Lecture 12: Kummer Theory

William Stein

Feb 8, 2010

1 Kummer Theory of Fields

Kummer theory is concerned with classifying the abelian extensions of exponent n of a field K, assuming that K contains the nth roots of unity. It's a generalization of the correspondence between quadratic extensions of $\mathbb{Q}$ and non-square squarefree integers.

Let n be a positive integer, and let K be a field of characteristic prime to n. Let L be a separable closure of K. Let $\mu_n(L)$ denote the set of elements of order dividing n in L.

Lemma 1.1. *$\mu_n(L)$ is a cyclic group of order n.*

Proof. The elements of $\mu_n(L)$ are exactly the roots in L of the polynomial $x^n - 1$. Since n is coprime to the characteristic, all roots of $x^n - 1$ are in L, so $\mu_n(L)$ has order at least n. But K is a field, so $x^n - 1$ can have at most n roots, so $\mu_n(L)$ has order n. Any finite subgroup of the multiplicative group of a field is cyclic, so $\mu_n(L)$ is cyclic. $\square$

Consider the exact sequence

$$1 \to \mu_n(L) \to L^* \xrightarrow{x \mapsto x^n} L^* \to 1$$

of $G_K = \mathrm{Gal}(L/K)$-modules. The associated long exact sequence of Galois cohomology yields

$$1 \to K^*/(K^*)^n \to \mathrm{H}^1(K, \mu_n(L)) \to \mathrm{H}^1(K, L^*) \to \cdots .$$

We proved that $\mathrm{H}^1(K, L^*) = 0$, so we conclude that

$$K^*/(K^*)^n \cong \mathrm{H}^1(K, \mu_n(L)),$$

where the isomorphism is via the δ connecting homomorphism. If $\alpha \in L^*$, we obtain the corresponding element $\delta(\alpha) \in \mathrm{H}^1(K, \mu_n(L))$ by finding some $\beta \in L^*$ such that $\beta^n = \alpha$; then the corresponding cocycle is $\sigma \mapsto \sigma(\beta)/\beta \in \mu_n(L)$.

As a special case, consider $n = 2$ and $K = \mathbb{Q}$. Then we have $\mu_2(\overline{\mathbb{Q}}) = \{\pm 1\}$, on which $G_{\mathbb{Q}}$ acts trivially. Recall that $\mathrm{H}^1(G, A) = \mathrm{Hom}(G, A)$ when G acts trivially on A. Thus

$$\mathbb{Q}^*/(\mathbb{Q}^*)^2 \cong \mathrm{Hom}(G_{\mathbb{Q}}, \{\pm 1\}),$$

where the homomorphisms are continuous. The set of squarefree integers are representative elements for the left hand side of the above isomorphism. The right hand side is the set of *continuous* homomorphisms $\varphi : G_{\mathbb{Q}} \to \{\pm 1\}$. To give such a nontrivial homorphism φ is exactly the same as giving a quadratic extension of $\mathbb{Q}$. We thus recover—in a conceptual way—the standard bijection between quadratic fields and squarefree integers $\neq 1$, which is one of the basic facts one learns in a first algebraic number theory course.

We generalize the above construction as follows. Suppose $\mu_n \subset K$, i.e., all the nth roots of unity are already in K. Then we have

$$K^*/(K^*)^n \cong \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}), \tag{1.1}$$

where as usual the homomorphisms are continuous. We associate to a homomorphism $\varphi : G_K \to \mathbb{Z}/n\mathbb{Z}$ an extension L^H of K, where $H = \ker(\varphi)$, and by Galois theory, $\mathrm{Gal}(L^H/K) \cong \mathrm{image}(\varphi) \subset \mathbb{Z}/n\mathbb{Z}$. Conversely, given any Galois extension M/K with Galois group contained in $\mathbb{Z}/n\mathbb{Z}$, there is an associated homorphism $\varphi : G_K \to \mathrm{Gal}(M/K) \subset \mathbb{Z}/n\mathbb{Z}$. Define an equivalence relation $\sim$ on $\mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z})$ by $\varphi \sim \psi$ if $\ker(\varphi) = \ker(\psi)$ (equivalently, $\varphi = m\psi$ for some integer m coprime to n). Then we have a bijection

$$\mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z})_{/\sim} \xrightarrow{\cong} \{\text{ Galois extensions } M/K \text{ with } \mathrm{Gal}(M/K) \subset \mathbb{Z}/n\mathbb{Z} \text{ }\}.$$

Using Equation 1.1 along with the explicit description of δ mentioned above, we thus see that the Galois extensions of K with $\mathrm{Gal}(M/K) \subset \mathbb{Z}/n\mathbb{Z}$ are the extensions of the form $K(\sqrt[n]{\alpha})$ for some $\alpha \in K^*$. An element $\sigma \in \mathrm{Gal}(M/K)$ acts by $\sqrt[n]{\alpha} \mapsto \sqrt[n]{\alpha}^b$ for some b, and the map $\mathrm{Gal}(M/K) \subset \mathbb{Z}/n\mathbb{Z}$ is $\sigma \mapsto b$.

The above observation is **Kummer theory**: *There is a conceptually simple description of the exponent n abelian extensions of K, assuming that all nth roots of unity are in K.* Of course, understanding $K^*/(K^*)^n$ well involves understanding the failure of unique factorization into primes, hence understanding the unit group and class group of the ring of integers of K well.

When the nth roots of unity are not in K, the situation is much more complicated, and is answered by Class Field Theory.

Remark 1.2. A concise general reference about Kummer theory of fields is Birch's article *Cyclotomic Fields and Kummer Extensions* in Cassels-Frohlich. For a Galois-cohomological approach to Class Field Theory, see the whole Cassels-Frohlich book.

2 Kummer Theory for an Elliptic Curve

Let n be a positive integer, and let E be an elliptic curve over a field K of characteristic coprime to n, and let $L = K^{\mathrm{sep}}$. We mimic the previous section, but for the G_K-module $E(L)$ instead of L^*. Consider the exact sequence

$$0 \to E[n] \to E \xrightarrow{[n]} E \to 0.$$

Taking cohomology we obtain an exact sequence

$$0 \to E(K)/nE(K) \to \mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(K, E)[n] \to 0.$$

Unlike the above situation where $\mathrm{H}^1(K, L^*) = 0$, the group $\mathrm{H}^1(K, E)[n]$ is often very large, e.g., when K is a number field, this group is always infinite.

In Kummer theory, we obtained a nice result under the hypothesis that $\mu_n \subset K$. The analogous hypothesis in the context of elliptic curves is that every element of $E[n]$ is defined over K, in which case

$$\mathrm{H}^1(K, E[n]) \approx \mathrm{Hom}(G_K, (\mathbb{Z}/n\mathbb{Z})^2),$$

where we have used that $E[n](L) \approx (\mathbb{Z}/n\mathbb{Z})^2$, which is a standard fact about elliptic curves, and as usual all homomorphisms are continuous. Another consequence of our hypothesis that $E[n](K) = E[n]$ is that $\mu_n \subset K$; this later fact can be proved using the Weil pairing, which is a nondegenerate G_K-invariant map

$$E[n] \otimes E[n] \to \mu_n.$$

As above, we can interpret the elements $\varphi \in \mathrm{Hom}(G_K, (\mathbb{Z}/n\mathbb{Z})^2)$ (modulo an equivalence relation) as corresponding to abelian extensions M of K such that $\mathrm{Gal}(M/K) \subset (\mathbb{Z}/n\mathbb{Z})^2$. Moreover, we have upon fixing a choice of basis for $E[n]$, an exact sequence

$$0 \to E(K)/nE(K) \to \mathrm{Hom}(G_K, (\mathbb{Z}/n\mathbb{Z})^2) \to \mathrm{H}^1(K, E)[n] \to 0,$$

or, using Kummer theory from the previous section,

$$0 \to E(K)/nE(K) \to (K^*/(K^*)^n)^2 \to \mathrm{H}^1(K, E)[n] \to 0.$$

Another standard fact about elliptic curves—the (weak) Mordell-Weil theorem—is that when K is a number field, then $E(K)/nE(K)$ is finite. Thus when $E[n](K) = E[n]$, we have a fairly explicit description of $\mathrm{H}^1(K, E)[n]$ in terms of K^* and $E(K)$. This idea is one of the foundations for using descent to compute Mordell-Weil groups of elliptic curves.

If we restrict to classes whose restriction everywhere locally is 0 we obtain the sequence

$$0 \to E(K)/nE(K) \to \mathrm{Sel}^{(n)}(E/K) \to Ш(E/K)[n] \to 0.$$

Here

$$\mathrm{Sel}^{(n)}(E/K) = \ker\left(\mathrm{H}^1(K, E[n]) \to \bigoplus_{\text{all } v} \mathrm{H}^1(K_v, E)\right),$$

and

$$Ш(E/K) = \ker\left(\mathrm{H}^1(K, E) \to \bigoplus_{\text{all } v} \mathrm{H}^1(K_v, E)\right).$$

When K is a number field, it is possible to describe $\mathrm{Sel}^{(n)}(E/K)$ so explicitly as a subgroup of $(K^*/(K^*)^n)^2$ that one can prove that $\mathrm{Sel}^{(n)}(E/K)$ is computable.

Theorem 2.1. *Given any elliptic curve E over any number field K, and any integer n, the group $\mathrm{Sel}^{(n)}(E/K)$ defined above is computable.*

It is a major open problem to show that $E(K)$ is computable. A positive solution would follow from the following conjecture:

Conjecture 2.2 (Shafarevich-Tate)**.** *The group $Ш(E/K)$ is finite.*

Conjecture 2.2 is extremely deep; for example, it is a very deep (hundreds of pages!) theorem when $E/\mathbb{Q}$ has "analytic rank" 0 or 1, and is not known for even a single elliptic curve defined over $\mathbb{Q}$ with analytic rank ≥ 2.

Example 2.3. Consider an elliptic curve E over $\mathbb{Q}$ of the form $y^2 = x(x-a)(x+b)$, so that all the 2-torsion of E is $\mathbb{Q}$-rational. As above, we obtain an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to ((\mathbb{Q}^*)/(\mathbb{Q}^*)^2)^2 \to \mathrm{H}^1(\mathbb{Q}, E)[2] \to 0.$$

From this diagram and the fact that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, we see that $\mathrm{H}^1(\mathbb{Q}, E)[2]$ is infinite. Moreover, given any pair (α, β) of nonzero rational numbers, we can write down an explicit Galois cohomology class in $\mathrm{H}^1(\mathbb{Q}, E)[2]$, and given any rational point $P \in E(\mathbb{Q})$ we obtain a pair of rationals in $((\mathbb{Q}^*)/(\mathbb{Q}^*)^2)^2$.