations réciproques du groupe

$$\varphi \equiv \frac{\omega + 4}{3\omega + 6}, \quad \chi \equiv \frac{4\omega + 1}{4\omega + 3}, \quad \psi \equiv \frac{6}{\omega} \pmod{7}.$$

Soit  $n$  l'ordre du sous-groupe engendré par les opérations  $\varphi$ ,  $\chi$  et  $\psi$ . On aura

$$\chi\psi \equiv \frac{3\omega + 4}{4\omega + 1} \pmod{7},$$

expression qui appartient à l'exposant 4 et, par conséquent, les opérations  $\chi$  et  $\psi$ , à elles seules, engendreront un sous-groupe d'ordre 8 en vertu du lemme II.

Comme de plus

$$\varphi\chi \equiv \frac{1}{6\omega + 6} \pmod{7}$$

appartient à l'exposant trois et

$$\varphi\chi\psi \equiv \omega + 1 \pmod{7}$$

appartient à l'exposant sept, il faut bien que le nombre  $n$  soit un multiple de 8, de 3 et de 7. Or, comme ce même nombre  $n$  doit être un diviseur de 168, on aura  $n = 168$ , ce qui veut dire que les

opérations  $\varphi$ ,  $\chi$  et  $\psi$  engendreront à elles seules le groupe de Galois à 168 éléments.

### III. — LE GROUPE DE GALOIS A 660 ÉLÉMENTS.

Ce groupe se définit d'une manière analogue, sauf que le nombre 11 prend la place du nombre 7. Il y a lieu, par conséquent, de considérer toutes les transformations qui changent  $\omega$  en

$$\frac{\alpha\omega + \beta}{\gamma\omega + \delta} \pmod{11},$$

où  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$  sont des nombres entiers pris suivant le module 11 et satisfaisant à la congruence

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{11}.$$

Cela étant ainsi, je considère les opérations réciproques

$$\varphi \equiv \frac{9\omega + 7}{4\omega + 2} \pmod{11},$$

$$\chi \equiv \frac{5\omega + 8}{5\omega + 6} \pmod{11},$$

$$\psi \equiv \frac{4}{8\omega} \pmod{11}.$$

On s'assure immédiatement que

$$\varphi\chi \equiv \frac{7}{3\omega + 3} \pmod{11}$$

appartient à l'exposant cinq; que

$$\varphi\psi \equiv \frac{5\omega + 8}{6\omega + 1}$$

appartient à l'exposant six; et enfin que

$$\varphi\chi\psi \equiv \omega + 1 \pmod{11}$$

appartient à l'exposant onze.

L'ordre du sous-groupe engendré par  $\varphi$ ,  $\chi$  et  $\psi$ , devant être en même temps un multiple de cinq, douze et onze et un diviseur de 660, sera égal au nombre 660 lui-même, ce qui prouve la proposition que nous avons en vue.