GAZETA MATEMATICĂ

REVISTĂ DE CULTURĂ MATEMATICĂ PENTRU TINERET

SERIA B

Fondată în anul 1895

ANUL CXIV nr. 6 **iunie 2009**

ARTICOLE ŞI NOTE MATEMATICE

LEMA LUI MERTENS ŞI APLICAŢII

MARCEL ŢENA[1)]

Abstract. The article presents a proof of the irreducibility of the cyclotomic polynomials and two applications of this result: the form of the endomorphisms of a cyclotomic field and the solutions for $\cos \frac{2\pi}{n} = x+y\sqrt{z}$, $n \in \mathbb{N}, x, y, z \in \mathbb{Q}$.

Keywords: primitive root, cyclotomic polynomial, cyclotomic field, irreducible polynomial.

MSC : 12E05, 12F05.

Preliminarii. Pentru $n \in \mathbb{N}^*$, notăm $\zeta = \cos \dfrac{2\pi}{n} + \mathrm{i} \sin \dfrac{2\pi}{n}$. Grupul ciclic:

$$U_n = \left\{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\right\} = \{x \in \mathbb{C} \mid x^n = 1\}$$

se numeşte *grupul rădăcinilor de ordinul n ale unităţii.*

Generatorii acestui grup (elementele de ordin n ale grupului) se numesc *rădăcini primitive de ordin n ale unităţii* şi sunt numerele:

$$\zeta^k, \quad \text{cu} \quad 0 \leq k \leq n-1, \quad (k,n) = 1.$$

Numărul rădăcinilor primitive de ordinul n ale unităţii este $\varphi(n)$, unde φ este indicatorul lui *Euler*.

Polinomul monic de grad minim, verificat de toate rădăcinile primitive de ordinul n ale unităţii, adică polinomul:

$$\Phi_n(X) = \prod_{\substack{0 \leq k \leq n-1 \\ (k,n)=1}} \left(X - \zeta^k\right)$$

se numeşte *al n-lea polinom ciclotomic.*

1) Profesor dr., Colegiul Naţional „Sf. Sava“, Bucureşti.

Polinomul $\Phi_n(X)$ are gradul $\varphi(n)$ şi coeficienţii săi sunt numere întregi (v. [8], teorema 13, pag. 22).

Corpul $\mathbb{Q}(\zeta) = \left\{ \dfrac{u(\zeta)}{v(\zeta)} \middle| u, v \in \mathbb{Q}[X],\ v(\zeta) \neq 0 \right\}$ este cel mai mic subcorp al corpului $\mathbb{C}$ care îl conţine pe ζ şi se numeşte *al n-lea corp ciclotomic.*

Rezultatele principale. Vom demonstra acum că polinomul ciclotomic $\Phi_n(X)$ este ireductibil în inelul $\mathbb{Q}[X]$. Această demonstraţie se bazează pe următoarea importantă:

Lemă (Mertens). *Dacă $f(X)$ este un polinom monic cu coeficienţi întregi, astfel ca $f(\zeta) = 0$, atunci $f(\zeta^k) = 0$ pentru orice $0 \leq k \leq n-1$, $(k, n) = 1$.*

Demonstraţie. (*Landau* [4], preluată şi în [8]). De la bun început facem precizarea că în rolul lui ζ în această lemă poate fi oricare dintre rădăcinile de ordinul n ale unităţii. Fixăm o rădăcină ε a polinomului $f(X)$ şi un întreg $i \in \{0, 1, \ldots, n-1\}$. Împărţind polinomul $f(X^i)$ prin polinomul $f(X)$ şi făcând apoi $X = \varepsilon$, obţinem că $f(\varepsilon^i) = g(\varepsilon)$, unde $g \in \mathbb{Z}[X]$ este restul împărţirii şi $\operatorname{grad}(g) < \operatorname{grad}(f)$. Considerăm toate aceste posibile polinoame $g \in \mathbb{Z}[X]$, când ε parcurge rădăcinile lui $f(X)$, iar i parcurge numerele $0, 1, \ldots, n-1$. Numărul acestor polinoame g este finit, prin urmare putem vorbi de maximul modulelor coeficienţilor acestor polinoame g, fie acestea A. Să fixăm un număr prim $p > A$. Dacă $p \equiv i_0 \pmod{n}$, cu $0 \leq i_0 \leq n-1$, rezultă $f(\zeta^p) = f(\zeta^{i_0}) = g_0(\zeta)$, unde g_0 este unul din polinoamele g de mai înainte. Coeficienţii lui $f(\zeta^p)$, fiind coeficienţii lui g_0, au modulele $\leq A < p$. Cum $f(\zeta) = 0$, avem însă $f(\zeta^p) = f(\zeta^p) - f(\zeta)^p$ şi, folosind teorema lui *Fermat*, rezultă că toţi coeficienţii lui $f(\zeta^p)$ se divid cu p. Prin urmare, toţi coeficienţii lui $f(\zeta^p)$ sunt nuli, deci $f(\zeta^p) = 0$.

Fie acum q un întreg care are în descompunerea sa doar factori primi $> A$, deci $q = p_1 p_2 \ldots p_s$, cu $p_1, p_2, \ldots, p_s > A$, nu neapărat distincte. Luând $p = p_1$, rezultă $f(\zeta^{p_1}) = 0$. Luând apoi în rolul lui ζ pe ζ^{p_1} şi în rolul lui p pe p_2, rezultă $f\left(\zeta^{p_1 p_2}\right) = 0$. Din aproape în aproape găsim că $f\left(\zeta^{p_1 p_2 \cdots p_s}\right) = 0$, adică $f\left(\zeta^q\right) = 0$.

Pentru un k din ipoteză, deci $0 \leq k \leq n-1$, $(k, n) = 1$, să luăm $q_0 = k + n \prod p$, unde produsul se face după toate numerele prime $p \leq A$, astfel încât p nu divide k. Deoarece $(k, n) = 1$, rezultă că q_0 nu are factori primi $\leq A$, adică q_0 are doar factori primi $> A$.

În baza celor de mai sus, avem $f\left(\zeta^{q_0}\right) = 0$ şi cum $q_0 \equiv k \pmod{n}$, rezultă $f\left(\zeta^k\right) = 0$.

Teoremă (Gauss-Dedekind). *Polinomul ciclotomic $\Phi_n(X)$ este ireductibil în inelul de polinoame $\mathbb{Q}[X]$.*

Demonstraţie. Polinomul $\Phi_n(X)$ se descompune în factori ireductibili în inelul $\mathbb{Z}[X]$. Notăm cu $f(X)$ acel factor ireductibil, monic, al lui $\Phi_n(X)$, pentru care $f(\zeta) = 0$. Conform lemei lui *Mertens*, vom avea $f\left(\zeta^k\right) = 0$, pentru orice $0 \leq k \leq n-1$, $(k,n)=1$. Aşadar, polinomul $f(X)$ are toate rădăcinile polinomului $\Phi_n(X)$, de unde rezultă că $f(X)=\Phi_n(X)$. Dar $f(X)$ este ireductibil în $\mathbb{Z}[X]$ şi atunci $\Phi_n(X)$ este un polinom ireductibil în inelul $\mathbb{Z}[X]$. Fiind un polinom monic şi ireductibil în inelul $\mathbb{Z}[X]$, polinomul $\Phi_n(X)$ rămâne ireductibil şi în inelul $\mathbb{Q}[X]$.

Aplicaţii. 1° Vom descrie acum endomorfismele corpului ciclotomic $\mathbb{Q}(\zeta)$. Deoarece polinomul $\Phi_n(X)$ este ireductibil în inelul $\mathbb{Q}[X]$, rezultă că orice polinom $f(X) \in \mathbb{Q}[X]$, cu $f(\zeta)=0$, se divide cu $\Phi_n(X)$ (întrucât în $\mathbb{Q}[X]$ c. m. m. d. c. al polinoamelor $f(X)$ şi $\Phi_n(X)$ este un divizor de grad ≥ 1 al lui $\Phi_n(X)$, deci coincide cu $\Phi_n(X)$). De aici rezultă că $\Phi_n(X)$ este *polinomul minimal al lui ζ peste* $\mathbb{Q}$ (adică polinomul monic de grad minim din $\mathbb{Q}[X]$ pe care îl verifică ζ) şi există egalităţile de mulţimi:

$$\mathbb{Q}(\zeta)=\{h(\zeta) \mid h \in \mathbb{Q}[X]\}=\{h(\zeta) \mid h \in \mathbb{Q}[X],\ \mathrm{grad}(h)<\varphi(n)\}$$

(v. [9], exerciţiul rezolvat 6, pag. 124).

Fie σ un endomorfism al corpului $\mathbb{Q}(\zeta)$. Din $\sigma(1)=1$, rezultă $\sigma(q)=q$, pentru orice $q \in \mathbb{Q}$. Aşadar, endomorfismul σ este determinat dacă se cunoaşte valoarea $\sigma(\zeta)$.

Dacă $x \in U_n$, din $x^n=1$, rezultă $\sigma(x^n)=1$ sau $\sigma(x)^n=1$, deci $\sigma(x) \in U_n$. Dar σ este injectiv (morfismele de corpuri sunt injective), prin urmare:

$$U_n=\sigma(U_n)=\left\{\sigma(1)=1, \sigma(\zeta), \sigma(\zeta^2)=\sigma(\zeta)^2, \ldots, \sigma(\zeta^{n-1})=\sigma(\zeta)^{n-1}\right\}.$$

Înseamnă că $\sigma(\zeta)$ este un generator al grupului U_n, deci:

$$\sigma(\zeta)=\zeta^k,\ \text{pentru un anumit } 0 \leq k \leq n-1,\ (k,n)=1.$$

Reciproc, pentru fiecare $0 \leq k \leq n-1$, $(k,n)=1$, aplicaţia $\sigma: \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$, definită prin $\sigma(h(\zeta))=h\left(\zeta^k\right)$, pentru orice $h \in \mathbb{Q}[X]$, este un endomorfism[1)] al corpului $\mathbb{Q}(\zeta)$, având proprietatea $\sigma(\zeta)=\zeta^k$. Aşadar, numărul endomorfismelor corpului $\mathbb{Q}(\zeta)$ este $\varphi(n)$.

Remarca 1. Dacă pentru $0 \leq k \leq n-1$, $(k,n)=1$, notăm cu σ_k endomorfismul $\mathbb{Q}(\zeta)$ pentru care $\sigma(\zeta)=\zeta^k$ şi luăm acel $0 \leq k' \leq n-1$, $(k',n)=1$, cu proprietatea $kk' \equiv 1 \pmod n$, rezultă că $\sigma_k \circ \sigma_{k'}=1_{\mathbb{Q}(\zeta)}$, ceea ce arată că endomorfismul σ_k este chiar un automorfism al corpului $\mathbb{Q}(\zeta)$.

Grupul automorfismelor corpului $\mathbb{Q}(\zeta)$ (în raport cu compunerea), notat $\mathrm{Aut}\mathbb{Q}(\zeta)$ este izomorf cu grupul $U(\mathbb{Z}_n)$ al unităţilor inelului $\mathbb{Z}_n$, prin

---

[1)] Aplicaţia σ este bine definită căci, dacă $h_1, h_2 \in \mathbb{Q}[X]$ sunt astfel încât $h_1(\zeta)=h_2(\zeta)$, atunci $(h_1-h_2)(\zeta)=0$, deci h_1-h_2 se divide cu $\Phi_n(X)$. Dar ζ^k este rădăcină a lui $\Phi_n(X)$, deci $(h_1-h_2)\left(\zeta^k\right)=0$, adică $h_1(\zeta^k)=h_2\left(\zeta^k\right)$. Aplicaţia σ este endomorfism al corpului $\mathbb{Q}(\zeta)$, căci pentru $h_1, h_2 \in \mathbb{Q}[X]$, arbitrare, avem: $\sigma(h_1(\zeta)+h_2(\zeta))=\sigma((h_1+h_2)(\zeta))=$ $=(h_1+h_2)\left(\zeta^k\right)=h_1\left(\zeta^k\right)+h_2\left(\zeta^k\right)=\sigma(h_1(\zeta))+\sigma(h_2(\zeta))$ şi analog $\sigma(h_1(\zeta)h_2(\zeta))=$ $=\sigma(h_1(\zeta))\,\sigma(h_2(\zeta))$.

izomorfismul:

$$F : (\mathrm{Aut}\mathbb{Q}(\zeta), \circ) \to (U(\mathbb{Z}_n), \cdot)\,,\ F(\sigma_k) = \widehat{k}$$

(v. [8], teorema 10, pag. 63).

Remarca 2. Putem regăsi lema lui *Mertens* în felul următor: egalitatea $f(\zeta) = 0$ din ipoteza lemei, are loc în corpul ciclotomic $\mathbb{Q}(\zeta)$ şi atunci îi putem aplica endomorfismul σ_k al corpului $\mathbb{Q}(\zeta)$, obţinând $f(\zeta^k) = 0$. Mai mult, rezultatul lemei se menţine în cazul mai general când f este un polinom nenul din $\mathbb{Q}[X]$, cu proprietatea $f(\zeta) = 0$.

2° Ne propunem să determinăm numerele naturale $n \geq 5$ şi $d \geq 2$, d liber de pătrate, pentru care există numerele raţionale a şi b, $b \neq 0$, astfel încât:

$$\cos\frac{2\pi}{n} = a + b\sqrt{d}.$$

Cerinţa se scrie echivalent $\frac{1}{2}\left(\zeta + \frac{1}{\zeta}\right) = a + b\sqrt{d}$, sau , după câteva calcule:

$$\zeta^4 + A\zeta^3 + B\zeta^2 + A\zeta + 1 = 0,$$

unde $A, B \in \mathbb{Q}$. Egalitatea precedentă arată că ζ verifică un polinom cu coeficienţi raţionali de gradul 4. Dar polinomul minimal al lui ζ peste $\mathbb{Q}$ este $\Phi_n(X)$, care are gradul $\varphi(n)$. Rezultă $\varphi(n) \leq 4$. Dar $\varphi(n)$ este par şi, în cazul nostru, $\varphi(n) \neq 2$ (căci $\varphi(n) = 2$ conduce la $n = 6$, deci $b = 0$, contrar ipotezei).

Aşadar $\varphi(n) = 4$ şi, ţinând seama de expresia lui $\varphi(n)$, obţinem $n \in \{5, 8, 10, 12\}$.

Pentru $n = 5$ avem $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$, deci $d = 5$.

Pentru $n = 8$ avem $\cos\frac{2\pi}{8} = \cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$, deci $d = 2$.

Pentru $n = 10$ avem $\cos\frac{2\pi}{10} = \cos\frac{\pi}{5} = \frac{1+\sqrt{5}}{4}$, deci $d = 5$.

Pentru $n = 12$ avem $\cos\frac{2\pi}{12} = \cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$, deci $d = 3$.

Comentariu istoric. Polinomul ciclotomic $\Phi_n(X)$ a fost studiat mai întâi de *Gauss* (1801,[2]) în cazul particular când $n = p =$ număr prim, apoi în cazul general de către *Dedekind* (1857, [1]).

Demonstraţia dată de *Mertens* (1905, 1908, [6]) pentru ireductibilitatea polinomului ciclotomic, bazată pe lema anterioară, pare a fi cea mai simplă. *Mertens* a dat însă altă demonstraţie acestei leme.

Demonstraţii ulterioare, mai simple, date lemei lui *Mertens* aparţin lui *Grandjot* (1924, [3]), *Landau* (1929, [4], prezentată în acest articol), *Schur* (1929, [7]), *Levi* (1934, [5]).

Bibliografie

[1] R. Dedekind, *Beweis für die Irreduktibilität der Kreisteilungsgleichungen*, J. f. Math. 54, 1857, S. 27-30.
[2] C. F. Gauss, *Disquisitiones arithmeticae*, Leipzig, 1801 (trad. rom. Cercetări aritmetice, Ed. Amarcord, Timişoara, 1999).
[3] K. Grandjot, *Über die Irreduzibilität der Kreisteilungsgleichung*, Math. Zeitsch., 19, 1924, S. 128-129.
[4] E. Landau, *Über die Irreduzibilität der Kreisteilungsgleichung*, Math. Zeitsch., 29, 1929, S. 462.
[5] F. Levi, *Zur Irreduzibilität der Kreisteilungspolynome*, Compositio Math. 1, 1934, S. 303-304.
[6] F. J. Mertens, Wiener Berichte 114, 1905, S. 1293-1296; Wiener Berichte 117, 1908, S. 689-690.
[7] I. Schur,*Zur Irreduzibilität der Kreisteilungsgleichung*, Math. Zeitsch., 29, 1929, S. 463.
[8] M. Ţena, *Rădăcinile unităţii*, Soc. Şt. Mat. Rom., 2005.
[9] M. Ţena, M. Andronache, D. Şerbănescu, *Matematică M1, manual cl. a XII-a*, Ed. Art, Bucureşti, 2007.

EXAMENE ŞI CONCURSURI

CONCURSUL DE MATEMATICĂ „ CRISTIAN S. CALUDE“

Ediţia a IX-a, Galaţi, 25 octombrie şi 1-2 noiembrie 2008

prezentare de Ion Mirică[1] şi Romeo Zamfir [2]

Catedra de matematică a Colegiului Naţional „Vasile Alecsandri“ organizează în colaborare cu Inspectoratul Şcolar al Judeţului Galaţi şi Societatea de Ştiinţe Matematice din România, filiala Galaţi, în fiecare an, în luna octombrie şi/sau noiembrie, Concursul Interjudeţean de Matematică „Cristian S. Calude“. Concursul este destinat elitelor matematicii româneşti şi se constituie într-o modalitate de stimulare a pregătirii elevilor pentru marea performanţă naţională şi internaţională.

În anul şcolar 2008-2009, pe 25 octombrie, 1 şi 2 noiembrie 2008, s-a desfăşurat a IX-a ediţie a acestui concurs aflat sub patronajul domnului profesor *Cristian S. Calude*, fost elev al Colegiului Naţional „Vasile Alecsandri“

1) Universitatea „Dunărea de Jos“ din Galaţi, str. Domnească, nr. 47, cod 800008 e-mail: imirică@ugal.ro

2) C. N. „Vasile Alecsandri“, Galaţi, str. Nicolae Bălcescu, nr. 41, cod 800001, e-mail: romeozamfir@gmail.com