Transcription de l'extrait (pages 44 à 47) de l'Encyclopédie des sciences mathématiques pures et appliquées de Jules Molk, volume 3, tome 1 de théorie des nombres, consacré aux imaginaires de Galois.

24. Imaginaires de Galois. L'étude des congruences des degrés supérieurs est facilitée par l'introduction des *imaginaires de Galois*.

Lorsque $F(x)$ est une fonction-première (mod. p), de degré $\pi > 1$, la congruence irréductible

$$F(x) \equiv 0 \text{ (mod. } p),$$

n'a aucune solution entière. Dans ce cas, *E. Galois*[1] introduit un symbole i auquel s'appliquent, par définition, les mêmes règles de calcul qu'aux nombres naturels et qui est, en outre, supposé tel que l'on ait

$$F(i) \equiv 0 \text{ (mod. } p).$$

On peut dire que i est une *solution imaginaire* de la congruence irréductible $F(x) \equiv 0$ (mod. p) ; rien n'empêche d'imaginer par exemple que i est une des racines de l'équation irréductible $F(x) = 0$. *E. Galois* a d'ailleurs mis en pleine lumière les avantages que l'on peut tirer de cette façon de parler, dans la théorie des congruences[2].

Une congruence de la forme

$$\varphi(x) \equiv \psi(x) \text{ (modd. } p, F(x)),$$

est complètement équivalente à la congruence

$$\varphi(i) \equiv \psi(i) \text{ (mod. } p).$$

On appelle *imaginaire de Galois*, toute fonction rationnelle entière de i, à coefficients entiers ; la condition nécessaire et suffisante pour qu'une imaginaire de Galois $f(i)$ soit $\equiv 0$ (mod. p), est que $f(x)$ soit $\equiv 0$ (modd. $p, F(x)$). Si l'on envisage comme égales deux imaginaires de Galois congrues (mod. p), il n'y a qu'un nombre limité p^π d'imaginaires de Galois distinctes, parmi lesquelles une seule est nulle tandis que $(p-1)$ sont congrues (mod. p) aux $(p-1)$ premiers nombres naturels ; chacune de ces p^π imaginaires de Galois peut être mise sous la forme

$$f(i) = a_0 + a_1 i + a_2 i^2 + \ldots + a_{n-1} i^{n-1} \text{ (mod. } p),$$

où $a_0, a_1, a_2, \ldots, a_{n-1}$ sont des nombres entiers que l'on peut choisir parmi les nombres $0, 1, 2, ..., p-1$.

Le produit de plusieurs imaginaires de Galois ne peut être $\equiv 0$ (mod. p) que si l'une de ces imaginaires est $\equiv 0$ (mod. p). A chaque imaginaire de Galois différente de 0 (mod. p), correspond une imaginaire associée $f_1(i)$ telle que l'on ait

$$f(i) f_1(i) \equiv 1 \text{ (mod. } p).$$

Réédition aux éditions Jacques Gabay de volumes édités de 1904 à 1916 par Gauthier-Villars et B.G.Teubner.
Transcription : Denise Vella-Chemla, août 2023.

[1] Cf. *P. Bachmann*, Niedere Zahlentheorie 1, p. 393, in *P. Bachmann, W. F. Meyer*, (eds) Encyklopädie der Mathematischen Wissenschaften mit Einschluss ihrer Anwendungen.

[2] Cf. *É. Borel* et *J. Drach*, Introd. à l'étude de la théorie des nombres, d'après des conférences de *J. Tannery*, Paris 1895, p. 58.

Lorsqu'on introduit les imaginaires de Galois, aux théorèmes démontrés pour les congruences prises suivant un système de modules $p, F(x)$, correspondent les théorèmes suivants concernant les congruences prises suivant un module p.

Chacune des p^π imaginaires de Galois $f(i)$ est racine de la congruence

$$x^{p^\pi} \equiv x \text{ (mod. } p),$$

en sorte que cette congruence a autant de racines que l'indique son degré.

Les racines de la *congruence fundamentale* $F(x) \equiv 0 \text{ (mod } p)$ sont $i, i^p, i^{p^2}, \ldots, i^{p^{\pi-1}}$.

Quelle que soit la congruence fondamentale $F(x) \equiv 0 \text{ (mod. } p)$ servant à définir les imaginaires de Galois, le nombre des racines (imaginaires de Galois) d'une congruence quelconque $\Phi(x) \equiv 0 \text{ (mod. } p)$ est au plus égal au degré de cette congruence.

Toute imaginaire de Galois $f(i)$ *appartient à un exposant* n qui divise $p^n - 1$; à chaque diviseur n de $p^n - 1$ appartiennent $\varphi(n)$ nombres $f(i)$; la congruence $x^{p^\pi} - x \equiv 0 \text{ (mod. } p)$ a $\varphi(p^\pi - 1)$ *racines primitives* $f(i)$ qui sont incongrues et *appartiennent* à l'exposant $p^\pi - 1$.

Chacune de ces $\varphi(p^\pi - 1)$ racines primitives est, comme i elle-même, racine d'une congruence irréductible de degré π, et ses puissances donnent toutes les racines de la congruence

$$x^{p^\pi} \equiv x \text{ (mod. } p),$$

c'est à dire des quantités $f(i)$ toutes incongrues. Ainsi les racines de la congruence[3]

$$x^{i^3} \equiv x \text{ (mod. } 7)$$

peuvent toutes, puisque $i^3 \equiv 2 \text{ (mod. } 7)$ est irréductible, se mettre sous la forme

$$a_0 + a_1 i + a_2 i^2 \text{ (mod. } 7);$$

on trouve comme racine primitive

$$j = i - i^2$$

c'est à dire une racine de la congruence irréductible

$$j^3 - j + 2 \equiv 0 \text{ (mod. } 7),$$

et toutes les racines de la congruence $x^{343} \equiv x \text{ (mod. } 7)$ sont aussi de la forme

$$a_0 + a_1 j + a_2 j^2 \text{ (mod. } 7).$$

Si m est le nombre auquel *convient* $f(i)$, c'est-à-dire le plus petit nombre naturel pour lequel $[f(i)]^{p^m-1} \equiv 1 \text{ (mod. } p)$, m est un diviseur de π, et si $a_1, a_2, a_3, \ldots, a_k$ sont les nombres premiers inégaux qui divisent m, le nombre naturel

$$p^m + \sum_{(i)} p^{\frac{m}{a_i}} + \sum_{(i<k)} p^{\frac{m}{a_i a_k}} - \sum_{(i<k<l)} p^{\frac{m}{a_i a_k a_l}} + \ldots \pm p^{\frac{m}{a_1 a_2 \ldots a_k}},$$

[3] *E. Galois*, Œuvres, publiées par É. Picard, Paris, 1897, p. 19 ; cf. *J. A. Serret*, Alg. sup. (5e éd.), 2, Paris 1885, p. 181.

où les sommes sont formées comme il a été expliqué plus haut, in-dique combien, parmi les nombres incongrus $f(i)$, il y en a qui *conviennent* à m.

Les puissances

$$f(i), [f(i)]^p, [f(i)]^{p^2}, ..., [f(i)]^{p^{m-1}},$$

sont les racines d'une congruence irréductible $\Phi(x) \equiv 0$ (mod. p) de degré m, en sorte que toute fonction symétrique entière de ces puissances, à coefficients entiers, est congrue (mod. p) à un nombre entier ; réciproquement, toute congruence entière à coefficients entiers, à laquelle satisfait $f(i)$, a, en même temps, ces puissances pour racines.

Si π est le degré de la congruence fondamentale $F(x) \equiv 0$ (mod. p) au moyen de laquelle on introduit les imaginaires de Galois, toute congruence *irréductible* $\Phi(x) \equiv 0$ (mod. p), dont le degré est un diviseur de π, a un nombre de racines égal à son degré, tandis que toute congruence *irréductible* $\Phi(x) \equiv 0$ (mod. p) dont le degré n'est pas diviseur de π n'admet pas de racine (imaginaire de Galois).

Si $\Psi(x) \equiv 0$ (mod. p) est une congruence quelconque, entière à coefficients entiers, si $f(x), f_1(x), ...$ sont les fonctions premières de degrés respectifs $\mu, \mu_1, \ldots$ dont $\Psi(x)$ est le produit (mod. p), si enfin π désigne le p.p.c.m. de $\mu, \mu_1, \ldots$, il existe une fonction-première $F(x)$ de degré π ; si l'on introduit l'imaginaire de Galois i définie par la relation

$$F(i) \equiv 0 \text{ (mod. } p),$$

la congruence $\Psi(x) \equiv 0$ (mod. p) aura un nombre de racines (imaginaires de Galois) égal à son degré.

Il suffit de rapprocher ce théorème du théorème fondamental de l'Algèbre pour avoir nettement conscience de l'utilité de l'introduction des imaginaires de Galois dans la Théorie des nombres. Ce théorème a d'ailleurs donné lieu à mainte application, notamment dans la Théorie des substitutions[4].

[4]Voir à ce sujet *C. Jordan*, Traité des substitutions, Paris 1870 ; cf I. 8.