1. Kummer theory and Galois cohomology

Let K be a field and let $\overline{K}$ be a separable closure of K. Let $G = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K.

Definition 1.1. *A discrete G-module M is an abelian group M with a continuous action of G, where we equip M with the discrete topology. A morphism of G-modules is a homomorpism of abelian groups compatible with the action of G.*

Let M be a discrete G-module. To M we associate two abelian groups:

- $H^0(G; M) = M^G$ the subgroup of M of elements invariant under the action of G.
- $H^1(G; M) = Z^1(G; M)/B^1(G; M)$ the group of one-cocycles modulo one-coboundaries. A *one-cocycle* is a continuous function $c\colon G \to M$ satisfying
$$c(\sigma\tau) = c(\sigma) + \sigma c(\tau).$$
A *one-coboundary* is a one-cocycle of the form
$$c(\sigma) = \sigma(m) - m,$$
where $m \in M$ is some element. It is not hard to see that the set of one-cocycles $Z^1(G; M)$ forms an abelian group, and that the set of one-coboundaries $B^1(G; M)$ defines a subgroup of $Z^1(G; M)$.

The assignments $M \mapsto H^0(G, M)$ and $M \mapsto H^1(G; M)$ are of course also functorial.

Example 1.2. Consider the G-module $\overline{K}^\times$. By Galois theory, we have
$$H^0(G; \overline{K}^\times) = (\overline{K}^\times)^G = K^\times.$$
It turns out that
$$H^1(G; \overline{K}^\times) = 0.$$
This is known as Hilbert's Theorem 90. You can find the proof in [Har, Theorem 5.2 and Corollary 5.3]. An alternative proof is suggested by the project "conics and quoternions" ;). ▲

The usefulness of the groups $H^0(G;M)$ and $H^1(G;M)$ stems from the following theorem.

Theorem 1.3. *Let*

$$0 \to M'' \to M \to M' \to 0$$

be a short exact sequence of G-modules. Then we obtain an exact sequence

$$\begin{aligned} 0 \to H^0(G;M'') \to H^0(G;M) \to H^0(G;M') \\ \xrightarrow{\delta} H^1(G;M'') \to H^1(G;M) \to H^1(G;M'). \end{aligned}$$

The connecting homomorphism $\delta\colon H^0(G;M) \to H^1(G;M')$ is defined by sending $x \in H^0(G;M) = M^G$ to the class of the one-cocycle

$$\sigma \mapsto \sigma(y) - y,$$

where y denotes a lift of x to M.

Proof. Exercise! ■

1.1. **Kummer Theory.** Fix an intger $n \geq 1$. We now specialize to the case where K contains μ_n, the group of n-th roots of unity in $\overline{K}$. Kummer theory explicitly gives us all finite cyclic extensions of K of order dividing n. Firstly, there is the following proposition.

Proposition 1.4. *There is a bijective correspondence between on the one hand cyclic extension $K \subset L \subset \overline{K}$ of K of order dividing n, and on the other hand cyclic subgroups of* $\mathrm{Hom}(G, \mu_n)$ *of order d dividing n.*

Proof. This is an exercise in Galois theory. ■

To connect the observation above with Galois cohomology, notice that μ_n is a G-module with trivial action of G, because $\mu_n \subset K$. It follows that

$$H^1(G, \mu_n) = \mathrm{Hom}(G, \mu_n).$$

We can understand the group $H^1(G, \mu_n)$ more concretely using Theorem 1.3 and Example 1.2. To this end, consider the exact sequence of G-modules

$$1 \to \mu_n \to \overline{K}^\times \xrightarrow{\times n} \overline{K}^\times \to 1.$$

From it, we obtain the exact sequence

$$K^\times \xrightarrow{\times n} K^\times \xrightarrow{\delta} H^1(G, \mu_n) \to H^1(G, \overline{K}^\times) = 0.$$

This in turn gives us an isomorphism

$$\delta\colon K^\times/(K^\times)^n \xrightarrow{\simeq} H^1(G, \mu_n).$$

Using the explicit description of the connecting map δ from the proof of 1.3, in combination with Proposition 1.4, we obtain

Theorem 1.5 ([Har, Theorem 5.6])**.** *There is a bijective correspondence between on the one hand cyclic extensions $K \subset L \subset \overline{K}$ of order dividing n, and on the other hand cyclic subgroups of $K^\times/(K^\times)^n$ of order dividing n. Explicitly, a subgroup $\langle \alpha \rangle \subset K^\times/(K^\times)^n$ corresponds to the extension $K \subset K(\sqrt[n]{\alpha})$.*

2. Goals for a report

Firstly, prove all the necessary theory on Galois cohomology, such as the long exact sequence and Hilbert's Theorem 90. If you want, you can define the cohomology groups very abstractly using the theory of derived functors as in [Har]. This is not necessary, however. Next, you should of course fully prove Kummer theory. Our Theorem 1.5 can be generalized, which you can also touch on in your report. See [Har, Corollary 5.7]. If you have time, you can discuss more applications of Galois cohomology.

2.1. **Prerequisites.**

As the description of this project makes clear, you should be familiar with Galois theory. Preferably, you also know infinite Galois theory, but this can be avoided entirely by "taking a limit over the finite Galois extensions". See [Har].

References

[Har] Kris Harper. *Group Cohomology and Kummer Theory*. URL: `https://www.math.uchicago.edu/~may/VIGRE/VIGRE2010/REUPapers/Harper.pdf`.