PROPRIÉTÉS ARITHMÉTIQUES DES ENTIERS ALGÉBRIQUES

Autor(en): **Marchay, R.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **31 (1932)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-24617

PROPRIÉTÉS ARITHMÉTIQUES DES ENTIERS ALGÉBRIQUES

PAR

R. MARCHAY (Rouen).

---

1. — Dans une Note publiée dans le *Sphinx-Œdipe* (1926, p. 129) sous le titre *Equation générale des diviseurs premiers d'un polynome*, nous avons démontré le théorème suivant:

Si F (x) *et* G (x) *sont deux polynomes à coefficients entiers, le premier coefficient de chaque polynome étant l'unité, en outre* a_1, a_2, a_3, ... *étant les racines de* F (x) *et* b_1, b_2, b_3, ... *étant celles de* G (x); *tout diviseur commun aux deux polynomes, pour une même valeur de* x, *divise les deux expressions*

$$\Pi G(a_j) \qquad \text{et} \qquad \Pi F(b_j)$$

qui sont deux nombres entiers égaux.

Nous développerons ici les théories exposées dans la Note citée en appliquant surtout la proposition rappelée.

Nous donnerons une généralisation de l'équation des diviseurs premiers, et terminerons par certaines congruences relatives aux entiers algébriques et à leurs polynomes générateurs.

2. — *Deux polynomes* F (x) *et* G (x) *irréductibles (c'est-à-dire ne pouvant être décomposés en des produits de polynomes à coefficients rationnels) dont les racines sont des entiers algébriques ne peuvent avoir qu'un nombre fini de diviseurs communs pour deux valeurs de* x *dont la différence* d *demeure finie, et, ces diviseurs restent tous inférieurs à la plus grande valeur absolue de*

$$\Pi G(a_j - d)$$

les a_j *étant les racines de* F (x).

D'après le théorème rappelé plus haut, tout diviseur commun à F (x) et G $(x - d)$ pour une valeur donnée de d, divise

$$\Pi\, G(a_j - d) \ ;$$

donc si F (x) et G (x) ont un nombre infini de diviseurs communs correspondants à deux valeurs de x dont la différence d reste finie, l'expression

$$\Pi\, G(a_j - d)$$

étant divisible par une infinité de nombres, pour un nombre fini de valeurs de d, il y a au moins une valeur de cette expression qui est nulle. Il y a donc un polynome G $(x - d)$ qui a une racine commune avec F (x).

Or cette conclusion est impossible; en effet, G (x) étant irréductible, il en est de même de G $(x - d)$, et les opérations du plus grand commun diviseur donnent pour celui-ci, une constante rationnelle ou un polynome à coefficients rationnels. C'est ce dernier cas qui se présenterait si F (x) et G $(x - d)$ avaient une ou plusieurs racines communes. Ils ne seraient donc pas irréductibles. Les deux polynomes ne peuvent donc pas avoir de racines communes.

$$\Pi\, G(a_j - d)$$

n'étant jamais nulle, a toujours sa valeur absolue au moins égale à ses diviseurs.

3. — *Si* F (x) *est un polynome à coefficients entiers dont le premier est l'unité (c'est-à-dire à racines entiers algébriques) et si* p *est un diviseur premier de* F (x), *il divise*

$$\Pi\left[(a_j + u)^m - 1\right]$$

pour m *valeurs de* u, *non congruentes*, m *étant un diviseur de* p — 1, *et les* a_j *étant les racines de* F (x).

p divise $x^m - 1$ pour m valeurs non congruentes de x.

Soient x_0 entier tel que

$$F(x_0) \equiv 0 \qquad (\text{mod. } p)$$

et x_1 entier tel que

$$x_1^m - 1 \equiv 0 \qquad (\text{mod. } p.)$$

posons

$$x_1 - x_0 = u \,. \qquad x_1 = u + x_0 \,;$$

p divise à la fois

$$(x_0 + u)^m - 1 \qquad \text{et} \qquad F(x_0) \,,$$

c'est-à-dire

$$(x + u)^m - 1 \qquad \text{et} \qquad F(x)$$

pour $x = x_0$.

Donc (n° 1)

$$\prod \left[(a_j + u)^m - 1\right] \equiv 0 \,. \qquad (\text{mod. } p) \qquad (1)$$

Or, il y a une valeur de u correspondante à toute racine de

$$x^m - 1 \equiv 0$$

donc il y a m valeurs de u racines de (1).

Dans tout ce qui suit, la lettre p désignera toujours un nombre premier.

4. — En particulier, si

$$F(x) = x^n - 1$$

n étant diviseur de $p - 1$, ce polynome admet p comme diviseur.

On a d'ailleurs

$$a_j = \cos\frac{2j\pi}{n} - i\sin\frac{2j\pi}{n} \,; \qquad 1 \leq j \leq n$$

Donc, *si* m *et* n *divisent* p — 1, *on a*

$$\prod_n^1 \left(\left[\cos\frac{2j\pi}{n} - i\sin\frac{2jn}{n} + u\right)^m - 1\right] \equiv 0 \qquad (\text{mod. } p)$$

pour m *valeurs de* u.

5. — *Si* $f_1(t)$ *et* $f_2(t)$ *sont deux polynomes dont les coefficients des termes de même degré sont congruents* (mod. u) *et si les entiers*

algébriques $x_1, x_2, x_3, \ldots, x_m$ *sont les racines d'un même polynome, une fonction symétrique rationnelle entière, à coefficients entiers des* $f_1(x_j)$ *est congruente (mod.* u*) à une fonction semblable des* $f_2(x_j)$.

Soient Φ_1 et Φ_2, les deux fonctions symétriques.

Posons

$$f_1(t) = A_n t^n + \ldots + A_1 t + A_0$$

$$f_2(t) = B_n t^n + \ldots + B_1 t + B_0$$

on a

$$B_k = A_k + M_k u ,$$

les M_k étant entiers.

Dès lors Φ_2 est un polynome en u dont les coefficients sont fonctions rationnelles entières, à coefficients entiers des x_j, des M_k et des A_k. Pour $u = 0$ elle se réduit à Φ_1, d'où

$$\Phi_2 - \Phi_1 = P u ,$$

P étant une fonction rationnelle, etc., des x_j et de u. L'interversion de deux des x_j, quand u est quelconque, n'altère pas cette fonction, c'est donc, quand u est entier, une fonction symétrique, à coefficients entiers des x_j seuls et, par suite, une fonction rationnelle, etc., des coefficients de l'équation génératrice des x_j, donc un nombre entier.

6. — *Si les entiers algébriques* $x_1, x_2, \ldots x_m$, *sont les racines du polynome* F (x), *on a, pour toute valeur entière de* x, *la congruence*

$$F(x) \Pi \left[(x - x_j)^{p-1} - 1\right] \equiv F(0) \Pi \left(x_j^{p-1} - 1\right) . \qquad (\text{mod. } p)$$

On a identiquement

$$(x - t)^{p-1} - 1 = x^{p-1} - (p-1) x^{p-2} t + \ldots + t^{p-1} - 1 \qquad (1)$$

et

$$t\left(\frac{x^{p-1} - t^{p-1}}{x - t}\right) = x^{p-2} t + x^{p-3} t^2 + \ldots + t^{p-1} . \qquad (2)$$

Si x est premier à p, le terme indépendant de t dans le second membre de (1) qui est

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

est multiple de p et, par suite, congruent au terme correspondant dans le second membre de (2) qui est nul.

Le coefficient de t dans (1) est

$$-(p-1)\,x^{p-2}$$

congruent à x^{p-2} coefficient de t dans (2).

En général, les nombres combinatoires

$$p-1,\ \frac{(p-1)(p-2)}{1\cdot 2},\ \ldots$$

sont respectivement congruents à

$$-1\ ,\ +1\ ,\ -1\ ,\ \ldots$$

par suite, les coefficients dans (1) sont respectivement congruents à

$$x^{p-2}\ ,\ x^{p-3}\ ,\ \ldots\ \text{et}\ 1$$

qui sont les coefficients dans (2).

On a donc, en vertu du théorème précédent et des identités (1) et (2)

$$\Pi\left[(x-x_j)^{p-1}\right] \equiv \Pi\, x_j \left(\frac{x^{p-1}-x_j^{p-1}}{x-x_j}\right) \qquad (\text{mod. } p)$$

$$\equiv \Pi - x_j \left(\frac{x_j^{p-1}-x^{p-1}}{x-x_j}\right)$$

$$\equiv \frac{F(0)}{F(x)}\,\Pi\left(x_j^{p-1}-x^{p-1}\right)$$

$$F(x)\,\Pi\left[(x-x_j)^{p-1}-1\right] \equiv F(0)\,\Pi\left(x_j^{p-1}-x^{p-1}\right). \qquad (3)$$

Or

$$t^{p-1}-x^{p-1} \qquad \text{et} \qquad t^{p-1}-1$$

sont deux polynomes dont les coefficients correspondants, par rapport à t, sont congruents; en leur appliquant le théorème n° 5, on a

$$\Pi\left(x_j^{p-1}-x^{p-1}\right) \equiv \Pi\left(x_j^{p-1}-1\right)$$

qui, par multiplication par F (0) et substitution dans (3) donne la congruence de l'énoncé.

Si x est multiple de p, la congruence est évidente.

7. — Dans le théorème précédent, si p divise F (x) pour une valeur entière de x, et ne divise pas F (0), il divise

$$\Pi\left(x_j^{p-1} - 1\right)$$

Réciproquement, si p divise ce produit et est non diviseur de

$$\Pi\left[(x - x_j)^{p-1} - 1\right]$$

pour une certaine valeur de x, il divise F (x) pour cette valeur.

8. — *Si les entiers algébriques* $x_1, x_2, \ldots x_m$ *sont les racines d'un même polynome* F (x), *on a, pour toute valeur de* x, *la congruence:*

$$F(x) \equiv \Pi\left(x - x_j^p\right) \qquad (\text{mod. } p)$$

On a

$$\Pi\left(x - x_j\right)^p = \Pi\left(x^p - px^{p-1}x_j + \ldots - x_j^p\right).$$

Les nombres combinatoires d'ordre p sont tous multiples de p sauf le premier et le dernier qui sont égaux à l'unité, et x^p est congruent à x.

Les deux polynomes en t,

$$x - t^p \qquad \text{et} \qquad x^p - px^{p-1}t + \frac{p(p-1)}{2}x^{p-2}t^2 + \ldots - t^p$$

ont leurs coefficients respectivement congruents.

Par suite on a (n° 5):

$$\Pi\left(x - x_j^p\right) \equiv \Pi\left(x - x_j\right)^p = F^p(x) \equiv F(x). \qquad (\text{mod. } p)$$