Pub. Mat. UAB
N°20 Set. 1980
Actes VII JMHL

A PRIMITIVITY CRITERION

Enric Nart, Núria Vila

Secció de Matemàtiques
Universitat Autònoma de Barcelona

Abstract. *In this note we give a generalization of Furtwängler's primitivity criterion* [2], *in order to assure that a polynomial is primitive through his coefficients.*

Let K be a field. We recall that a polynomial $f(X)\in K[X]$ is called primitive over K if its Galois group over K is primitive as a permutation group of its roots [3,ch.VI,49].

Throughout this note R will denote a Dedekind domain and K its field of quotients. If $\mathfrak{p}$ is a prime ideal of R, we denote by $v_{\mathfrak{p}}$ the valuation of R associated to $\mathfrak{p}$.

Furtwängler proved the following criterion [2,th.3]: If $f(X)=X^n+a_1X^{n-1}+\ldots+a_n \in\mathbb{Z}[X]$ is an irreducible polynomial and for a prime p is $v_p(a_i)>0$, $1\leq i\leq n$, $v_p(a_{n-1})=1$ and $v_p(a_n)>1$, then f(X) is primitive.

In this note we prove the following generalization:

<u>Theorem</u>. Let $f(X)=X^n+a_1X^{n-1}+\ldots+a_n \in R[X]$ be an irreducible polynomial. Let $\mathfrak{p}$ be a prime ideal of R such that $e_i=v_{\mathfrak{p}}(a_i)\geq 1$ for every $1\leq i\leq n$. Let $0<k<n$ be such that $e_i/i \geq e_k/k$ for every $1\leq i\leq n$. Suppose that n=rs, and the roots of f(X) can be divided in s subsets of imprimitivity. If in every s-tuple $(i_1,\ldots,i_s)$ of indexs with $0\leq i_m\leq r$, $1\leq m\leq s$, and $i_1+\ldots+i_s=k$, there exists an index i_q such that $(i_q,k)=1$, then $s \geq k/(k,e_k)$.

First we need an easy lemma:

<u>Lemma</u>. Let $f(X)=X^n+a_1X^{n-1}+\ldots+a_n \in R[X]$. Let α be a root of $f(X)$. Let $\mathfrak{q}$ be a prime ideal of K and $\mathfrak{p}$ a prime ideal of $K(\alpha)$ lying over $\mathfrak{q}$. Let $\lambda\in\mathbb{Q}$ and $e=e(\mathfrak{p}/\mathfrak{q})$.

i) If $v_{\mathfrak{q}}(a_i)\geqslant i\lambda$ for every $1\leqslant i\leqslant n$, then $v_{\mathfrak{p}}(\alpha)\geqslant e\lambda$

ii) If $v_{\mathfrak{q}}(a_i)> i\lambda$ for every $1\leqslant i\leqslant n$, then $v_{\mathfrak{p}}(\alpha)> e\lambda$

<u>Proof</u>. The slope of any segment of the Newton's polygon associated to $f(X)$ is $\geqslant \lambda$, by [1 ,ch.2,5] is $v_{\mathfrak{p}}(\alpha)/e\geqslant\lambda$.

<u>Proof of the theorem</u>. Let L be a splitting field of $f(X)$ over K. Let $\mathfrak{p}$ be a prime ideal of L lying over $\mathfrak{q}$, and $e=e(\mathfrak{p},\mathfrak{q})$. Let

$$\alpha_1^1,\ldots,\alpha_r^1;\alpha_1^2,\ldots,\alpha_r^2;\ldots;\alpha_1^s,\ldots,\alpha_r^s,$$

be a division of the roots of $f(X)$ in subsets of imprimitivity. Let

$$f_i(X) = \prod_{j=1}^{r} (X-\alpha_j^i) = X^r+\xi_1^iX^{r-1}+\ldots+\xi_r^i,\ 1\leqslant i\leqslant s.$$

Clearly the elements $\xi_j^1,\ldots,\xi_j^s$ are conjugated over K for every $1\leqslant j\leqslant r$. Let

$$g_j(X) = X^s+b_1^jX^{s-1}+\ldots+b_s^j,\ 1\leqslant j\leqslant r,$$

be their irreducible polynomial over K. Being the roots of $f(X)$ integers over K, the same happens with the ξ_i^j's, hence $g_j(X)\in R[X]$ for every $1\leqslant j\leqslant r$. If α is a root of $f(X)$, it follows from the lemma that $v_{\mathfrak{p}}(\alpha)\geqslant ee_k/k$, hence

$$v_{\mathfrak{p}}(\xi_j^i) \geqslant jee_k/k. \qquad (1)$$

Thus, $v_{\mathfrak{p}}(b_i^j) \geqslant ijee_k/k$, hence

$$v_{\mathfrak{q}}(b_i^j) \geqslant ije_k/k. \qquad (2)$$

Clearly $f(X) = \prod_{i=1}^{s} f_i(X)$, hence

$$a_k = \sum_{\substack{0\leqslant i_m\leqslant r,\ 1\leqslant m\leqslant s\\ i_1+\ldots+i_s=k}} \xi_{i_1}^1\ldots\xi_{i_s}^s,\ \text{where } \xi_0^i=1 \text{ for every } 1\leqslant i\leqslant s.$$

By (1) every summand has

$$v_{\mathfrak{p}}(\xi_{i_1}^{1}\cdots\xi_{i_s}^{s}) \geqslant ee_k. \qquad (3)$$

Since $v_{\mathfrak{p}}(a_k)=ee_k$, there exists one s-tuple $(i_1,\ldots,i_s)$ for which equality holds in (3). Hence, for this s-tuple we have

$$v_{\mathfrak{p}}(\xi_{i_m}^{m}) = i_m ee_k/k, \text{ for every } 1\leqslant m\leqslant s.$$

Let i_q be the index in this s-tuple such that $(i_q,k)=1$. By (2) and ii) of the lemma, there exists an index t, $1\leqslant t\leqslant s$, such that

$$v_{\mathfrak{P}}(b_t^{i_q}) = ti_q e_k/k.$$

Since $v_{\mathfrak{P}}(b_t^{i_q})$ is an integer and $(i_q,k)=1$ we conclude that te_k/k is an integer, hence t is a multiple of $k/(k,e_k)$. Thus $s\geqslant t\geqslant k/(k,e_k)$.

<u>Corollary</u>. In the following cases f(X) is primitive:

i) If $k=n-1$ and $(n-1,e_{n-1})=1$.

ii) If $n>3$, $k=n-1$ and $e_{n-1}=1$ or 2.

iii) If n is odd, $k=n-2$ and $(n-2,e_{n-2})=1$.

iv) If $n>6$, $3\nmid n$, $k=n-3$ and $(n-3,e_{n-3})=1$.

v) If p is a prime number $n/2<p<n$ and $k=p$.

<u>Proof</u>. All are an easy consequence of the theorem. Let us remark that there always exists a prime number satisfying the condition of v) by a theorem of Tchebyscheff.

<u>Remark</u>. Furtwängler's primitivity criterion is the special case $e_{n-1}=1$ in i) of the corollary.

<u>References</u>.

1. E.Artin, Algebraic numbers and algebraic functions, Gordon and Breach, N.York,1967.

2. Ph. Furtwängler, Über Kriterien für irreduzible und für primitive Gleichungen und über die Aufstellung affektfreier Gleichungen, Math. Ann. 85 (1922) 34-40.

3. B.L. Van der Waerden, Modern Algebra, Vol.I, Ungar, N.York,1953.