Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 22 (1921-1922)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: UN CHAPITRE DE MÉTHODOLOGIE MATHÉMATIQUE LES IMAGINAIRES DE GALOIS

Autor: Stuyvaert, M.

DOI: https://doi.org/10.5169/seals-515741

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: 13.07.2025

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

UN CHAPITRE DE MÉTHODOLOGIE MATHÉMATIQUE, LES IMAGINAIRES DE GALOIS

PAR

M. STUYVAERT (Gand).

Considérons deux polynomes à coefficients entiers,

$$F(x) = a_0 x^m + a_1 x^{m-1} + \dots + a_m ,$$
$$f(x) = b_0 x^n + b_1 x^{n-1} + \dots + b_n$$

et soit $m \geqq n$. L'étude de ces fonctions relativement à un MODULE PREMIER P a été commencée dans un chapitre antérieur de notre Cours de Méthodologie: on y a montré l'existence et l'unicité de la *congruence fondamentale*,

$$F(x) - f(x)Q(x) - R(x) \equiv 0 \qquad (\text{mod. } p)$$

où $R(x)$ est de degré inférieur à n.

On dit que $F(x)$ est *divisible* par $f(x)$ suivant le module p, si le polynome $R(x)$ ci-dessus est congru à zéro, donc s'il existe un polynome $Q(x)$ tel que le polynome $F(x) - f(x)\,Q(x)$ ait tous ses coefficients multiples de p, ce qui s'écrit

$$F(x) \equiv f(x)\,Q(x) \ . \qquad (\text{mod. } p)$$

Quand cette condition n'est pas satisfaite, la congruence fondamentale donne lieu à la même suite d'opérations que l'algorithme d'Euclide pour le p. g. c. d.

Alors, si un polynome $\psi(x)$ divise (mod. p) les polynomes $F(x)$ et $f(x)$; il divise $R(x)$, car soient

$$F(x) \equiv \psi(x)\,G(x) \ , \qquad f(x) \equiv \psi(x)\,g(x) \qquad (\text{mod. } p)$$

il en résulte que

$$\psi(x)\,G(x) - \psi(x)\,g(x)\,Q(x) - R(x)$$

a tous ses coefficients multiples de p ou que $R(x)$ est divisible (mod. p) par $\psi(x)$. On voit de même que si un polynome divise (mod p) $f(x)$ et $R(x)$, il divise (mod. p) $F(x)$.

Les divisions successives de l'algorithme d'Euclide, appliquées à $F(x)$ et $f(x)$ doivent aboutir, parce que le degré des restes décroît. En dernier lieu on trouve, ou bien un reste ayant tous ses coefficients congrus à zéro, et alors l'avant-dernier reste $D(x)$ divise (mod. p) le précédent et tous ceux qui viennent avant lui, notamment $F(x)$ et $f(x)$; — ou bien un reste indépendant de x mais non multiple de p et alors les deux polynomes donnés ne sont pas divisibles par un même polynome.

Il faut encore établir l'unicité du p. g. c. d. (mod. p), c'est-à-dire du polynome de degré le plus élevé divisant (mod p) $F(x)$ et $f(x)$: s'il y en a un autre, il divise les restes successifs, donc le p. g. c. d. déjà trouvé et comme ils doivent être de même degré, le quotient est indépendant de x.

On appelle *polynome irréductible* suivant le module p un polynome qui n'est pas congru au produit de deux polynomes.

On a démontré dans un chapitre antérieur ceci: si $f(x) \equiv 0$ (mod. p) a une racine α, le polynome $f(x)$ est divisible (mod. p) par $x - \alpha$; et la réciproque est immédiate. Donc un polynome irréductible de degré supérieur à 1 n'a pas de racine; mais la réciproque n'est pas exacte, car un polynome peut n'avoir aucune racine et cependant être réductible; il est alors congru au produit de facteurs irréductibles de degré supérieur à 1.

Il est facile de former des polynomes irréductibles du second degré, pour un module premier impair quelconque, 7 par exemple. Le polynome $x(x-1) - d$ ne peut avoir que des diviseurs du premier degré; donc, s'il n'a pas de racine, il est irréductible; or il n'a pour racine, ni 1, ni 0, si d n'est pas $\equiv 0$ (mod. 7); remplaçons x par 2, 3, 4, 5, 6 dans $x(x-1)$; nous aurons cinq résultats qui peuvent être, dans le cas le plus défavorable, non congrus entre eux pour le module 7; il reste toujours au moins une valeur de d qui n'est congrue ni à zéro, ni à ces cinq résultats

$[2(2-1) \equiv 2\ ;\ 3(3-1) \equiv 6\ ;\ 4(4-1) \equiv 5\ ;\ 5(5-1) \equiv 6\ ;\ 6(6-1) \equiv 2]$

on peut prendre pour d toute valeur non congrue à 0, 2, 5, 6; par conséquent

$$x(x-1)-1\ , \qquad x(x-1)-3\ , \qquad x(x-1)-4$$

sont des polynomes irréductibles (mod. 7). La même méthode réussit encore pour des congruences du troisième degré, parce que tout polynome cubique réductible a au moins un facteur linéaire. Nous verrons plus loin l'existence de polynomes irréductibles de tous les degrés.

THÉORÈME. *Tout polynome irréductible* $P(x)$ *qui divise* (*mod.* p) *un produit de deux polynomes* $F(x)$ $G(x)$ *divise* (*mod.* p) *un des facteurs.*

1° Si $P(x)$ est de degré égal ou inférieur à $F(x)$ et s'il ne divise pas $F(x)$, on forme, au moyen de l'algorithme d'Euclide, la suite de polynomes

$$F(x)\ , \qquad P(x)\ , \qquad R(x)\ , \qquad R'(x)\ , \ldots n$$

qui doit aboutir, puisque $P(x)$ est irréductible, à un entier n non multiple de p. Multiplions par $G(x)$ tous les termes de la suite; $P(x)$ divisant FG et PG divise RG,R'G,...nG, donc aussi $wn\mathrm{G} \equiv \mathrm{G}$, w étant l'entier, toujours existant et unique, tel que $wn \equiv 1$ (mod. p).

2° Si $F(x)$ est de degré inférieur à $P(x)$ la suite de polynomes a pour premier terme $P(x)$, pour second terme $F(x)$, et la démonstration s'achève comme ci-dessus.

Corollaires. Si les congruences

$$F(x) \equiv 0\ ; \qquad f(x) \equiv 0\ ; \qquad \text{(mod. } p)$$

ont une racine commune α, le binome $x-\alpha$ divise (mod. p) les deux polynomes $F(x)$ et $f(x)$. Donc il y a un p. g. c. d. (mod. p) $D(x)$ de $F(x)$ et $f(x)$. Visiblement toute racine de $D(x)$ est racine de $F(x)$ et $f(x)$. Mais si ce p. g. c. d. n'existe pas ou s'il est irréductible et de degré supérieur à 1, $F(x)$ et $f(x)$ n'ont aucune racine commune.

On démontre, comme pour les nombres entiers, que

$$D(x) \equiv F(x)g(x) + f(x)G(x) \qquad \text{(mod. } p)$$

$G(x)$ et $g(x)$ étant deux polynomes.

De tout ceci résulte, comme dans la théorie des polynomes algébriques, qu'un polynome est congru, d'une seule manière, à un produit de polynomes irréductibles, avec les conséquences habituelles.

Application. Toute racine α, non multiple de p, de la congruence

$$f(x) \equiv 0 \qquad (\text{mod. } p)$$

est aussi racine de $x^{p-1} - 1$; donc $f(x)$ et $x^{p-1} - 1$ ont un p. g. c. d. (mod. p) $D(x)$; on le calcule par l'algorithme d'Euclide. Le polynome $D(x)$ a autant de racines que l'indique son degré, car, comme il divise $x^{p-1} - 1$, il est congru à un produit de binomes tels que $x - \alpha$.

Si $f(x)$ a moins de racines que son degré ne l'indique, il est congru au produit de facteurs binomes affectés peut-être d'exposants, et peut-être de polynomes irréductibles. Le calcul effectué à l'instant fournit le produit $D(x)$ des facteurs binomes chacun avec l'exposant 1.

Comme on a

$$x^{p-1} - 1 \equiv D(x)\,Q(x)$$

on ne doit résoudre que celle des deux congruences $D(x) \equiv 0$, $Q(x) \equiv 0$ qui a le moindre degré; et cette remarque ramène la résolution de toute congruence à celle d'une congruence de degré au plus égal à $\frac{p-1}{2}$.

Toute congruence douée d'autant de racines *distinctes* que l'indique son degré divise (mod. p) l'expression $x^{p-1} - 1$; mais ceci n'est plus vrai s'il y a des racines multiples: par exemple $(x - \alpha)^2(x - \beta)$ ne divise pas (mod. p) le polynome $x^{p-1} - 1$, car alors $x^{p-1} - 1$ pourrait se décomposer en facteurs irréductibles de deux manières [1].

Avant d'aborder la recherche des congruences irréductibles, nous devons établir ce lemme d'analyse combinatoire:

Si $\Gamma_{m,n}$ *désigne le nombre de combinaisons à répétition de* m *lettres prises* n *à* n, *on a la formule*

$$(k-1)\,\Gamma_{p-1,k} + (k-2)\,p\,\Gamma_{p-1,k-1} + (k-3)\,p^2\Gamma_{p-1,k-2} + \cdots$$
$$+ 2p^{k-3}\Gamma_{p-1,3} + p^{k-2}\Gamma_{p-1,2} + \Gamma_{p,k} = p^k\,. \qquad (1)$$

[1] *Exercice.* Décomposer en facteurs irréductibles, suivant le module 7, le polynome $x^5 - 3x^4 - 2x^3 - 2x^2 - x - 2$. (V. J. Serret, *Alg. sup.*).

La formule se vérifie pour $k = 2$, car on a, dans ce cas

$$\Gamma_{p-1,2} + \Gamma_{p,2} = \frac{p(p-1)}{2} + \frac{p(p+1)}{2} = p^2 .$$

Supposons donc la formule démontrée pour le nombre k et appliquons ensuite à $k + 1$,

$$\begin{aligned} k\Gamma_{p-1,k+1} + (k-1)p\Gamma_{p-1,k} + (k-2)p^2\Gamma_{p-1,k-1} + \cdots \\ + 2p^{k-2}\Gamma_{p-1,3} + p^{k-1}\Gamma_{p-1,2} + \Gamma_{p,k+1} = p^{k+1} ; \end{aligned} \tag{2}$$

multiplions la formule (1) par p et soustrayons de (2), il vient

$$k\Gamma_{p-1,k+1} + \Gamma_{p,k+1} = p\Gamma_{p,k}$$

ou encore

$$\frac{(p-1)p(p+1)\ldots(p+k-1)}{1.2.3\ldots(k+1)} + \frac{p(p+1)\ldots(p+k)}{1.2\ldots(k+1)}$$
$$= p\,\frac{p(p+1)\ldots(p+k-1)}{1.2\ldots k} ,$$

ce qui se vérifie en divisant les deux membres par

$$\frac{p(p+1)\ldots(p+k-1)}{1.2\ldots k} ;$$

on obtient en effet l'identité

$$\frac{k(p-1)}{k+1} + \frac{p+k}{k+1} = p .$$

THÉORÈME. *Suivant un module premier* p *il y a des congruences irréductibles de tout degré* k; *leur nombre est au moins*

$$(k-1)\Gamma_{p-1,k}$$

en appelant $\Gamma_{m,n}$ *le nombre de combinaisons à répétition de* m *objets pris* n *à* n [1].

Dans cet énoncé ne sont pas considérées comme distinctes deux congruences dont l'une s'obtient en multipliant l'autre par un facteur constant. Cette opération est en effet sans influence sur la réductibilité et nous pouvons toujours débuter par la *préparation* connue des congruences qui consiste à rendre égal à l'unité le coefficient du terme le plus élevé en x.

[1] Cf. *Encyc. des sc. math.*, t. I, vol. 3, fasc. 1, p. 41.

Dès lors les congruences

$$x^2 + ax + b \equiv 0$$

sont en nombre p^2, puisque a et b peuvent prendre les valeurs de 0 à $p - 1$. Pour avoir celles qui sont irréductibles, il faut écarter celles qui ont la forme $(x - i)(x - j)$, où i et j prennent des valeurs, distinctes ou égales, de 0 à p — 1, leur nombre est $\Gamma_{p,2}$. Le nombre des congruences irréductibles du second degré est donc

$$p^2 - \Gamma_{p,2} = 1 \,.\, \Gamma_{p-1,2}$$

Supposons la formule $(k - 1)\,\Gamma_{p-1,k}$ établie pour toutes les congruences jusque et y compris celles d'ordre $k - 1$. Enumérons les p^k congruences d'ordre k: celles qui ont k racines sont en nombre $\Gamma_{p,k}$; celles qui sont le produit d'un polynome irréductible du second degré par un autre polynome quelconque sont en nombre $p^{k-2}\,\Gamma_{p-1,2}$ et ainsi de suite; le lemme ci-dessus donne pour résidu

$$(k - 1)\,\Gamma_{p-1,k} \,.$$

Seulement si un polynome d'ordre k est congru au produit de trois facteurs irréductibles par exemple d'ordres h, i, j par des facteurs binomes, il figure trois fois parmi les congruences exclues et il faut rétablir le nombre exact en ajoutant $2\,\Gamma_{p,k-h-i-j}$. Si $h + i + j$ est égal à k, il n'y a pas d'autre correction de ce chef; mais si $h + i + j < k$, il y a eu des erreurs analogues dans l'énumération des polynomes réductibles d'ordre $k - 1$, etc., et il faut retrancher

$$2\,\Gamma_{k-1,k-h-i-j-1} \,.\quad \text{etc} \;;$$

or on vérifie que si $k > \alpha$,

$$\Gamma_{k,\alpha} > \Gamma_{k-1,\alpha-1} + \Gamma_{k-2,\alpha-2} + \cdots + \Gamma_{k-\alpha+1,1} + 1 \;,$$

car la chose est visible pour $\alpha = 1$ quel que soit k; supposons-la démontrée pour $\Gamma_{k-1\,\alpha-1}$; nous constatons que

$$\Gamma_{k,\alpha} = \Gamma_{k,\alpha-1} + \Gamma_{k-1,\alpha}$$

d'où pareillement

$$\Gamma_{k,\alpha} = \Gamma_{k-1,\alpha-1} + \Gamma_{k,\alpha-2} + \Gamma_{k-1,\alpha-1} + \Gamma_{k-2,\alpha} > \Gamma_{k-1,\alpha-1} + \Gamma_{k-1,\alpha-1}$$

ce dernier terme est par hypothèse supérieur à

$$\Gamma_{k-2,\alpha-2} + \Gamma_{k-3,\alpha-3} + \cdots$$

donc *a fortiori* on a l'inégalité à démontrer.

Ce qui précède ne démontre pas seulement l'existence de congruences irréductibles de tout degré, mais donne un moyen théorique de les déterminer toutes. En effet, pour une congruence quelconque, la solution n'exige qu'un nombre fini d'essais. Seulement les calculs étant fort longs, il est bon de chercher quelque moyen de les raccourcir.

Pour les congruences de second et troisième ordre, la question de l'irréductibilité se confond avec celle de n'avoir pas de racine; c'est pourquoi nous dirons quelques mots de ce dernier problème.

Le système de classes de restes pour un module premier constitue un CORPS. Par conséquent, on peut appliquer ici tout ce que l'algèbre enseigne sur le résultant de deux équations en x, car la théorie du résultant ne comporte que des opérations rationnelles. Par exemple, on a ce théorème relatif à deux congruences (que nous supposons *préparées*),

$$\left.\begin{aligned} F &\equiv x^m + a_1 x^{m-1} + \ldots + a_m \equiv 0 \\ G &\equiv x^n + b_1 x^{n-1} + \ldots + b_n \equiv 0 \end{aligned}\right\} . \qquad (\text{mod. } p)$$

Pour que les deux polynomes F, G *aient un p. g. c. d.* (*mod. p*) δ *contenant* x, *il faut et il suffit que*

$$\Delta = \begin{vmatrix} 1 & . & . & 1 & . & . \\ a_1 & 1 & . & b_1 & 1 & . \\ a_2 & a_1 & . & b_2 & b_1 & . \\ . & a_2 & . & . & b_2 & . \\ a_m & . & . & b_n & . & . \\ . & a_m & . & . & b_n & . \end{vmatrix} = M \, . \, p \, .$$

La remarque faite à l'instant dispense de démonstration; toutefois, nous consignons ici le raisonnement entièrement calqué sur celui qui concerne les équations algébriques.

Si F et G ont un p. g. c. d. (mod. p) δ contenant x, on a identiquement

$$F \equiv \delta U \quad \text{ou} \quad \delta(u_0 x^{m-1} + u_1 x^{m-2} + \dots u_{m-1}) \equiv 0 \quad (\text{mod.}\, p)$$

$$G \equiv \delta V \quad \text{ou} \quad \delta(v_0 x^{n-1} + v_1 x^{n-2} + \dots v_{n-1}) \equiv 0 \quad \text{»}$$

d'où identiquement

$$FV \equiv GU \qquad (\text{mod.}\, p)$$

ou

$$\left.\begin{array}{l} u_0 - v_0 \equiv 0 \\ b_1 u_0 + u_1 - a_1 v_0 - v_1 \equiv 0 \\ \dots\dots\dots\dots \end{array}\right\} \qquad (\text{mod.}\, p)$$

les polynomes U, V sont de degrés maximés $m - 1$ et $n - 1$; un au moins des coefficients u n'est pas multiple de p, soit u_{k-1}; multiplions ces dernières congruences par les mineurs relatifs à la $k^{\text{ième}}$ colonne du déterminant Δ; nous obtenons $\Delta u_{k-1} = M \,.\, p$ et p ne divisant pas u_{k-1}, divise Δ.

Réciproquement, si $\Delta = Mp$, multiplions les lignes du déterminant Δ par les puissances x^{m+n-1}, x^{m+n-2}, ... x, 1 de l'indéterminée x et additionnons: la dernière ligne devient ainsi

$$x^{n-1} F \,, \quad x^{n-2} F \,, \quad \dots F \,, \quad x^{m-1} G \,, \quad x^{m-2} G \,, \quad \dots G$$

et en développant Δ suivant cette dernière ligne, on a identiquement

$$FV - GU \equiv 0 \qquad (\text{mod}\, p)$$

or on a, par la théorie du *p. g. c. d.* (mod p), identiquement

$$V.\, p.\, g.\, c.\, d.\, (F, G) \equiv p.\, g.\, c.\, d.\, (FV, GV) \equiv p.\, g.\, c.\, d.\, (GU, GV)$$
$$\equiv G\; p.\, g.\, c.\, d.\, (U, V) \;;$$

or G est de degré n et V est de degré moindre, donc le *p. g. c. d.* (F, G) contient effectivement x.

Corollaire. Pour que la congruence

$$x^n + a_1 x^{n-1} + \dots a_n \equiv 0 \qquad (\text{mod.}\, p)$$

ait une racine non multiple de p, il faut et il suffit qu'elle ait

une racine commune avec

$$x^{p-1} - 1 \equiv 0$$

d'où

$$\begin{vmatrix} 1 & . & . & 1 & . & . \\ a_1 & 1 & . & 0 & 1 & . \\ a_2 & a_1 & . & 0 & 0 & . \\ . & a_2 & . & . & 0 & . \\ a_n & . & . & -1 & . & . \\ . & a_n & . & . & -1 & . \end{vmatrix} = \mathrm{M} \cdot p \ .$$

Comme APPLICATION, cherchons, pour le module 5, les congruences irréductibles du second degré.

Le déterminant suivant doit être non multiple de 5,

$$\begin{vmatrix} 1 & . & . & . & 1 & . \\ a_1 & 1 & . & . & 0 & 1 \\ a_2 & a_1 & 1 & . & 0 & 0 \\ . & a_2 & a_1 & 1 & 0 & 0 \\ . & . & a_2 & a_1 & -1 & 0 \\ . & . & . & a_2 & . & -1 \end{vmatrix} ;$$

ce déterminant développé

$$1 - a_1^4 + a_2^4 + 4a_1^2 a_2 - 2a_2^2$$

ne contient que les puissances paires de a_1, c'est-à-dire que les trinomes irréductibles ont la forme

$$x^2 \pm a_1 x + a_2 \ .$$

Pour $a_2 \equiv \pm 1$, on doit avoir

$$1 - a_1^4 + 1 \pm 4a_1^2 - 2 = -a_1^2(a_1^2 \mp 4) \text{ non multiple de } 5 \ ;$$

dont on doit exclure

$$a_2 \equiv 1 \quad \text{avec} \quad a_1 \equiv 0 \quad \text{ou} \quad 2$$
$$a_2 \equiv -1 \quad \text{»} \quad a_1 \equiv 0 \quad \text{ou} \quad 1 .$$

Pour $a_2 \equiv \pm 2$, on doit avoir

$$1 - a_1^4 + 16 \pm 8 a_1^2 - 8 \equiv 4 a_1^4 \pm 8 a_1^2 + 4 = 4 \left(a_1^2 \pm 1\right)^2$$

non multiple de 5; donc il faut exclure

$$a_2 = 2 , \qquad a_1 = 2 ,$$
$$a_2 = -2 , \qquad a_1 = 1 .$$

En résumé les trinomes irréductibles sont

$$x^2 \pm x + 1 , \quad x^2 \pm 2x - 1 , \quad x^2 \pm x + 2 , \quad x^2 \pm 2x - 2 , \quad x^2 \pm 2 ;$$

la dernière formule est connue, puisque $+2$ et -2 sont les non résidus quadratiques pour le module 5.

Examinons de plus près le résultant de $x^{p-1} - 1$ et de

$$F(x) \quad \text{ou} \quad x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a^n \, (n < p - 1) ,$$

$$\Delta = \left| \begin{array}{cccccccc}
1 & & & & 1 & & & \\
0 & 1 & & & a_1 & 1 & & \\
0 & 0 & 1 & & a_2 & a_1 & 1 & \\
. & 0 & 0 & . & . & a_2 & a_1 & . \\
. & . & 0 & . & a_n & . & a_2 & . \\
-1 & . & . & . & & a_n & . & . \\
 & -1 & . & . & & & a_n & . \\
 & & -1 & . & & & & . \\
 & & & . & & & & . \\
\underbrace{\qquad\qquad}_{n \text{ col.}} & & & & \underbrace{\qquad\qquad}_{p-1 \text{ col.}} & & &
\end{array} \right|$$

ajoutons la première ligne à la $p^{\text{ième}}$, la $2^{\text{ième}}$ à la $(p+1)^{\text{ième}}$ ... la $n^{\text{ième}}$ à la $(p+n-1)^{\text{ième}}$; alors le déterminanta partiel

des n premières lignes et colonnes se réduit à son terme principal, et l'on peut supprimer les n premières lignes et colonnes, donc

$$\Delta = \left|\begin{array}{cccccc} a_n & & & a_1 & 1 & . \\ . & a_n & & a_2 & a_1 & . \\ . & . & & . & a_2 & . \\ 1 & . & . & a_n & . & . \\ a_1 & 1 & . & . & a_n & . \\ a_2 & a_1 & . & . & . & . \\ . & a_2 & . & . & . & \\ . & . & . & 1 & & \\ \multicolumn{4}{c}{\underbrace{\qquad\qquad}_{n \text{ col.}}} & \multicolumn{2}{c}{\underbrace{\qquad}_{p-n-1}} \end{array}\right|$$

Pour une CONGRUENCE BINOME $x^n + q \equiv 0$, le résultant est

$$\left|\begin{array}{cccccc} q & & & 1 & & \\ . & q & & . & 1 & \\ . & . & q & . & . & . \\ 1 & . & . & q & . & . \\ & 1 & . & & q & . \\ & & 1 & . & & . \\ & & & . & & . \end{array}\right| ;$$

développons: le terme principal est q^{p-1}; prenons un élément q de la diagonale principale et remplaçons-le par l'élément 1 de la même colonne, mais, comme on ne peut prendre qu'un élément dans chaque ligne, il faut remplacer un second élément de la diagonale principale situé à un intervalle n du premier, en descendant la diagonale ou en reprenant au début si besoin, etc. Si donc n est premier avec $p - 1$, on ne revient au point de départ qu'après avoir épuisé la diagonale principale; pour amener tous les éléments 1 sur la diagonale principale, il faut faire un nombre impair $p - 2$ d'échanges de lignes; donc le déterminant développé est $q^{p-1} - 1$; or ceci est congru à zéro pour toute valeur de q, donc, *si n est premier avec $p - 1$, $x^n + q \equiv 0$ n'a pas de racine.*

Si n et $p-1$ ont un p.g.c.d δ, on revient au point de départ après avoir pris $\frac{p-1}{\delta}$ éléments q de la diagonale principale et les avoir remplacés par des éléments 1, ce qui nécessite $\frac{p-1}{\delta}-1$ échanges de lignes ou un changement de signe si $\frac{p-1}{\delta}$ est pair et donne un terme en $q\left(\frac{p-1}{\delta}\right)(\delta-1)$; on peut faire ceci de δ manières, puis on doit prendre de ces groupes 2 à 2, 3 à 3, etc., finalement le déterminant développé est

$$q^{\frac{p-1}{\delta}\delta} \mp \delta q^{\frac{p-1}{\delta}(\delta-1)} + \frac{\delta(\delta-1}{2} q^{\frac{p-1}{\delta}(\delta-2)} + \ldots = \left(q^{\frac{p-1}{\delta}} \mp 1\right)^{\delta}$$

or $q^{\frac{p-1}{\delta}} \mp 1$ est un diviseur algébrique de $q^{p-1}-1$ et a $\frac{p-1}{\delta}$ racines; donc $x^n + q \equiv 0$ est possible pour $p-1-\frac{p-1}{\delta}$ valeurs de q. On retrouve des résultats connus, mais avec ceci de curieux que les polygones de Poinsot apparaissent sur la diagonale d'un déterminant (on rendrait la chose plus saisissante en enroulant le déterminant sur un cylindre).

Remarque. Non seulement la théorie de l'élimination d'une inconnue entre deux équations se transporte aux congruences, mais aussi la même théorie pour plusieurs équations. Ainsi pour que deux congruences aient une racine commune, il ne suffit pas que le résultant soit M.p. car il pourrait y avoir un p.g. c. d. irréductible d'ordre supérieur à 1, mais que les deux congruences aient une racine commune avec $x^{p-1}-1$, ce qui peut s'exprimer en posant que tous les déterminants extraits d'une matrice soient M. p. Etc. (Voir notre *Algèbre à deux dimensions*, Gand, 1920).

Arrivons à la définition des IMAGINAIRES DE GALOIS[1]. Le module p étant premier, soit $f(x)$ un polynome irréductible de degré $n > 1$. Il n'a pas de racine. Posons néanmoins

$$f(i) \equiv 0 \; ; \qquad \text{(mod. } p\text{)}$$

[1] V. *Encyc. sc. math.*, t. I, vol. 3, fasc. 1, p, 44; BOREL-DRACH, *Introduct. à la théorie des nombres, etc.*

i ne désigne pas $\sqrt{-1}$; c'est ici le symbole d'un entier imaginaire, symbole vide de sens, car l'opération est impossible par hypothèse. Son calcul s'établit par des conventions:

Convenons de dire que deux expressions $\varphi(i)$, $\psi(i)$ sont *congrues* et d'écrire

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

quand la différence des polynomes $\varphi(x)$ et $\psi(x)$ est égale terme à terme à une expression

$$\mathrm{R}f(x) + \mathrm{S}p$$

où R et S sont des polynomes en x à coefficients entiers. On exprime la chose en écrivant

$$\varphi(x) - \psi(x) \equiv 0 \; ; \qquad (\text{mod. } p, f(x)) \qquad (1)$$

cette congruence à *deux modules* est d'après notre hypothèse, vérifiée pour tout entier réel x.

La convention est permise, car dans le cas particulier où $f(x)$ est réductible et a pour racine l'entier réel i, on a $f(i) = \mathrm{Q}p$ et, d'après la relation (1),

$$\varphi(i) - \psi(i) = (\mathrm{RQ} + \mathrm{S})p \equiv 0 \qquad (\text{mod. } p)$$

Tout polynome $\varphi(i)$ en i à coefficients entiers réels est une IMAGINAIRE DE GALOIS. D'après nos conventions, elle ne peut être $\equiv 0$ (mod p) que si l'on a

$$\varphi(x) \equiv 0 \; . \qquad (\text{mod. } p, f(x))$$

Elle sera dite *racine* de la congruence $\mathrm{F}(z) \equiv 0$ (mod. p) si l'on a $\mathrm{F}(\varphi(i)) \equiv 0$ (mod. p), c'est-à-dire

$$\mathrm{F}(\varphi(x)) \equiv 0 \; ; \qquad (\text{mod. } p, f(x))$$

en particulier i est *racine* de la congruence fondamentale $f(z) \equiv 0$ (mod. p).

A cause de l'hypothèse $f(i) \equiv 0$, on peut abaisser toute imaginaire de Galois au-dessous du degré n: on divise algébriquement $\varphi(z)$ par $f(z)$ et l'on prend le reste; de plus, on peut abaisser tous les coefficients au-dessous de p.

Les imaginaires de Galois ont donc la forme

$$g = a_0 + a_1 i + a_2 i^2 + \dots a_{n-1} i^{n-1}$$

où les cœfficients ont les valeurs de 0 à $p - 1$: il y a p^n imaginaires distinctes (non congrues pour le mod. p). Pour $a_1 = a_2 = \dots a_{n-1} = 0$, on a, comme cas particulier, les entiers réels.

Convenons de faire, terme à terme la SOMME de deux imaginaires, et leur PRODUIT comme si c'étaient deux polynomes, et d'abaisser au-dessous du degré n par la congruence initiale $f(z) \equiv 0$.

Si le produit $g_1(i) \,.\, g_2(i)$ est congru à 0 (mod. p), c'est, d'après nos conventions, que $g_1(x) \,.\, g_2(x) \equiv 0$ (mod. p, $f(x)$) ou que $g_1(x) \,.\, g_2(x)$ est divisible (mod. p) par $f(x)$; mais un polynome irréductible qui divise (mod. p) un produit, divise un des facteurs, donc *le produit* $g_1(x) \,.\, g_2(x)$ *ne peut être congru à* 0 (*mod.* p) *que si l'un des facteurs est congru à* 0 (*mod.* p). Cette propriété s'étend immédiatement à plusieurs facteurs.

Si l'on multiplie l'imaginaire A non $\equiv 0$ (mod. p) par les p^n imaginaires distinctes, on a des produits distincts, car s'il y en avait deux, Ag_1 et Ag_2, congrus pour le mod. p, on aurait $A\,(g_1 - g_2) \equiv 0$ (mod. p) et comme A n'est pas $\equiv 0$, g_1 et g_2 ne sont pas distincts. Par suite, la congruence linéaire $AX \equiv B$ (mod. p), et en particulier $AX \equiv 1$ a toujours une racine et une seule.

Si l'on pose $Ag \equiv g'$ (mod. p) et qu'on fasse parcourir à g les $p^n - 1$ imaginaires distinctes, non $\equiv 0$, g' parcourt les mêmes imaginaires, et en multipliant membre à membre,

$$\left(A^{p^n - 1} - 1\right) \pi g \equiv 0 \qquad \text{(mod. } p\text{)}$$

et comme πg n'est pas $\equiv 0$, on a la formule analogue à celle du THÉORÈME DE FERMAT,

$$A^{p^n - 1} \equiv 1 \qquad \text{(mod. } p\text{)}$$

ou encore, quelle que soit l'imaginaire A, même $\equiv 0$,

$$A^{p^n} - A \equiv 0 \qquad \text{(mod. } p\text{)}$$

Ceci signifie, d'après nos conventions, que si $f(x)$ est irréductible suivant le module p et $\theta(x)$ un polynome quelconque,

$$[\theta(x)]^{p^n} - \theta(x)$$

est divisible (mod. p) par $f(x)$.

Les imaginaires de Galois relatives à un polynome irréductible constituent un *corps* puisque les quatre opérations fondamentales s'y pratiquent comme pour les classes de reste (mod. p). Par conséquent la division algébrique s'étend sans autre démonstration, aux POLYNOMES A COEFFICIENTS IMAGINAIRES DE GALOIS.

Entrons toutefois dans quelque détail. Soit

$$\varphi(x) = g_0(i)x^m + g_1(i)x^{m-1} + \dots g_m(i)$$

un polynome entier en x à coefficients imaginaires de Galois. L'imaginaire $\theta(i)$ est dite racine de $\varphi(x)$ si l'on a

$$\varphi[\theta(i)] \equiv 0 \; ; \qquad \text{(mod. } p)$$

comme le premier membre s'obtient par des additions et multiplications, cette congruence a un sens, d'après nos conventions.

Le polynome $\varphi(x)$ est identiquement nul pour le module p si tous ses coefficients sont $\equiv 0$ (mod. p); dans ce cas la congruence $\varphi(x) \equiv 0$ est satisfaite par une imaginaire quelconque.

Le produit de deux polynomes pareils ne peut être identiquement nul (mod. p) que si l'un des facteurs l'est. Car soient A le premier coefficient non nul du premier polynome et B celui du second; on sait que AB n'est pas $\equiv 0$. Par suite le degré d'un produit de polynomes est la somme des degrés des facteurs.

Un polynome $\varphi(x)$, entier en x et i est divisible (mod. p) par un autre pareil $\psi(x)$ non identiquement nul (mod. p) si l'on peut former un polynome $\pi(x)$ tel que l'expression

$$\varphi(x) - \psi(x)\pi(x)$$

soit identiquement nulle (mod. p).

Soit $\varphi(x)$ de degré au moins égal à $\psi(x)$. Dire que $\psi(x)$ est de degré m c'est dire que le coefficient B_0 de x^m est une imaginaire de Galois non $\equiv 0$; on a toujours et d'une seule manière,

$$(\Gamma) \quad \varphi(x) \equiv \psi(x)Q(x) + R(x) \qquad \text{(mod. } p)$$

où $R(x)$ est de degré inférieur à $\psi(x)$. Car en comparant les coefficients des puissances successives de x dans les deux membres, on détermine les coefficients de $Q(x)$ puis ceux de $R(x)$ sans ambiguïté, chaque fois par une congruence linéaire. D'où la théorie du p. g. c. d. avec les propriétés habituelles. Nous aurons à revenir sur cette congruence fondamentale (Γ).

Mais d'abord voici un CAS PARTICULIER. Soit le polynome $\varphi(x)$ ayant pour racine l'imaginaire g_1. On peut former la congruence

$$\varphi(x) \equiv (x - g_1)\, Q(x) + R \qquad (\text{mod. } p)$$

où R est de degré inférieur à $x - g_1$ donc indépendant de x. Cette congruence étant identique, on peut remplacer x par g_1 et, comme $\varphi(x_1) \equiv 0$, on obtient $R \equiv 0$, donc $\varphi(x)$ est divisible (mod. p) par $x - g_1$. Soit g_2 une *autre* racine,

$$\varphi(g_2) \equiv (g_2 - g_1)\, Q(g_2) \qquad (\text{mod. } p)$$

et comme le premier membre est congru à 0 et que $g_2 - g_1$ ne l'est pas, g_2 est racine de $Q(x)$ et $\varphi(x)$ est divisible par $(x - g_1)(x - g_2)$. etc. Ainsi, une congruence d'ordre m ne peut avoir qu'une racine de plus que la congruence d'ordre $m - 1$ et, de proche en proche, une congruence ne peut avoir plus de racines que ne l'indique son degré, à moins d'être identique.

Un rôle spécial revient au polynome $x^{p^n} - x$ qui a pour racines toutes les imaginaires de Galois, donc autant que l'indique son degré; il est congru au produit

$$x\,(x - g_1)\,(x - g_2) \ldots ,$$

$g_1, g_2 \ldots$ étant toutes les imaginaires. Soit $F(x)$ un autre polynome ayant la même propriété: on a

$$F(x) \equiv (x^{p^n} - x)\, q(x) + r(x) \qquad (\text{mod. } p)$$

$F(x)$ et $(x^{p^n} - x)$ étant $\equiv 0$ pour toutes les imaginaires de Galois, il en est de même de $r(x)$ qui a donc plus de racines que ne l'indique son degré et disparaît.; donc tout polynome ayant pour racines toutes les imaginaires de Galois est de la forme

$$(x^{p^n} - x)\, \pi(x)$$

où $\pi(x)$ est un polynome arbitraire.

Soit deux POLYNOMES A COEFFICIENTS RÉELS, $F(x)$ et $F_1(x)$, soit D leur p. g. c. d. (mod. p); on sait que l'on peut trouver deux polynomes G, G_1 tels que

$$D - FG_1 - F_1 G$$

ait tous ses coefficients (réels) multiples de p.

Dire que l'imaginaire de Galois $g(i)$ est racine de F et F_1, c'est dire que $F(g(x))$ et $F_1(g(x))$ sont divisibles (mod. p) par $f(x)$; il en est de même de D $(g(x))$. Ainsi les racines communes à F et F_1, tant réelles qu'imaginaires de Galois, sont racines de $D(x)$.

Or $x^{p^n} - x$ a pour racines toutes les imaginaires de Galois, donc les racines de $F(x)$ sont racines du p. g. c. d. (mod. p) $\Delta(x)$ de $F(x)$ et $x^{p^n} - x$.

$\Delta(x)$ polynome à coefficients réels divise (mod. p) $F(x)$; si $F(x)$ est irréductible (mod. p), $\Delta(x)$ est ou bien indépendant de x, ou bien congru à $F(x)$; donc une congruence irréductible à coefficients réels a, ou bien aucune racine imaginaire de Galois, ou bien en a autant que l'indique son degré, car $\Delta(x)$ est diviseur (mod. p) de $x^{p^n} - x$.

En particulier $f(x)$ est irréductible, de degré n, à coefficients réels et a une racine imaginaire i, donc elle en a n, et $f(x)$ divise (mod. p) le polynome $x^{p^n} - x$. Celui-ci est donc divisible (mod. p) par *tout* polynome irréductible de degré n, car $f(x)$ a été choisi arbitrairement.

De même si l'entier r divise n, l'entier $p^r - 1$ divise $p^n - 1$, et le polynome $x^{p^r-1} - 1$ divise algébriquement $x^{p^n-1} - 1$.

Ainsi toute congruence irréductible dont le degré r est n ou un diviseur de n a autant de racines imaginaires de Galois que l'indique son degré.

Toute autre congruence irréductible est privée de racine. Car on sait, d'après les propriétés des coefficients binomiaux, que

$$(a + b + c + \ldots)^p \equiv a^p + b^p + c^p + \ldots \qquad (\text{mod. } p)$$

donc

$$(a + bx + cx^2 + \ldots)^p \equiv a^p + b^p x^p + c^p x^{2p} + \ldots \qquad (\text{mod. } p)$$

et ceci d'après le théorème de Fermat, est congru à

$$a + bx^p + cx^{2p} + \ldots ,$$

c'est-à-dire que

$$(\varphi(x))^p \equiv \varphi(x^p) \; ; \qquad (\text{mod. } p)$$

remplaçons x par x^p,

$$\varphi(x^{p^2}) \equiv (\varphi(x^p))^p \equiv \left((\varphi(x)^p)\right)^p \equiv (\varphi(x))^{p^2} \qquad (\text{mod. } p)$$

et, de proche en proche,

$$[\varphi(x)]^{p^r} \equiv \varphi(x^{p^r}) \qquad (\text{mod. } p)$$

A présent si un polynome irréductible de degré n pouvait diviser $x^{p^r} - x$ dans l'hypothèse $r < n$, ce polynome définirait une imaginaire de Galois i qui serait racine de $x^{p^r} - x$, donc on aurait

$$i^{p^r} \equiv i \; , \qquad \text{d'où} \qquad \varphi(i^{p^r}) \equiv \varphi(i) \qquad (\text{mod. } p)$$

et, d'après la remarque précédente,

$$\varphi(i^{p^r}) \equiv (\varphi(i))^{p^r} \equiv \varphi(i)$$

c'est-à-dire que la congruence $x^{p^r} - x$ aurait pour racine toute expression $\varphi(i)$ donc toutes les imaginaires déduites de i en nombre p^n, et aurait plus de racines que son degré ne l'indique.

Ainsi $x^{p^n} - x$ ne peut être divisible (mod. p) par un polynome irréductible de degré supérieur à n.

Enfin, si $n = mq + r$ $(0 < r < m)$, l'expression $x^{p^n} - x$ ne peut être divisible par un polynome irréductible $F(x)$ de degré m, car $x^{p^{mq}} - x$ est divisible par $F(x)$ d'après un résultat trouvé à l'instant, $x^{p^n} - x$ l'est aussi par hypothèse, donc $F(x)$ divise (mod. p) leur différence

$$x^{p^{mq+r}} - x^{p^{mq}}$$

et celle-ci d'après une remarque ci-dessus est congrue à

$$(x^{p^r} - x)^{p^{mq}}$$

et n'est pas divisible par $F(x)$ puisque $r < m$ (un polynome irréductible qui divise un produit $(x^{p^r} - x)^{p^{mq}}$ divise un facteur $x^{p^r} - x$).

En résumé, $x^{p^n} - x$ *est le produit de tous les polynomes irréductibles dont les degrés sont* n *ou des diviseurs de* n.

Signalons comme *corollaire* facile ou exercice (cf. Encyc., t. I, v. 3, fasc. 1, p. 42): si N est le nombre des congruences irréductibles d'ordre n, on a

$$nN = p^n - \sum_{(i)} p^{\frac{n}{a_i}} + \sum_{(i<k)} p^{\frac{n}{a_i a_k}} - \sum_{(i<k<l)} p^{\frac{n}{a_i a_k a_l}} + \dots \pm p^{\frac{n}{a_1 a_2 \dots a_n}},$$

où la première somme est étendue à tous les facteurs premiers inégaux $a_1, a_2, \dots a_n$ de n, la seconde à toutes les combinaisons 2 à 2 de ces facteurs, ...et où l'exposant du dernier terme est le quotient de n par le produit de ces facteurs.

Autre *corollaire*: $x^{p^n} - x$ n'a pas de facteurs multiples, car s'il avait la forme $f^\alpha g^\beta h^\gamma \dots$, le produit $fgh\dots$ contenant toutes les imaginaires de Galois serait de degré au moins égal à $x^{p^n} - x$.

Terminons par une propriété connue des CORPS A UN NOMBRE FINI D'ÉLÉMENTS (Encyc., t. I, v. 2, fasc. 2, p. 249):

Les seuls corps à un nombre fini d'éléments sont ceux formés par les classes de restes suivant un module premier auxquelles on adjoint une imaginaire de Galois.

D'abord les multiples successifs de l'unité absolue doivent aboutir à zéro, donc constituer une classe de restes et nous avons vu au chapitre *Corps et Domaines* que, pour avoir un *corps*, il faut prendre un module premier p.

Ensuite, on ne peut, au corps de classes de restes (mod. p) *adjoindre* une quantité i de manière à avoir un nouveau corps à un nombre fini d'éléments que si i est une imaginaire de Galois. Car i, i^2, i^3.... sont des éléments du nouveau corps : comme il n'y en a qu'un nombre fini, on doit avoir à la fin

$$i^m = \frac{\alpha + \beta i + \gamma i^2 + \dots \mu i^{m-1}}{\alpha' + \beta' i + \gamma' i^2 + \dots \mu' i^{m-1}}$$

le second membre existe puisque l'on a un *corps*, et multiplié par le dénominateur il donne le numérateur, ainsi i est racine d'une équation ou plutôt congruence à coefficients du corps initial; si celle-ci est réductible, un des facteurs irréductibles doit être nul, car c'est une propriété essentielle du corps qu'on produit ne s'annule que si un des facteurs s'évanouit; ainsi i est une imaginaire de Galois.

Supposons à présent deux éléments i et j adjoints au corps de classes de restes (mod. p). Les puissances successives étant en nombre infini, une relation identique doit permettre d'exprimer les puissances de i à partir de la $h^{\text{ième}}$ et celles de j à partir de la $k^{\text{ième}}$ au moyen des puissances précédentes.

Ces deux relations ne peuvent être les mêmes, car soit pour fixer les idées, $i^2 + j^2 \equiv 1$; utilisons-la pour ne garder que $1, i, j, j^2$ et exprimons j^3; nous aurons

$$j^3 \equiv j^2 \cdot j \equiv j(1 - i^2) \equiv j - ji^2 \equiv j - j(1 - j^2) \equiv j^3 \ ;$$

nous retombons sur j^3 et cela provient de ce que remplaçant i^2 et j^2 tirés de la même relation, nous aboutissons à une identité.

Ainsi il y a deux relations *distinctes* entre i et j; nous pouvons en *éliminer* j ou i car c'est une opération rationnelle, donc i et j sont séparément imaginaires de Galois, et de même, de proche en proche pour plusieurs éléments adjoints.

Montrons enfin que l'adjonction simultanée de deux (pour fixer les idées) imaginaires i, j, équivaut à une adjonction unique. Soit i définie par une congruence $f(x) \equiv 0$ irréductible d'ordre n et j par une congruence $\varphi(x)$ d'ordre n'; les polynomes $f(x)$, $\varphi(x)$ divisent respectivement

$$x^{p^n - 1} - 1 \qquad \text{et} \qquad x^{p^{n'} - 1} - 1 \ ;$$

soit μ un multiple commun quelconque de n et n'; $p^\mu - 1$ est divisible par $p^n - 1$ et par $p^{n'-1}$ donc

$$x^{p^\mu - 1} - 1$$

est divisible algébriquement par $x^{p^n} - 1$ et $x^{p^{n'}} - 1$; il existe des polynomes irréductibles d'ordre μ; l'un d'eux définit des imaginaires de Galois et d'après le théorème précédent, i et j sont exprimables par les nouvelles imaginaires.