proof of Kummer theory

Canonical name	ProofOfKummerTheory
Date of creation	2013-03-22 18:42:07
Last modified on	2013-03-22 18:42:07
Owner	rm50 (10146)
Last modified by	rm50 (10146)
Numerical id	5
Author	rm50 (10146)
Entry type	Proof
Classification	msc 12F05

Proof. Let $\zeta \in K$ be a primitive n^{th} root of unity, and denote by $\boldsymbol{\mu}_n$ the subgroup of $K^\star$ generated by ζ.

(1) Let $L = K(\sqrt[n]{a})$; then L/K is Galois since K contains all n^{th} roots of unity and thus is a splitting field for $x^n - a$, which is separable since $n \neq 0$ in K. Thus the elements of $\mathrm{Gal}(L/K)$ permute the roots of $x^n - a$, which are

$$\sqrt[n]{a},\ \zeta\sqrt[n]{a},\ \zeta^2\sqrt[n]{a},\ \ldots,\ \zeta^{n-1}\sqrt[n]{a}$$

and thus for $\sigma \in \mathrm{Gal}(L/K)$, we have $\sigma(\sqrt[n]{a}) = \zeta_\sigma\sqrt[n]{a}$ for some $\zeta_\sigma \in \boldsymbol{\mu}_n$. Define a map

$$p : \mathrm{Gal}(L/K) \to \boldsymbol{\mu}_n : \sigma \mapsto \zeta_\sigma$$

We will show that p is an injective homomorphism, which proves the result.

Since $\boldsymbol{\mu}_n \subset K$, each n^{th} root of unity is fixed by $\mathrm{Gal}(L/K)$. Then for $\sigma, \tau \in \mathrm{Gal}(L/K)$,

$$\zeta_{\sigma\tau}\sqrt[n]{a} = \sigma\tau(\sqrt[n]{a}) = \sigma(\zeta_\tau\sqrt[n]{a}) = \zeta_\tau(\sigma(\sqrt[n]{a})) = \zeta_\sigma\zeta_\tau\sqrt[n]{a}$$

so that $\zeta_{\sigma\tau} = \zeta_\sigma\zeta_\tau$ and p is a homomorphism. The kernel of the map consists of all elements of $\mathrm{Gal}(L/K)$ which fix $\sqrt[n]{a}$, so that p is injective and we are done.

(2) Note that $\mathrm{N}_{L/K}(\zeta) = 1$ since ζ is a root of $x^n - 1$, so that by Hilbert's Theorem 90,

$$\zeta = \sigma(u)/u, \quad \text{for some } u \in L$$

But then $\sigma(u) = \zeta u$ so that $\sigma(u^n) = \sigma(u)^n = \zeta^n u^n = u^n$ and $a = u^n \in K$ since it is fixed by a generator of $\mathrm{Gal}(L/K)$. Then clearly $K(u)$ is a splitting field of $x^n - a$, and the elements of $\mathrm{Gal}(L/K)$ send u into distinct elements of $K(u)$. Thus $K(u)$ admits at least n automorphisms over K, so that $[K(u) : K] \geq n = [L : K]$. But $K(u) \subset L$, so $K(\sqrt[n]{a}) = K(u) = L$. □

References

[1] Dummit, D., Foote, R.M., *Abstract Algebra, Third Edition*, Wiley, 2004.

[2] Kaplansky, I., *Fields and Rings*, University of Chicago Press, 1969.