characterization of abelian extensions of exponent n

Canonical name	CharacterizationOfAbelianExtensionsOfExponentN
Date of creation	2013-03-22 18:42:13
Last modified on	2013-03-22 18:42:13
Owner	rm50 (10146)
Last modified by	rm50 (10146)
Numerical id	4
Author	rm50 (10146)
Entry type	Theorem
Classification	msc 12F10

Theorem 1. *Let K be a field containing the n^{th} roots of unity, with characteristic not dividing n. Let L be a finite extension of K. Then the following are equivalent:*

1. *L/K is Galois with abelian Galois group of exponent dividing n*
2. *$L = K(\sqrt[n]{a_1},\ \ldots,\ \sqrt[n]{a_k})$ for some $a_i \in K$.*

Proof. Let $\zeta \in K$ be a primitive n^{th} root of unity.

$(2 \Rightarrow 1)$: Choose $\alpha_i \in L$ such that $\alpha_i^n = a_i \in K$. Then for each i, the elements $\alpha_i,\ \zeta\alpha_i,\ \ldots,\ \zeta^{n-1}\alpha_i$ are distinct and are all the roots of $x^n - a_i$ in L. Thus $x^n - a_i$ is separable over K and splits in L, so that L is the splitting field of the set of polynomials $\{x^n - a_i \mid 1 \leq i \leq k\}$. Thus L/K is Galois. Given $\sigma \in \mathrm{Gal}(L/K)$, for each i we have $\sigma(\alpha_i) = \zeta^j\alpha_i$ for some $1 \leq j \leq n$, so that $\sigma^k(\alpha_i) = \zeta^{kj}\alpha_i$. It follows that σ^n is the identity for every $\sigma \in \mathrm{Gal}(L/K)$, so that the exponent of $\mathrm{Gal}(L/K)$ divides n. It remains to show that $\mathrm{Gal}(L/K)$ is abelian; this follows trivially from the simple definition of the Galois action as multiplication by some n^{th} root of unity: if $\sigma, \tau \in \mathrm{Gal}(L/K)$ with $\sigma(\alpha_i) = \zeta^r\alpha_i, \quad \tau(\alpha_i) = \zeta^s\alpha_i$, then

$$(\sigma\tau)(\alpha_i) = \sigma(\zeta^s\alpha_i) = \zeta^s\zeta^r\alpha_i$$
$$(\tau\sigma)(\alpha_i) = \tau(\zeta^r\alpha_i) = \zeta^r\zeta^s\alpha_i$$

Thus $\sigma\tau = \tau\sigma$ on each α_i. But the α_i generate L/K, so $\sigma\tau = \tau\sigma$ on L and $\mathrm{Gal}(L/K)$ is abelian.

$(1 \Rightarrow 2)$: Let $G = \mathrm{Gal}(L/K)$, and write $G = C_1 \times \cdots \times C_r$ where each C_i is cyclic; $|C_i| = m_i \mid n$ for each i. For each i, define a subgroup $H_i \leq G$ by

$$H_i = C_1 \times \cdots \times C_{i-1} \times C_{i+1} \times \cdots \times C_r$$

Then $G/H_i \cong C_i$. Let L_i be the fixed field of H_i. L_i is normal over K since H_i is normal in G, and $\mathrm{Gal}(L_i/K) \cong G/H_i \cong C_i$ and thus L_i/K is cyclic Galois of order m_i. K contains the primitive m_i^{th} root of unity ζ^{n/m_i} and thus $L_i = K(\alpha_i)$ for some $\alpha_i \in L$ with $\alpha_i^{m_i} \in K$ (by Kummer theory). But then also $\alpha_i^n \in K$. Then

$$\mathrm{Gal}(L : K(\alpha_1, \ldots, \alpha_r)) = H_1 \cap \cdots \cap H_r = \{1\}$$

since any element of the left-hand group fixes each α_i and thus fixes L_i so is the identity in G/H_i. Thus $L = K(\alpha_1, \ldots, \alpha_r)$. $\square$

Corollary 2. *If L/K is the maximal abelian extension of K of exponent n, where n is prime to the characteristic of K, then $L = K(\{\sqrt[n]{a}\})$ for some set of $a \in K$.*

Proof. Clearly $K(\{\sqrt[n]{a} \mid a \in K^*)$ is an infinite abelian extension of exponent n. If L is the maximal such extension, choose $b \in L$. Then $K(b)$ is a finite extension of exponent dividing n and thus $K(b)$ is of the required form. Thus $L = \cup_{b \in L} K(b)$ is also of the required form; for example, if $S \subset K^*$ is a set of coset representatives for $K^*/(K^*)^n$, then $L = K(S)$. $\square$

References

[1] Morandi, P., *Field and Galois Theory*, Springer, 1996.