Algebraic Number Theory – Lecture 14

Michael Harvey

"Kummer Kummer Kummer Kummer Kummer-Kummeleon."

– Boy George

1. Kummer extensions

Class field theory is the outcome of attempts to generalise Gauss' reciprocity laws. Nowadays, it's almost synonymous with the study of abelian extensions of fields.

Definition. An extension L/K is called abelian, cyclic, etc. if it's a Galois extension and $\mathrm{Gal}(L/K)$ is an abelian, cyclic, etc. group.

Important note: Throughout this talk we'll assume that the ground field K contains nth roots of unity, i.e. $\mu_n \subset K$.

Definition. Let $\Delta \subseteq K^\times$, then a Kummer extension of K is of the form $K(\sqrt[n]{\Delta})$.

Definition. An abelian group of exponent n is an abelian group G such that $x^n = 1$ for every $x \in G$.

Definition. The compositum of two field extensions L/K and M/K is the smallest field extension N/K that contains L and M. It is denoted LM.

Proposition 1. *A Kummer extension $K(\sqrt[n]{\Delta})/K$ is Galois, and $\mathrm{Gal}(K(\sqrt[n]{\Delta})/K)$ is abelian of exponent n.*

Proof. Choose $a \in \Delta$. There is an injective homomorphism

$$\begin{aligned} \mathrm{Gal}(K(\sqrt[n]{\Delta})/K) &\hookrightarrow \mu_n \\ \sigma &\mapsto \frac{\sigma(\alpha)}{\alpha}, \quad \alpha^n = a. \end{aligned}$$

The choice of α is not important, suppose $\alpha = \zeta_n^r \beta$ with $\beta^n = a$ and $0 \leqslant r \leqslant n-1$. Then

$$\begin{aligned} \sigma(\alpha) &= \sigma(\zeta_n^r \beta) \\ &= \sigma(\zeta_n^r)\sigma(\beta) \\ &= \zeta_n^r \sigma(\beta). \end{aligned}$$

It's a fact of Galois theory that if L and M are Galois extensions of K then $\mathrm{Gal}(LM/K) \cong H$ where

$$H \leqslant \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$$

and

$$H = \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$$

if $L \cap M = K$. So $K(\sqrt[n]{\Delta})$ is the compositum $\prod_{a\in\Delta} K(\sqrt[n]{a})$. So

$$\begin{aligned} \mathrm{Gal}(K(\sqrt[n]{\Delta})/K) &\hookrightarrow \prod_{a\in\Delta} \mathrm{Gal}(K(\sqrt[n]{a})/K) \\ &\hookrightarrow \mu_n^\Delta. \end{aligned}$$

□

Interestingly, the converse is also true.

Proposition 2. *Suppose L/K is an abelian extension of exponent n, then $L = K(\sqrt[n]{\Delta})$ where $\Delta = (L^\times)^n \cap K^\times$. If, in particular, L/K is a cyclic extension then $L = K(\sqrt[n]{a})$ for some $a \in K^\times$.*

We'll need a theorem of Hilbert to prove this.

Definition. Given a field extension L/K, define $H^{-1}(\mathrm{Gal}(L/K), L^\times) = \{\ell \in L : N_{L/K}(\ell) = 1\}/I_{\mathrm{Gal}(L/K)}$ where $I_{\mathrm{Gal}(L/K)}$ is the subgroup of $\{\ell \in L : N_{L/K}(\ell) = 1\}$ generated by all elements $\sigma(a)/a$, $a \in L^\times$, $\sigma \in \mathrm{Gal}(L/K)$. Note that if $\mathrm{Gal}(L/K)$ is cyclic with generator σ then

$$I_{\mathrm{Gal}(L/K)} = \{\sigma(a)/a : a \in L^\times\}.$$

Theorem (Hilbert 90)**.** *If L/K is a cyclic extension then*

$$H^{-1}(\mathrm{Gal}(L/K), L^\times) = 1,$$

i.e. if $\alpha \in L^\times$, $N_{L/K}(\alpha) = 1$, then $\alpha = 1\sigma(\beta)/\beta$ for some $\beta \in L^\times$.

□

Proof of Proposition 2. Want to show that $L = K(\sqrt[n]{\Delta})$, $\Delta = (L^\times)^n \cap K^\times$.

First we'll show $K(\sqrt[n]{\Delta}) \subseteq L$. Pick $\alpha \in \sqrt[n]{\Delta}$, then $\alpha^n \in (L^\times)^n \cap K^\times$. Say $\alpha^n = a$, so $a = \beta^n$ for some $\beta \in L^\times$. Then $\alpha = \zeta_n^r \beta$, $0 \leqslant r < n$, hence $\alpha \in L$.

Now we'll show that $L \subseteq K(\sqrt[n]{\Delta})$. L is the compositum of all finite intermediate field extensions M/K. Each group $\mathrm{Gal}(M/K)$ is abelian and finite, hence is a product of cyclic groups. In fact, then, L is the compositum of cyclic extensions. Let M/K be a cyclic intermediate field extension. If we can show that $M \subseteq K(\sqrt[n]{\Delta})$ then $L \subseteq K(\sqrt[n]{\Delta})$.

Let σ generate $\mathrm{Gal}(M/K)$ and let $d = [M : K]$, so $d \mid n$, say $n = dd'$. Consider $\xi = \zeta_n^{d'}$. Note that $\xi \in K$ and is a $n/d' = d$-th root of unity. We have $N_{M/K}(\xi) = \xi^d = 1$, so, by Hilbert 90,

$$\xi = \frac{\sigma(\alpha)}{\alpha}, \quad \alpha \in M^\times.$$

So $K(\alpha) \subseteq M$. Also,

$$\begin{aligned}\sigma^2(\alpha) &= \sigma(\xi\alpha) \\ &= \sigma(\xi)\sigma(\alpha) \\ &= \xi\xi\alpha \\ &= \xi^2\alpha.\end{aligned}$$

Indeed, $\sigma^i(\alpha) = \xi^i\alpha$, so $\sigma^i(\alpha) = \alpha$ if and only if $\xi^i = 1$, and since ξ is a dth root of unity this occurs if and only if $d \mid i$. Hence, by standard Galois theory, $K(\alpha) = M$. If $\alpha \in \sqrt[n]{\Delta}$, we're done. But

$$\frac{\sigma(\alpha^n)}{\alpha^n} = \left(\frac{\sigma(\alpha)}{\alpha}\right)^n = \xi^n = 1,$$

since $d \mid n$. So $\sigma(\alpha^n) = \alpha^n$, and so inductively $\sigma^i(\alpha^n) = \alpha^n$ for all i, so $\alpha^n \in K^\times$, hence $\alpha^n \in (M^\times)^n \cap K^\times \subseteq \Delta$. □

Theorem. *The correspondence $\Delta \to L = K(\sqrt[n]{\Delta})$ is a bijection between groups Δ such that $(K^\times)^n \subseteq \Delta \subseteq K^\times$ and abelian extensions of exponent n. If Δ and L correspond to one another then $\Delta = (L^\times)^n \cap K^\times$ and there is a canonical isomorphism $\Delta/(K^\times)^n \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$.*

□