GALOIS EXTENSIONS AND GALOIS COHOMOLOGY

GAL PORAT

Abstract. In this note we use Galois cohomology to describe Galois extensions of a given base field. A control theorem allows us to relate these Galois extensions as we change the base field via the representation theory of these cohomology groups. As applications, we derive classical Kummer theory and give a description $\mathbb{Z}/p$ extensions of an arbitrary field. Many of the results described here are also consequences of class field theory, but the arguments given here are unconditional.

1. Generalities on Galois cohomology and Galois extensions

Throughout this note, all homomorphisms are assumed continuous and all subgroups are closed. Say a topological group A is *nice* if it has the following property: for any subgroups $H_1, H_2 \leq A$ and an isomorphism $\psi : H_1 \xrightarrow{\sim} H_2$, there exists an $\alpha \in \mathrm{Aut} A$ with $\alpha|_{H_1} = \psi$. (Pro-) cyclic groups are nice, and so are p-torsion group; S_3 is a nonabelian example.

For this section we fix a field K as well as a nice abelian group A. For all future applications the reader may assume that A is (pro-)cyclic.

Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K.

For nice groups (even if they are not abelian), we have the following classification of Galois extensions of K whose Galois group embeds into A. In the following, $\mathrm{Gal}(E/K) \leq A$ is always meant in the sense that there exists an embedding of $\mathrm{Gal}(E/K)$ into A.

Theorem 1.1. *There is a $1-1$ correspondence*

$$\{E/K \text{ Galois such that } \mathrm{Gal}(E/K) \leq A\} \longleftrightarrow \mathrm{Hom}(G_K, A)/\mathrm{Aut}(A).$$

Proof. By the Galois correspondence

$$\begin{aligned}\{E/K \text{ Galois such that } \mathrm{Gal}(E/K) \leq A\} &\longleftrightarrow \{N \triangleleft G_K \text{ such that } G_K/N \leq A\} \\ &\longleftrightarrow \{\ker\psi : \psi \in \mathrm{Hom}(G_K, A)\}.\end{aligned}$$

Now suppose $\psi_1, \psi_2 \in \mathrm{Hom}(G_K, A)$ and $N = \ker\psi_1 = \ker\psi_2$. Then $\mathrm{Im}\psi_1$ and $\mathrm{Im}\psi_2$ are isomorphic via $\mathrm{Im}\psi_1 \xrightarrow{\psi_1^{-1}} G_K/N \xrightarrow{\psi_2} \mathrm{Im}\psi_2$, and since G is nice, there exists an $\alpha \in \mathrm{Aut}A$ with $\alpha|_{\mathrm{Im}\psi_1} = \psi_2 \circ \psi_1^{-1}$; thus $\alpha \circ \psi_1 = \psi_2$. This shows that

$$\{\ker\psi : \psi \in \mathrm{Hom}(G_K, A)\} \longleftrightarrow \mathrm{Hom}(G_K, A)/\mathrm{Aut}(A),$$

concluding the proof. $\square$

Let L/K be a Galois extension, and set $\Gamma = \mathrm{Gal}(L/K)$. Sometimes $\mathrm{Hom}(G_L, A)$ is simpler than $\mathrm{Hom}(G_K, A)$, so it is useful to have the following control theorem.

Theorem 1.2. *There is an exact sequence*

$$0 \to \mathrm{Hom}(\Gamma, A) \to \mathrm{Hom}(G_K, A) \to \ker\left(\mathrm{Hom}(G_L, A)^\Gamma \to \mathrm{H}^2(\Gamma, A)\right) \to 0.$$

Here Γ *is acting on* $\mathrm{Hom}(G_L, A)$ *by conjugation on* G_L*.*

Proof. Use the inflation-restriction sequence. □

Corollary 1.1. *If* A *is coprime to* Γ *then* $\mathrm{Hom}(G_K, A) \xrightarrow{\sim} \mathrm{Hom}(G_L, A)^\Gamma$.

Remark 1.1. By Theorem 1.1, $\mathrm{Hom}(G_L, A)/\mathrm{Aut}(A)$ corresponds to those Galois extensions E/L for which $\mathrm{Gal}(E/L) \hookrightarrow A$. If A is coprime to Γ, Corollary 1.1 implies that $\mathrm{Hom}(G_K, A)/\mathrm{Aut}(A)$ maps isomorphically onto $\mathrm{Hom}(G_L, A)^\Gamma/\mathrm{Aut}(A)$; these are those extensions which descend to a Galois extension of K.

Remark 1.2. It is easy to check that Theorem 1.1 always induces a correspondence

$$\{E/K \text{ Galois such that } \mathrm{Gal}(E/L) \leq A\} \longleftrightarrow \left(\mathrm{Hom}(G_L, A)/\mathrm{Aut}(A)\right)^\Gamma.$$

Remark 1.3. If A is also a ring, then $A^\times \hookrightarrow \mathrm{Aut}(A)$ by multiplication, and $\mathrm{Hom}(G_L, A)$ can be thought of as an $A[\Gamma]$-module (or $A[[\Gamma]]$ if A and Γ are profinite). Then $\left(\mathrm{Hom}(G_L, A)/A^\times\right)^\Gamma$ is the set of rank ≤ 1 $A[\Gamma]$-submodules of $\mathrm{Hom}(G_L, A)$. Combining this with observation 1.2 shows that

$$\{E/K \text{ Galois such that } \mathrm{Gal}(E/L) \leq A\} \longleftrightarrow \{\text{rank} \leq 1\ A[\Gamma]\text{-submodules of } \mathrm{Hom}(G_L,\mathrm{A})\}/(\mathrm{Aut}(A)/A^\times).$$

In particular if A is cyclic, then $\mathrm{Aut}A = A^\times$ for the natural ring structure, as every automorphism is determined by the image of a generator. The correspondonce above then simplifies to

$$\{E/K \text{ Galois such that } \mathrm{Gal}(E/L) \leq A\} \longleftrightarrow \{\text{rank} \leq 1\ A[\Gamma]\text{-submodules of } \mathrm{Hom}(G_L,\mathrm{A})\}.$$

These extensions with $\mathrm{Gal}(E/L) \cong A$ correspond to saturated modules on the right hand side, which are those rank 1 $A[\Gamma]$-submodules of $\mathrm{Hom}(G_L, A)$ which are free over A.

Remark 1.4. If A is cyclic and coprime to Γ, then every extension of Γ by A is split by the Schur-Zassenhaus theorem. Thus any Galois extension E/K with $\mathrm{Gal}(E/L) \cong A$ has $\mathrm{Gal}(E/K) \cong A \rtimes \Gamma$. The action of Γ on A is then the same as the character $\Gamma \to \mathrm{Aut}(A) \cong A^\times$ determined by the corresponding rank 1 $A[\Gamma]$-module.

2. Classical Kummer Theory

In this section suppose that $\mu_n \subset K$. Under this assumption we can compute $\mathrm{Hom}(G_K, \mathbb{Z}/n)$. Indeed, taking Galois cohomology of the Kummer sequence

$$0 \to \mu_n \to \overline{K}^\times \xrightarrow{n} \overline{K}^\times \to 0$$

and applying Hilbert's theorem 90 shows that $\mathrm{Hom}(G_K, \mathbb{Z}/n) = \mathrm{H}^1(G_K, \mu_n) \xrightarrow{\sim} K^\times/K^{\times n}$. Thus in this case Theorem 1.1 is saying that

$$\{E/K \text{ Galois such that } \mathrm{Gal}(E/K) \leq \mathbb{Z}/n\} \longleftrightarrow \left(K^\times/K^{\times n}\right)/(\mathbb{Z}/n\mathbb{Z})^\times.$$

3. $\mathbb{Z}/p$ extensions

The case when $\mu_p \subset K$ was dealt with in the previous section, so let's assume $\mu_p \not\subseteq K$. Indeed, let $L = K(\mu_p)$, and let $\Delta = \mathrm{Gal}(L/K)$, as is standard notation. Then Δ is cyclic and has size dividing $p-1$, and in particular is coprime to p; we let ω be the cyclotomic character $\omega : \Delta \to \mathbb{F}_p^\times$ given by the action of Δ on μ_p. Then as Δ-representations, we have

$$\mathrm{Hom}(G_L, \mathbb{Z}/p)(1) = \mathrm{Hom}(G_L, \mu_p) = \mathrm{H}^1(G_L, \mu_p) \cong L^\times/L^{\times p}.$$

Letting $A = \mathbb{Z}/p = \mathbb{F}_p$, Remark 1.3 is saying that

$$\{E/K \text{ Galois with } \mathrm{Gal}(E/L) \cong \mathbb{F}_p\} \longleftrightarrow \left\{\text{rank 1 } \mathbb{F}_p[\Delta]\text{-submodules of } L^\times/L^{\times p}\text{(-1)}\right\}.$$

Remark 1.4 is saying that if a line on the right hand side is given by a character $\chi : \Delta \to \mathbb{F}_p^\times$, then the corresponding extension has Galois group $\mathbb{F}_p \rtimes_\chi \Delta$. On the other hand, as Δ is coprime to p, its representation theory over $\mathbb{F}_p$ is semisimple. So $L^\times/L^{\times p}(-1)$ can be written as some direct sum $\oplus \mathbb{F}_p(\omega^i)$, and each ω^i corresponds to a Galois extension with Galois group $\mathbb{F}_p \rtimes_{\omega^i} \Delta$. In particular, the $\mathbb{Z}/p$ extensions of K correspond to these lines of $L^\times/L^{\times p}$ for which Δ acts by ω.

3.1. K **a local field with residue characteristic** $\neq p$**.** In this case $\mathcal{O}_L^\times \simeq$ (prime to -p)$\times \mu$, where μ are the roots of unity of order prime to Char$K$. So $\mathcal{O}_L^\times/\mathcal{O}_L^{\times p} \cong \mathbb{F}_p(1)$, and tensoring the exact sequence $0 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0$ with $\mathbb{F}_p$ gives $0 \to \mathbb{F}_p(1) \to L^\times/L^{\times p} \to \mathbb{F}_p \to 0$. Therefore

$$L^\times/L^{\times p}(-1) \cong \mathbb{F}_p(-1) \oplus \mathbb{F}_p,$$

so there are 2 Galois extensions E of K containing L, such that $\mathrm{Gal}(E/L) \cong \mathbb{F}_p$. One of them has Galois group $\mathbb{F}_p \rtimes_{\omega^{-1}} \Delta$ and the other $\mathbb{F}_p \times \Delta$; the latter one rises from a $\mathbb{Z}/p$ extension of K, which is then the unique $\mathbb{Z}/p$-extension of K.

3.2. K **a local field with residue characterstic** p**.** Once again we have an exact sequence $0 \to \mathcal{O}_L^\times/\mathcal{O}_L^{\times p} \to L^\times/L^{\times p} \to \mathbb{F}_p \to 0$, and we need to analyze the first term. Let $\mathcal{M}_L$ be the maximal ideal of L, and let $\mathcal{O}_L^{(n)} := 1 + \mathcal{M}_L^n$. Then $\mathcal{O}_L^\times =$ (coprime to p) $\times\, \mathcal{O}_L^{(1)}$, so it suffices to analyze $\mathcal{O}_L^{(1)}$. We have the sequence

$$0 \to \mu_p \to \mathcal{O}_L^{(1)} \to \mathcal{O}_L^{(1)}/\mu_p \to 0$$

in which $\mathcal{O}_L^{(1)}/\mu_p$ is a free $\mathbb{Z}_p$-module, given that μ_p is the set of p-power roots of unity in L. In particular, it is flat, so it remains exact after tensoring with $\mathbb{F}_p$. As $\mathbb{F}_p[\Delta]$ is semisimple, this implies that

$$\mathcal{O}_L^\times/\mathcal{O}_L^{\times p} \cong \mathbb{F}_p \oplus \mathcal{O}_L^{(1)} \otimes \mathbb{F}_p = \mathbb{F}_p \oplus \mathbb{F}_p(1) \oplus \left(\mathcal{O}_L^{(1)}/\mu_p \otimes \mathbb{F}_p\right)$$

as $\mathbb{F}_p[\Delta]$ modules. Thus it remains to analyze $\mathcal{O}_L^{(1)}/\mu_p \otimes \mathbb{F}_p$.

Taking $n >> 0$, the $\mathbb{Z}_p$-module $\mathcal{O}_L^{(n)}$ becomes isomorphic to $\mathcal{O}_L$ as $\mathbb{F}_p[\Delta]$-modules via the logarithm map. By the normal basis theorem, $L \cong K[\Delta]$ as $K[\Delta]$-modules, so this implies that $\mathcal{O}_K[\Delta]$ is contained in $\mathcal{O}_L$, and hence in $\mathcal{O}_L^{(n)}$, as a $\mathbb{Z}_p[\Delta]$-submodule. The natural map $\mathcal{O}_L^{(n)} \to \mathcal{O}_L^{(1)}/\mu_p$ is injective for $n >> 0$, so $\mathcal{O}_L^{(1)}/\mu_p$ contains $\mathcal{O}_K[\Delta]$ as a $\mathbb{Z}_p[\Delta]$-submodule.

But both $\mathcal{O}_L^{(1)}/\mu_p$ and $\mathcal{O}_K[\Delta]$ have the same rank; as $\mathcal{O}_L^{(1)}/\mu_p$ is free over $\mathbb{Z}_p$, the only option is that $\mathcal{O}_L^{(1)}/\mu_p \cong \mathbb{Z}_p[\Delta]^{\oplus \#\Delta}$.
Putting this all together, we obtain

$$L^\times/L^{\times p}(-1) \cong \mathbb{F}_p(-1) \oplus \mathbb{F}_p \oplus \mathbb{F}_p[\Delta]^{\oplus\#\Delta},$$

so there are $2 + (\#\Delta)^2$ Galois extensions E of K containing L, such that $\mathrm{Gal}(E/L) \cong \mathbb{F}_p$. We have that $1 + \#\Delta$ of them have Galois group $\mathbb{F}_p \rtimes_{\omega^{-1}} \Delta$ and $\mathbb{F}_p \times \Delta$, and $\#\Delta$ of them have Galois group $\mathbb{F}_p \rtimes_{\omega^i} \Delta$ where $i \neq 0, -1$. In particular, there are $1 + \#\Delta$ different $\mathbb{Z}/p$-extensions of K.

3.3. $K = \mathbb{Q}$**.** The case $p = 2$ is treated by classical Kummer Theory, so we assume $p > 2$. Then $L = \mathbb{Q}(\mu_p)$ and $\Delta = \mathrm{Gal}(L/\mathbb{Q})$ has order $p-1$. We have the following exact sequence

$$0 \to \mathcal{O}_L^\times/\mathcal{O}_L^{\times p} \to L^\times/L^{\times p} \to \mathcal{I}/\mathcal{I}^p \to \mathcal{C}/\mathcal{C}^p \to 0,$$

where $\mathcal{I}$ is the group of ideals of L and $\mathcal{C}$ is the class group. Let's analyze the different components:

- The group $\mathcal{I}$ is free over $\mathbb{Z}$. Let l be a prime; if $l = p$ there is only one prime of $\mathcal{I}$ lying above it, and it is fixed by the action of Δ. If $l \neq p$, it is unramified of inertia degree $f = f_l$, where f is the order of l mod p; thus $l\mathcal{O}_L = \beta_1 \cdot ... \cdot \beta_g$, where $fg = p-1$. The action of Δ permuts these ideals transitively, which means that $\mathrm{span}_{\mathbb{F}_p}\{\beta_1, ..., \beta_g\} \cong \mathbb{F}_p \oplus \mathbb{F}_p(f) \oplus ... \oplus \mathbb{F}_p(f(g-1))$. Thus
$$\mathcal{I}/\mathcal{I}^p \cong \mathbb{F}_p \oplus \bigoplus_{l\neq p} \left(\mathbb{F}_p \oplus ... \oplus \mathbb{F}_p(f_l(g_l-1))\right).$$
- The representation $\mathcal{C}/\mathcal{C}^p$ is complicated: it is known that $\mathbb{F}_p, \mathbb{F}_p(1)$ do not appear as a consequence of Stickleberger's theorem. For $3 \leq n \leq p-2$ odd, it is known that $\mathbb{F}_p(n)$ appears if and only if p divides the Bernoulli number B_{p-n}. For $2 \leq n \leq p-1$ even, Vandiver's conjecture states that $\mathbb{F}_p(n)$ does not appear; it also implies (via a "reflection theorem") that for $3 \leq n \leq p-2$ odd, $\mathbb{F}_p(n)$ can appear at most once.
- Finally, we analyze $\mathcal{O}_L^\times/\mathcal{O}_L^{\times p}$. Let $L_+ = L \cap \mathbb{R}$; it is well known that $\mathcal{O}_L^\times = \mathcal{O}_{L_+}^\times$(roots of unity). This is equivalent to the exact sequence
$$0 \to \{\pm 1\} \to (\text{roots of unity}) \times \mathcal{O}_{L_+}^\times \to \mathcal{O}_L^\times \to 0,$$
which shows that
$$\mathcal{O}_L^\times/\mathcal{O}_L^{\times p} \cong \mathcal{O}_{L_+}^\times/\mathcal{O}_{L_+}^{\times p} \oplus \mathbb{F}_p(1).$$
Now let a be a generator of $\mathbb{F}_p^\times$, and consider the group C_+ of cyclotomic units in L_+, i.e. the group generated by the elements $\frac{\zeta_p^{at} - \zeta_p^{-at}}{\zeta_p - \zeta_p^{-1}}$, $t = 1, 2, ..., (p-1)/2$. The $(p-1)/2$ elements $\frac{\zeta_p^{at} - \zeta_p^{-at}}{\zeta_p^t - \zeta_p^{-t}}$ are all conjugate to each other by the action of . Therefore $\mathbb{Z}_p[\Delta/\{\pm 1\}] \cong C_+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \mathcal{O}_{L_+}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and $\mathcal{O}_{L_+}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is free of rank $(p-1)/2$, so the only option is that $\mathcal{O}_{L_+}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}_p[\Delta/\{\pm 1\}]$. Therefore
$$\mathcal{O}_L^\times/\mathcal{O}_L^{\times p} \cong (\mathbb{F}_p \oplus \mathbb{F}_p(2) \oplus ... \oplus \mathbb{F}_p(p-3)) \oplus \mathbb{F}_p(1).$$

Putting this all together, we have

$$L^\times/L^{\times p} \cong (\mathbb{F}_p \oplus \mathbb{F}_p(2) \oplus ... \oplus \mathbb{F}_p(p-3)) \oplus \mathbb{F}_p(1) \oplus \mathbb{F}_p \oplus \bigoplus_{l \neq p} (\mathbb{F}_p \oplus ... \oplus \mathbb{F}_p(f_l(g_l - 1))) \oplus \mathcal{C}/\mathcal{C}^p,$$

with $\mathcal{C}/\mathcal{C}^p$ conjecturally understood.

In any case, we do understand the $\mathbb{F}_p(1)$ component completely, because it never appears in $\mathcal{C}/\mathcal{C}^p$. We get one appearing in $\mathcal{O}_L^\times/\mathcal{O}_L^{\times p}$, which corresponds to $\mathbb{Z}/p$-extension contained in $\mathbb{Q}(\mu_p)$; and we get one appearing in $\mathbb{Q}(\mu_l)$ for each $l \equiv 1 \mod p$. In other words, this analysis proves Kronecker-Weber for cyclic extension of prime order.