COLLOQUIUM MATHEMATICUM

VOL. LXVIII 1995 FASC. 2

CRITERION FOR A FIELD TO BE ABELIAN

BY

J. WÓJCIK

The following theorem of Kummer is known (see [1], p. 11):

Let $\alpha \in P_p^*$, p a prime, $P_p = \mathbb{Q}(\zeta_p)$, $\zeta_p = e^{2\pi i/p}$. Assume that α is of order p with respect to $(P_p^*)^p$. Let $\sigma = (\zeta_p \to \zeta_p^\varrho)$, where ϱ is a primitive root mod p. The extension $P_p(\sqrt[p]{\alpha})/\mathbb{Q}$ is abelian if and only if the number $\alpha^{\sigma-\varrho}$ is a pth power in P_p.

H. Hasse gives in [1], p. 11, a more general result:

Let F, M be algebraic number fields such that $F \subseteq M$ and the extension M/F is cyclic. Assume that $\zeta_n \in M$. Let σ denote a generator of $G(M/F)$, $\zeta_n^\sigma = \zeta_n^\varrho$. Let $\alpha \in M$. Assume that α is of order n with respect to M^n. Put $L = M(\sqrt[n]{\alpha})$. The extension L/F is abelian if and only if the number $\alpha^{\sigma-\varrho}$ is an nth power in M.

The aim of this paper is to prove a similar theorem which contains the above result. Namely, we have the following:

THEOREM. *Let F be a field and n a positive integer not divisible by the characteristic of F. Let M/F be an abelian extension of finite degree and $L = M(\sqrt[n]{\alpha})$ for some $\alpha \in M^*$. Further, let $\sigma_1, \ldots, \sigma_i$ be a basis of $G(M(\zeta_n)/F)$ with $\zeta_n^{\sigma_j} = \zeta_n^{a_j}$, $a_j \in \mathbb{Z}$. The extension L/F is abelian if and only if there exist $A_1, \ldots, A_r \in M^*$ such that*

(1) $$\alpha^{\sigma_j - a_j} = A_j^n \quad (1 \le j \le r),$$

(2) $$A_j^{\sigma_i - a_i} = A_i^{\sigma_j - a_j} \quad (1 \le i, j \le r).$$

COROLLARY 1. *Let F be a field and n a positive integer not divisible by the characteristic of F. Let the extension $M(\zeta_n)/F$ be cyclic and $L = M(\sqrt[n]{\alpha})$ for some $\alpha \in M^*$. Further, let σ be a generator of $G(M(\zeta_n)/F)$ with $\zeta_n^\sigma = \zeta_n^a$, $a \in \mathbb{Z}$. The extension L/F is abelian if and only if the number $\alpha^{\sigma-a}$ is an nth power in M.*

Remark 1. Corollary 1 contains Hasse's result quoted above.

1991 *Mathematics Subject Classification*: Primary 11R20.

COROLLARY 2 (A. Schinzel [3]). *Let F be a field and n a positive integer not divisible by the characteristic of F. A binomial $x^n - \alpha$ has an abelian Galois group over F if and only if $\alpha^{w_n} = \gamma^n$, where $\gamma \in F$ and w_n is the number of nth roots of unity contained in F.*

Proof of Theorem. Let $\alpha = \beta^n$, $L = M(\beta)$ and $\overline{L} = L(\zeta_n)$.

Necessity. Assume that the extension L/F is abelian. Then $\overline{L}/F$ and $\overline{L}/M$ are also abelian. Put $G = G(\overline{L}/F)$ and $H = G(\overline{L}/M)$. Let $\overline{\sigma}_j \in G$ with $\overline{\sigma}_j = \sigma_j$ on $M(\zeta_n)$, and $\tau \in H$. We have $\beta^\tau = \zeta_n^k \beta$, $\beta^{\overline{\sigma}_j \tau} = \beta^{\tau \overline{\sigma}_j} = \zeta_n^{a_j k} \beta^{\overline{\sigma}_j}$ and

$$\beta^{(\overline{\sigma}_j - a_j)\tau} = \beta^{\overline{\sigma}_j - a_j} =: A_j \in M^*. \tag{3}$$

Hence $\alpha^{\sigma_j - a_j} = A_j^n$. Thus (1) holds.

By (3), $A_j^{\sigma_i - a_i} = A_j^{\overline{\sigma}_i - a_i} = \beta^{(\overline{\sigma}_j - a_j)(\overline{\sigma}_i - a_i)} = \beta^{(\overline{\sigma}_i - a_i)(\overline{\sigma}_j - a_j)} = A_i^{\sigma_j - a_j}$. Thus (2) holds.

Sufficiency. Assume that conditions (1) and (2) hold. We shall prove that the extension L/F is abelian. It is enough to prove that $\overline{L}/F$ is abelian. We have $F \subseteq M \subseteq L \subseteq \overline{L}$. Since M/F, L/M and $\overline{L}/L$ are separable, so is $\overline{L}/F$.

Let $\overline{\sigma}$ be an arbitrary isomorphism of $\overline{L}$ over F with $\overline{\sigma} = \sigma$ on $M(\zeta_n)$, $\sigma \in G(M(\zeta_n)/F)$. We have

$$M = F(\gamma) \tag{4}$$

and

$$\overline{L} = F(\beta, \gamma, \zeta_n). \tag{5}$$

Since the extension M/F is normal,

$$\gamma^{\overline{\sigma}} \in M \subseteq \overline{L}. \tag{6}$$

Obviously

$$\zeta_n^{\overline{\sigma}} \in \overline{L}. \tag{7}$$

We have

$$\sigma = \sigma_1^{t_1} \ldots \sigma_r^{t_r}, \qquad t_j \in \mathbb{Z},\ 0 \le t_j < h_j,\ h_j = \operatorname{ord} \sigma_j. \tag{8}$$

Put

$$A_\sigma := \prod_{j=1}^r A_j^{a_1^{t_1} \ldots a_{j-1}^{t_{j-1}} \sigma_{j+1}^{t_{j+1}} \ldots \sigma_r^{t_r} \frac{\sigma_j^{t_j} - a_j^{t_j}}{\sigma_j - a_j}}. \tag{9}$$

Obviously $A_\sigma \in M^*$. We now show that

$$\alpha^{\sigma - a} = A_\sigma^n, \qquad \text{where} \quad a = a_1^{t_1} \ldots a_r^{t_r}. \tag{10}$$

We have

$$a_1^{t_1}\dots a_{j-1}^{t_{j-1}}\sigma_{j+1}^{t_{j+1}}\dots\sigma_r^{t_r}(\sigma_j^{t_j}-a_j^{t_j})+a_1^{t_1}\dots a_j^{t_j}\sigma_{j+2}^{t_{j+2}}\dots\sigma_r^{t_r}(\sigma_{j+1}^{t_{j+1}}-a_{j+1}^{t_{j+1}})$$
$$=a_1^{t_1}\dots a_{j-1}^{t_{j-1}}\sigma_j^{t_j}\dots\sigma_r^{t_r}-a_1^{t_1}a_{j+1}^{t_{j+1}}\sigma_{j+2}^{t_{j+2}}\dots\sigma_r^{t_r}\qquad\text{for } 1\le j\le r-1.$$

Hence

$$\sigma-a=\sum_{j=1}^{r}a_1^{t_1}\dots a_{j-1}^{t_{j-1}}\sigma_{j+1}^{t_{j+1}}\dots\sigma_r^{t_r}(\sigma_j^{t_j}-a_j^{t_j}).\tag{11}$$

By (11), (1) and (9),

$$\alpha^{\sigma-a}=\prod_{j=1}^{r}\alpha^{(\sigma_j-a_j)a_1^{t_1}\dots a_{j-1}^{t_{j-1}}\sigma_{j+1}^{t_{j+1}}\dots\sigma_r^{t_r}\frac{\sigma_j^{t_j}-a_j^{t_j}}{\sigma_j-a_j}}$$
$$=\Big(\prod_{j=1}^{r}A_j^{a_1^{t_1}\dots a_{j-1}^{t_{j-1}}\sigma_{j+1}^{t_{j+1}}\dots\sigma_r^{t_r}\frac{\sigma_j^{t_j}-a_j^{t_j}}{\sigma_j-a_j}}\Big)^n=A_\sigma^n.$$

Thus (10) holds.

By (10), $\beta^{\overline{\sigma}n}=\alpha^{\overline{\sigma}}=\alpha^{\sigma}=\alpha^aA_\sigma^n=(\beta^aA_\sigma)^n$. Hence

$$\beta^{\overline{\sigma}}=\zeta_n^u\beta^aA_\sigma\in\overline{L}.\tag{12}$$

Since the extension $\overline{L}/F$ is separable and, by (5)–(7) and (12), normal, it is a Galois extension and $\overline{\sigma}$ is an automorphism.

Let $\overline{\tau}$ be any automorphism of $\overline{L}$ over F with $\overline{\tau}=\tau$ on $M(\zeta_n)$, $\tau\in G(M(\zeta_n)/F)$. Since the extension M/F is abelian we have, by (4),

$$\gamma^{\overline{\sigma}\,\overline{\tau}}=\gamma^{\overline{\tau}\,\overline{\sigma}}.\tag{13}$$

Obviously

$$\zeta_n^{\overline{\sigma}\,\overline{\tau}}=\zeta_n^{\overline{\tau}\,\overline{\sigma}}.\tag{14}$$

We have

$$\tau=\sigma_1^{u_1}\dots\sigma_r^{u_r},\qquad u_i\in\mathbb{Z},\ 0\le u_i<h_i,\ h_i=\operatorname{ord}\sigma_i.\tag{15}$$

We now show that

$$A_\sigma^{\tau-b}=A_\tau^{\sigma-a},\quad\text{where}\quad b=a_1^{u_1}\dots a_r^{u_r}.\tag{16}$$

By (15) and (11),

$$\tau-b=\sum_{i=1}^{r}a_1^{u_1}\dots a_{i-1}^{u_{i-1}}\sigma_{i+1}^{u_{i+1}}\dots\sigma_r^{u_r}(\sigma_i^{u_i}-a_i^{u_i}).\tag{17}$$

By (15) and (9),

$$A_\tau=\prod_{i=1}^{r}A_i^{a_1^{u_1}\dots a_{i-1}^{u_{i-1}}\sigma_{i+1}^{u_{i+1}}\dots\sigma_r^{u_r}\frac{\sigma_i^{u_i}-a_i^{u_i}}{\sigma_i-a_i}}.\tag{18}$$

By (2), (9), (17), (18) and (11),

$$\begin{aligned}
A_\sigma^{\tau-b} &= \prod_{j=1}^{r}\prod_{i=1}^{r} A_j^{(\sigma_i-a_i)a_1^{t_1}\ldots a_{j-1}^{t_{j-1}}\sigma_{j+1}^{t_{j+1}}\ldots\sigma_r^{t_r}\frac{\sigma_j^{t_j}-a_j^{t_j}}{\sigma_j-a_j}a_1^{u_1}\ldots a_{i-1}^{u_{i-1}}\sigma_{i+1}^{u_{i+1}}\ldots\sigma_r^{u_r}\frac{\sigma_i^{u_i}-a_i^{u_i}}{\sigma_i-a_i}} \\
&= \prod_{i=1}^{r}\prod_{j=1}^{r} A_i^{(\sigma_j-a_j)a_1^{u_1}\ldots a_{i-1}^{u_{i-1}}\sigma_{i+1}^{u_{i+1}}\ldots\sigma_r^{u_r}\frac{\sigma_i^{u_i}-a_i^{u_i}}{\sigma_i-a_i}a_1^{t_1}\ldots a_{j-1}^{t_{j-1}}\sigma_{j+1}^{t_{j+1}}\ldots\sigma_r^{t_r}\frac{\sigma_j^{t_j}-a_j^{t_j}}{\sigma_j-a_j}} \\
&= A_\tau^{\sigma-a}.
\end{aligned}$$

Thus (16) holds.

By (12),

$$\beta^{\overline{\tau}} = \zeta_n^v \beta^b A_\tau. \tag{19}$$

By (8),

$$\zeta_n^{\overline{\sigma}} = \zeta_n^{\sigma} = \zeta_n^{a_1^{t_1}\ldots a_1^{t_r}} = \zeta_n^a. \tag{20}$$

Similarly,

$$\zeta_n^{\overline{\tau}} = \zeta_n^b. \tag{21}$$

By (12) and (19)–(21),

$$\beta^{\overline{\sigma}\,\overline{\tau}} = \zeta_n^{ub+va}\beta^{ab}A_\tau^a A_\sigma^r, \tag{22}$$

$$\beta^{\overline{\tau}\,\overline{\sigma}} = \zeta_n^{ub+va}\beta^{ab}A_\sigma^b A_\tau^\sigma. \tag{23}$$

By (16), $A_\tau^a A_\sigma^\tau = A_\sigma^b A_\tau^\sigma$. By (22) and (23),

$$\beta^{\overline{\sigma}\,\overline{\tau}} = \beta^{\overline{\tau}\,\overline{\sigma}}. \tag{24}$$

By (5), (24), (13) and (14) the extension $\overline{L}/F$ is abelian. ∎

P r o o f o f C o r o l l a r y 2. We put $M = F$ in the Theorem. It is enough to prove that $\alpha^{1-a_j} = A_j^n$ and $A_j^{1-a_i} = A_i^{1-a_j}$ $(A_i, A_j \in F) \Leftrightarrow \alpha^{w_n} = \gamma^n$ $(\gamma \in F)$.

By Galois theory $w_n = (1-a_1, \ldots, 1-a_r, n)$. Hence $\alpha^{1-a_j} = A_j^n \Leftrightarrow \alpha^{w_n} = \gamma^n$. It is enough to prove that $\alpha^{1-a_j} = A_j^n \Rightarrow A_j^{1-a_i} = A_i^{1-a_j}$. Assume that $\alpha^{1-a_j} = A_j^n$. Then

$$\alpha^{1-a_j} = \alpha^{w_n(1-a_j)/w_n} = \gamma^{n(1-a_j)/w_n} = A_j^n.$$

Hence $A_j = \zeta_{w_n}^{x_j}\gamma^{(1-a_j)/w_n}$ and

$$A_j^{1-a_i} = \gamma^{(1-a_j)(1-a_i)/w_n} = A_i^{1-a_j}. \ ∎$$

R e m a r k 2. In special cases conditions (1) and (2) in the Theorem can be replaced just by (1). We have such a situation in Corollaries 1 and 2. In general we cannot drop (2). This is shown by the following example:

$F = \mathbb{Q}$, $M = P_4$, $n = 8$, $\alpha = -4$, $L = P_4(\sqrt[8]{-4})$. Put $\sigma_1 = (\zeta_8 \to \zeta_8^{-1})$, $\sigma_2 = (\zeta_8 \to \zeta_8^5)$, $a_1 = -1$, $a_2 = 5$. Then (1) is satisfied:

$$\alpha^{\sigma_1 - a_1} = (-4)^2 = A_1^8, \quad \alpha^{\sigma_2 - a_2} = (-4)^{-4} = A_2^8,$$

where $A_1 = \zeta_4^i(1-\zeta_4)$, $A_2 = \zeta_4^j(1+\zeta_4)^{-2}$, $A_1, A_2 \in P_4$, i, j are arbitrary rational integers. However, the extension L/F is not abelian. Otherwise by Corollary 2 we would have $\alpha^2 = 16 = \gamma^8$ with $\gamma \in \mathbb{Q}$, which is impossible. The condition (2) is not satisfied. Indeed, $A_1^{\sigma_2 - a_2} = -1/4$, $A_2^{\sigma_1 - a_1} = 1/4$.

Remark 3. In the case $F = \mathbb{Q}$, $M = P_m$, where $P_m = \mathbb{Q}(\zeta_m)$ and $m(n-1)$ is even, there is a simple criterion for abelianity. Namely, the extension L/F is abelian if and only if α is of the form

$$\alpha = \zeta\tau(\chi)^n\gamma^n,$$

where $\zeta, \gamma \in P_m$, ζ is a root of unity, χ is some proper character with conductor f and of order k such that $(m, f) = 1$ or 2, $k \mid (n, m)$ and $\tau(\chi)$ is the normalized proper Gaussian sum corresponding to χ, with $\tau(\chi)^n \in P_m$. This follows from Kronecker–Weber's theorem and from the Theorem in [4].

Remark 4. Below we give a new proof of Corollary 2 connected with the proof of the Theorem (in fact, with the proof of necessity). This proof is much shorter than other known proofs of Corollary 2 (see [3], [5] and [2], p. 435).

Proof. *Sufficiency*. Assume that $\alpha^{w_n} = \gamma^n$, $\gamma \in F$. Put $\alpha = \beta^n$, $\gamma = \beta_1^{w_n}$. We have $\beta_1 \in F^{ab}$ ($\zeta_{w_n} \in F$) and $\beta = \zeta_{nw_n}^a \beta_1 \in F^{ab}$. Thus the extension $F(\beta, \zeta_n)/F$ is abelian.

Necessity. Assume that the Galois group of $x^n - \alpha$ is abelian. Put $\alpha = \beta^n$, $G = G(F(\beta, \zeta_n)/F)$, $H = G(F(\zeta_n)/F)$ and $\sigma_a = (\zeta_n \to \zeta_n^a)$. Let $\sigma, \tau \in G$ with $\sigma = \sigma_a$ on $F(\zeta_n)$. We have $\beta^\tau = \zeta_n^j\beta$, $\beta^{\sigma\tau} = \beta^{\tau\sigma} = \zeta_n^{aj}\beta^\sigma$ and $\beta^{(\sigma-a)\tau} = \beta^{\sigma-a} = A_a \in F$. Hence $\alpha^{1-a} = A_a^n$. By Galois theory $w_n = \text{g.c.d.}_{\sigma_a \in H}(\{1-a\}, n)$. Hence $\alpha^{w_n} = \gamma^n$, $\gamma \in F$. ∎

REFERENCES

[1] H. Hasse, *Invariante Kennzeichnung relativ-abelscher Zahlkörper mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers*, Abh. Deutsch. Akad. Wiss. 8 (1947), 5–56.

[2] G. Karpilowsky, *Topics in Field Theory*, North-Holland, Amsterdam, 1989.

[3] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. 32 (1977), 245–274.

[4] J. Wójcik, *Powers of cyclotomic numbers*, Comment. Math. 32 (1992), 213–223.

[5] W. Y. Yelez, *On normal binomials*, ibid. 36 (1980), 113–124.

Reçu par la Rédaction le 19.12.1993