Galois Cohomology and Kummer Theory

1 A Question about Cyclic Field Extensions

Here's a natural question.

Question 1.1

Let L/K be a Galois extension, and suppose that the Galois group $G = Gal(L/K) \cong \mathbb{Z}/n\mathbb{Z}$. Then is $L = K(\sqrt[n]{a})$ for some $a \in K$?

The answer, it turns out, is no, and one doesn't have to look far to find a counterexample, just take any Galois extension $K/\mathbb{Q}$ with Galois group $\mathbb{Z}/3\mathbb{Z}$ (for example, the splitting field of $x^3 + x^2 - 2x - 1$.). The proof isn't too tricky, if $K = \mathbb{Q}(\sqrt[3]{a})$, then as a $\mathbb{Q}$-vecor space $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt[3]{a} \oplus \mathbb{Q}\sqrt[3]{a}^2 \subseteq \mathbb{R}$. But the Galois conjugates of $\sqrt[3]{a}$ are:

$$\sqrt[3]{a}, \zeta\sqrt[3]{a}, \zeta^2\sqrt[3]{a},$$

where ζ is a primitive cube root of 1. In particular, the last two of these are not contained in K, so that K is not Galois. (You can also factor $x^3 - a = (x - \sqrt[3]{a})(x^2 + x\sqrt[3]{a} + \sqrt[3]{a}^2)$ and see that the discriminant of the latter is negative, so that it can't factor any further and thus the minimal polynomial of $\sqrt[3]{a}$ doesn't split).

Notice that if $\mathbb{Q}$ had contained ζ, then we would have had no trouble observing that the extension K was Galois. Indeed, an extension K is Galois precisely when all the conjugates of a primitive element are in K. Alternatively, one could factor the minimal polynomial $x^3 - a = (x - \sqrt[3]{a})(x - \zeta\sqrt[3]{a})(x - \zeta^2\sqrt[3]{a})$ and see it splits.

Let's summarize our observations so far, but in a slightly more general context. Suppose L/K is a Galois extension with $Gal(L/K) \cong \mathbb{Z}/n\mathbb{Z}$. If we want $L \cong K(\sqrt[n]{a})$ for some $a \in K$, (notice this implicitly assumes $x^n - a$ is irreducible in $K[x]$), then we need the n-th roots of unity to be in L. Indeed, as L is Galois, the minimal polynomial of a must split in L:

$$x^n - a = (x - \sqrt[n]{a})(x - \zeta\sqrt[n]{a}) \cdots (x - \zeta^{n-1}\sqrt[n]{a}).$$

Here ζ is now a primitive n'th root of 1. Since Galois acts transitively on the roots of this polynomial, this says that $\zeta\sqrt[n]{a} \in L$ so that $\zeta = \zeta\sqrt[n]{a}/\sqrt[n]{a} \in L$.

Question 1.2

Can one use that the Galois group is $\mathbb{Z}/n\mathbb{Z}$ to show that in fact $\zeta \in K$?

In particular, we've seen that that a positive answer to Question 1.1 has an explicit obstruction: if K does not contain a primitive n'th root of unity, then the answer is no. On its surface, this obstruction seems much stronger than what is necessary. It tells us that if K does not contain a primitive n'th root of unity, then $K(\sqrt[n]{a})$ isn't even Galois of degree n. That is, it tells us that the answer to Question 1.1 is **always no**. That is, at a glance, giving K a primitive root of 1 puts us in the situation where maybe the answer to Question 1.1 is **sometimes**. The remarkable fact is that this is the *only* obstruction. That is, if K has a primitive root of unity, the answer to Question 1.1 is **always yes**! (With some restrictions on the characteristic of K).

Theorem 1.3

Let L/K be a Galois extension and suppose that the Galois group $G = Gal(L/K) \cong \mathbb{Z}/n\mathbb{Z}$, and suppose that the characteristic of K does not divide n. If K contains a primitive n'th root of 1, then $L \cong K(\sqrt[n]{a})$ for some $a \in K$.

The goal of this project is to prove this fact. Notice that there is nothing cohomological in nature about this statement. But a remarkably clever proof of this fact can be extracted from the long exact sequence on cohomlogy for a particular (right) derived functor.

2 Group Cohomology

To turn this problem into a cohomological one we use the following definition.

Definition 2.1. *Let G be a group. A G module is an abelian group A equipped with an action by G by automorphisms.*

Exercise 2.2

Show that the following characterizations of the notion of a G-module are equivalent.

1. A G-module A (as in Definition 2.1).
2. An abelian group A together with a group homomorphisms $G \to \operatorname{Aut} A$.
3. A (ring theoretic) module A over the group algebra $\mathbb{Z}[G]$.

The crucial example for this project is the following.

Example 2.3

Let K be a field and L/K a Galois field extension with Galois group G. Then the Galois action naturally makes K and L into G-modules with their underlying additive abelian group structure. (What is the action on K?). Similarly, the multiplicative groups $K^\times$ and $L^\times$ have natural G-module strucutres (with their multiplicative abelian group structures).

We can make G-modules into a category as follows.

Definition 2.4. *Let A and B be G-modules. A homomorphism $\varphi : A \to B$ is called G-equivariant if for any $g \in G$ and $a \in A$ one has:*

$$\varphi(g \cdot a) = g \cdot \varphi(a).$$

Exercise 2.5

1. Show that the category of G-modules with G-equivariant homomorphisms is an abelian category.
2. Show that the category of G-modules has enough injectives.

We now can define the following functor from G-modules to abelian groups:

Definition 2.6. *Let A be a G-module. The G-invariance of A is $A^G = \{a \in A : g \cdot a = a \text{ for all } g \in G\}$.*

Exercise 2.7

Let K and L be as in example 2.3. Compute $L^G, (L^\times)^G, K^G, (K^\times)^G$.

Exercise 2.8

Show that $A \mapsto A^G$ is a left exact functor from the category of G-modules to the category of abelian groups.

Due to Exercises 2.5 and 2.8, we may define the right derived functors of invariance, which is the *group cohomology*. The i'th right derived functor will be denoted:

$$\mathrm{H}^i(G, \bullet).$$

Exercise 2.9

Let $\mathbb{Z}$ be a G-module equipped with a trivial action, and A any G-module. View both as (ring theoretic) $\mathbb{Z}[G]$ modules.

1. Show $A^G \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$.
2. Show $\mathrm{H}^i(G, A) \cong \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$

3 Galois Cohomology and the Kummer Sequence

Now we have the basic construction of group cohomology. We want to apply this general framework in a Galois theoretic context. Like we saw in Example 2.3 and Exercise 2.7, Galois theory gives us a natural source of G-modules. We first give the following definition.

Definition 3.1. *For a positive integer n and a ring R, we define the n'th roots of unity to be*

$$\mu_n(R) := \{r \in R : r^n = 1\}.$$

Notice that taking the n'th roots of unity gives a functor from commutative rings to abelian groups.

Exercise 3.2

Let K be a field extension and n an integer prime the the characteristic of K. Let $\overline{K}$ be a separable closure of K (in characteristic 0 this is the same as an algebraic closure). Let $\Gamma_K = Gal(\overline{K}/K)$ be the Galois group.

1. Show that $\mu_n(\overline{K})$ is a Γ_K module, and compute its invariance: $\mu_n(\overline{K})^{\Gamma_K}$.
2. Prove that the following is an exact sequence in the category of Γ_K-modules:
$$1 \longrightarrow \mu_n(\overline{K}) \longrightarrow \overline{K}^\times \xrightarrow{x \mapsto x^n} \overline{K}^\times \longrightarrow 1.$$
This is often called the *Kummer sequence.*

Now let's outline the general strategy to prove Theorem 1.3. Indeed, we can run the general machinery of cohomology to automatically obtain the following exact sequence:

$$0 \longrightarrow \mu_n(\overline{K})^{\Gamma_K} \longrightarrow (\overline{K}^\times)^{\Gamma_K} \longrightarrow (\overline{K}^\times)^{\Gamma_K} \xrightarrow{\delta} \mathrm{H}^1(\Gamma_K, \mu_n(\overline{K})) \longrightarrow \mathrm{H}^1(\Gamma_K, \overline{K}^\times). \tag{1}$$

Your objectives are now the following.

Exercise 3.3

(i) Prove $\mathrm{H}^1(\Gamma_K, \overline{K}^\times) = 0$. This is often known as Hilbert's theorem 90.

(ii) Suppose $\mu_n(\overline{K}) \subseteq K$. Then establish a correpondence between elements of $\mathrm{H}^1(\Gamma_K, \mu_n(\overline{K}))$ and Galois extension of K with galois group isomorphic to $\mathbb{Z}/m\mathbb{Z}$ for some m dividing n.

(iii) Find a suitable interpretation of the boundary map δ in terms of part (b). That is, given some element $a \in (\overline{K}^\times)^{\Gamma_K}$, describe the cyclic extension $\delta(a)$ correesponds to in terms of a. (Recall that you computed $(\overline{K}^\times)^{\Gamma_K}$ in exercise 2.7.

Putting Exercise 3.3 together with the exactness of Sequence (1) should then give a straightforward proof of Theorem 1.3.

4 The Bar Resolution

The key to solving Exercise 3.3 (and the general trick to excplicitly computing group cohomology, at least in low degrees) is to construct an explicit cochain complex $C^\bullet(G, A)$ for which:

$$\mathrm{H}^i(G, A) = \mathrm{H}^i(C^\bullet(G, A)).$$

One can do this quite explicitly, the idea is to use Exercise 2.9 to translate the problem into finding a projective resolution $\mathbb{Z}$ in the category of $\mathbb{Z}[G]$-modules, and then applying $\mathrm{Hom}_{\mathbb{Z}[G]}(\bullet, A)$ to that resolution. This resolution I think is called the Bar resolution.

Exercise 4.1

A good reference for this part (which spells out some of the details more carefully) is Dummit and Foote Chapter 17.2 Exercises 1 and 3. For this problem we let G be a finite group.

1. Show that the *augmentation map aug* : $\mathbb{Z}[G] \to \mathbb{Z}$ defined by the rule $\sum a_i g_i \mapsto \sum a_i$ is a surjective map of G-modules.

2. Define:
$$F_n := \underbrace{\mathbb{Z}[G] \otimes \mathbb{Z}[G] \otimes \cdots \otimes \mathbb{Z}[G]}_{n+1\text{-times}}.$$
Define an action on of G F_n on simple tensors via the rule:
$$g \cdot (g_0 \otimes g_1 \otimes \cdots \otimes g_n) = gg_0 \otimes g_1 \otimes \cdots \otimes g_n.$$
Show that F_n is a projective (even free!) $\mathbb{Z}[G]$-module, generated by elements of the for $1 \otimes g_1 \otimes \cdots \otimes g_n$.

3. For $n > 0$, define a differential $d_n : F_n \to F_{n-1}$ on generators via the rule:
$$1 \otimes g_1 \otimes \cdots \otimes g_n \mapsto g_1 \otimes \cdots \otimes g_n + \sum_{i=1}^{n-1} g_1 \otimes \cdots \otimes g_i g_{i+1} \otimes \cdots \otimes g_n + (-1)^n g_1 \otimes \cdots \otimes g_{n-1}.$$
Prove that:
$$\cdots \xrightarrow{d_4} F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{aug} \mathbb{Z},$$
is a projective (even free!) resolution of $\mathbb{Z}$ in the category of G-modules. (Show it's null homotopic. [DF] 17.2 Exercise 1 describes a chain homotopy which might be helpful).

4. We now get a cochain complex by applying mapping into A. Define $C^i(G, A) = \mathrm{Hom}_{\mathbb{Z}[G]}(F_i, A)$. Deduce that:
$$\mathrm{H}^i(G, A) = \mathrm{H}^i(C^\bullet(G, A)).$$

5. This is really only helpful if we can get a good grasp on what $C^i(G, A)$ is. But the F_i are taylor made to translate back into group theory. Give an identification between $\mathrm{Hom}_{\mathbb{Z}[G]}(F_i, A)$ and the set of functions $G^i \to A$ (not group homomorphisms!). (Here G^i is the cartesian product of i-copies of G, where $G^0 = \{id\}$). Unwind what the differentials do with this intepretation. (This is written up in [DF] Equation 17.18).

6. That was a mouthful. As a sanity check, use your intepretation from part (e) to confirm that $\mathrm{H}^0(G, A) = A^G$.

7. We care about H^1. Give an explicit description of H^1. In particular, by part (e) you can identify $C^1(G, A)$ with functions $f : G \to A$. Explicitly describe what it means for f to be a cocycle. What about a coboundary?