degree of algebraic number*

pahio†

2013-03-22 3:20:55

Theorem. The degree of any algebraic number α in the number field $\mathbb{Q}(\vartheta)$ divides the degree of ϑ. The zeroes of the characteristic polynomial $g(x)$ of α consist of the algebraic conjugates of α, each of which having equal multiplicity as zero of $g(x)$.

Proof. Let the minimal polynomial of α be

$$a(x) := x^k + a_1 x^{k-1} + \ldots + a_k$$

and all zeroes of this be $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_k$. Denote the canonical polynomial of α with respect to the primitive element ϑ by $r(x)$; then

$$a(r(\vartheta)) = a(\alpha) = 0.$$

If $a(r(x)) := \varphi(x)$, then the equation

$$\varphi(x) = 0$$

has rational coefficients and is satisfied by ϑ. Since the minimal polynomial $f(x)$ of ϑ is irreducible, it must divide $\varphi(x)$ and all algebraic conjugates $\vartheta_1 = \vartheta, \vartheta_2, \ldots, \vartheta_n$ of ϑ make $\varphi(x)$ zero. Hence we have

$$a(\alpha^{(i)}) = a(r(\vartheta_i)) = 0 \quad \text{for} \quad i = 1, 2, \ldots, n$$

where the numbers $\alpha^{(i)}$ are the $\mathbb{Q}(\vartheta)$-conjugates of α. Thus these $\mathbb{Q}(\vartheta)$-conjugates are roots of the irreducible equation $a(x) = 0$, whence $a(x)$ must divide the characteristic polynomial $g(x)$. Let the power $[a(x)]^m$ exactly divide $g(x)$, when

$$g(x) = [a(x)]^m b(x), \quad a(x) \nmid b(x).$$

Antithesis: $\deg(b(x)) \geqq 1$ and $b(\beta) = 0$.
This implies that $g(\beta) = 0$, i.e. β is one of the numbers $\alpha^{(i)}$. Therefore, β

*⟨*DegreeOfAlgebraicNumber*⟩* created: ⟨*2013-03-2*⟩ by: ⟨*pahio*⟩ version: ⟨*42050*⟩ Privacy setting: ⟨*1*⟩ ⟨*Theorem*⟩ ⟨*11R04*⟩ ⟨*11C08*⟩ ⟨*12F05*⟩ ⟨*12E05*⟩

were a zero of $a(x)$ and thus $a(x) \mid b(x)$, which is impossible. Consequently,the antithesis is wrong, i.e. $b(x)$ is a constant, which must be 1 because $g(x)$ and $a(x)$ are monic polynomials. So, $g(x) = [a(x)]^m$. Since

$$a(x) \;=\; (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k),$$

it follows that

$$g(x) \;=\; (x-\alpha_1)^m(x-\alpha_2)^m\cdots(x-\alpha_k)^m.$$

Hence $km \;=\; n$ and k divides n, as asserted. Moreover, each α_j is a zero of order m of $g(x)$, i.e. appears among the roots $\alpha^{(1)}$, $\alpha^{(2)}$, $\ldots$, $\alpha^{(n)}$ of the equation $g(x) = 0$ m times.