

Math 250A Lecture 26 Notes

Daniel Raban

November 30, 2017

1 Infinite Extensions and Galois Cohomology

1.1 Hilbert's Theorem 90

Let's introduce the notation Lang uses for his version of Hilbert's theorem 90. Let G be a group and A be an abelian group with $G \curvearrowright A$.

Definition 1.1. A 1-cocycle of G in A is a family of elements $\{\alpha_\sigma\}_{\sigma \in G}$ such that

$$\alpha_{\sigma\tau} = \alpha_\sigma + \sigma\alpha_\tau.$$

Definition 1.2. A 1-coboundary of G in A is a family of elements $\{\alpha_\sigma\}_{\sigma \in G}$ such that there exists a fixed $\beta \in A$ such that $\alpha_\sigma = \sigma\beta - \beta$ for all $\sigma \in G$.

Theorem 1.1 (Hilbert's Theorem 90). *Let L/K be Galois with Galois group G . Then $H^1(G, L^*) = 1$.*

Proof. A 1-cocycle gives a twisted action $G \curvearrowright L$ given by $\sigma \mapsto a_\sigma\sigma$. So $(a_\sigma\sigma)(a_\tau\tau) = a_{\sigma\tau}\sigma\tau$ by the 1-cocycle condition. We want to find b with $a_\sigma\sigma b = b$ for all σ ; b is fixed by the twisted action and $b \neq 0$.

Find a fixed vector under G as $\sum_{\sigma \in G} \sigma v$, which is always fixed by G . A fixed vector under the twisted action is given by $b = \sum_{\sigma \in G} a_\sigma \cdot \sigma v$. We want to find v so b is nonzero. This is possible by Artin's theorem on the independence of σ , since otherwise, we could find a nonzero linear relation between these homomorphisms equal to 0. \square

Suppose G is cyclic, and let $N(a) = 1$ and $a = b/\sigma b$, where σ generates G . What is a 1-cocycle? Put $a_1 = 1$, $a_\sigma = a$, $a_{\sigma^2} = a_\sigma\sigma a_\sigma = a\sigma a$, and in general, $a_{\sigma^n} = a\sigma(a)\sigma^2(a) \cdots \sigma^{n-1}(a) = a_1 = 1$. So $N(a) = 1$ for this to give a 1-cocycle.

So since $N(a) = 1$, we get a 1-cocycle as above. Note that $a = b/\sigma b$ iff there is a cocycle given by $a_{\sigma^i} = b/\sigma^i b$ for all i , so a 1-cocycle is a 1-coboundary.

Theorem 1.2 (Hilbert's theorem 90). $H^1(G, L) = 0$, where L is considered as an additive group.

Proof. As a module over $K[H]$, L is isomorphic to $K[G]$, so it is a free module. L has a basis of the form $\{\sigma w : \sigma \in G\}$ for some fixed w ; this is a result called the normal basis theorem.¹ This shows that $H^i(G, L) = 0$ for $i > 0$. \square

Does $H^i(G, L^*) = 1$ for $i > 0$? No. $H^2(G, L^*)$ is often nonzero. This is related to the *Brauer group*. $H^1(G, L^*)$ is related to the *Picard group*. The Picard group of integers of a number field is a *class group*.

Why is Lang's definition of H^1 as cocycles/coboundaries ($a_{\sigma\tau} = a_\sigma + \sigma(a_\tau)$) the same as Borchers's definition $\text{Ext}_{\mathbb{Z}[G]}^1(\mathbb{Z}, M)$? Here is a sketch of a proof that they are the same.

To find $\text{Ext}(A, B)$, Take the free resolution of A . So we want a free resolution of \mathbb{Q} by free \mathbb{Z} -modules.

$$\mathbb{Z}[G] \otimes \mathbb{Z}[G] \otimes \mathbb{Z}[G] \rightarrow \mathbb{Z}[G] \otimes \mathbb{Z}[G] \rightarrow \mathbb{Z}[G] \rightarrow 0$$

These have respective \mathbb{Z} -bases

$$g_0 \otimes g_1 \otimes g_2, \quad g_0 \otimes g_1, \quad g_0, \quad 1$$

And we can map the basis elements by a map d , which sends a component to the identity. G acts by acting on each component. You should check that $d^2 = 0$ and that if $da = 0$, then $a = db$ for some b .

Now form the exact sequence

$$\leftarrow \text{Hom}(F_0, B) \leftarrow \text{Hom}(F_1, B) \leftarrow \text{Hom}(F_2, B)$$

where F_i is the *free resolution*.

Check that $d(a_\sigma) = 0$ iff the a_σ are a 1-cocycle (exercise). Then $\{a_\sigma\} = d(*)$ iff the a_σ s are a 1-coboundary.

1.2 Infinite Galois extensions

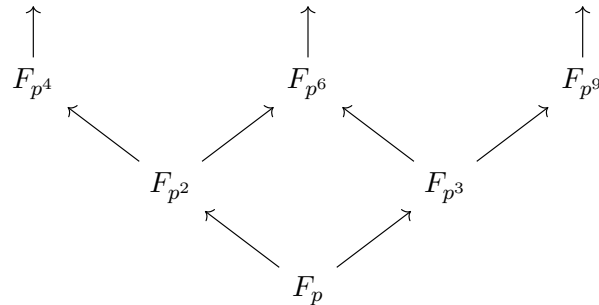
We want to look at extensions that are algebraic, normal, and separable.

Example 1.1. Take $\bar{\mathbb{Q}}/\mathbb{Q}$, where $\bar{\mathbb{Q}}$ is the algebraic closure.

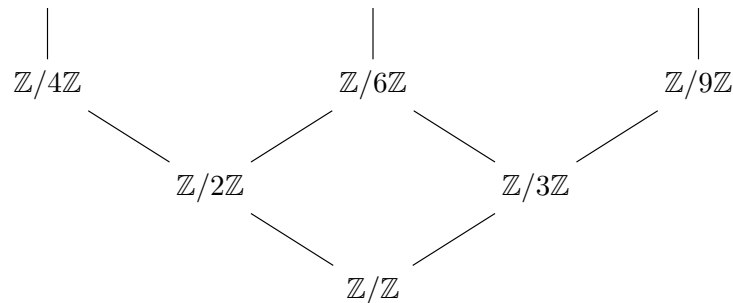
Suppose L/K is an infinite Galois extension. What does the Galois group look like? Any automorphism of L gives automorphisms of all finite extensions L_i/K . An element of $\text{Aut}(L/K)$ is a set of elements of $\text{Aut}(L_i/K)$ that are compatible. So $\text{Gal}(L/K)$ is the inverse limit of the groups $\text{Gal}(L_i/K)$.

¹Professor Borchers never remembers the proof, so see Lang.

Example 1.2. Let $K = F_p$, and let $L = \bar{F}_p$. $L = \bigcup_{p \geq 1} F_{p^k}$. We have the following picture:



So the groups will look like this:



So $\text{Gal}(\bar{F}/F) = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})$. This is called the *profinite completion* of \mathbb{Z} .

Definition 1.3. A *profinite group* is an inverse limit of finite groups

Definition 1.4. The *profinite completion* of G is

$$\varprojlim_{\substack{G_i \text{ normal} \\ G/G_i \text{ finite}}} G/G_i.$$

This is a subset of $\prod G/G_i$, with the discrete topology. There is a universal map from G to a profinite group. The image of G is dense in the *Krull topology*², so $\varprojlim G/G_i$ is a sort of completion of G .

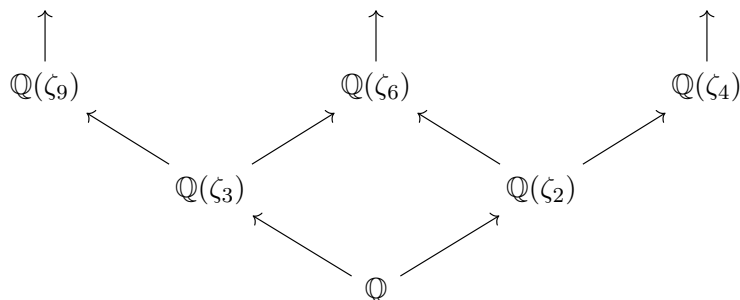
Example 1.3. Recall that $\mathbb{Z}/n\mathbb{Z} \cong \prod \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, where $n = \prod p_i^{k_i}$ (by the Chinese remainder theorem). Then $\varprojlim \mathbb{Z}/n\mathbb{Z} = \prod \varprojlim_{k_i} \mathbb{Z}/p_i^{k_i}\mathbb{Z} = \prod_p \mathbb{Z}_p$, the p -adic integers.

²Professor Borchers expressed his displeasure with the fact that there is a Marvel villain named Krull.

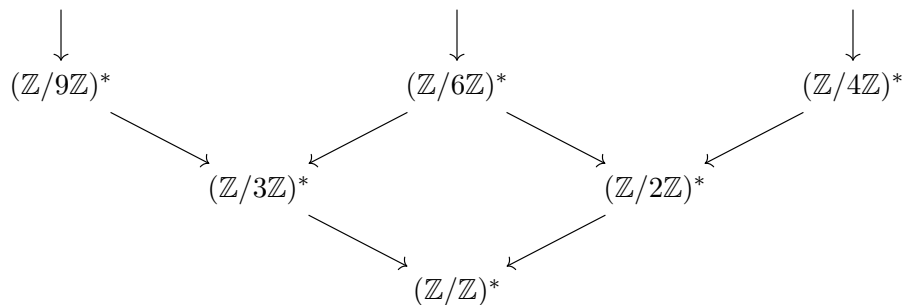
For finite extensions, we get a 1 to 1 correspondence between extensions of K in L and subgroups of $\text{Gal}(L/K)$. Is the same true for infinite extensions? No. Suppose $\alpha \in L$. Look at $K(\alpha)/L$. The set of things in the Galois group fixing α is closed in the Krull topology; this is the set of things fixing α in M/K , where M is the normal closure of α . A subgroup fixing any element $\alpha \in L$ is always closed in the Krull topology. So a subgroup fixing all elements of an extension M is an intersection of closed subgroups and is hence closed.

Instead, we get a 1 to 1 correspondence between extensions of K in L and closed subgroups of $\text{Gal}(L/K)$. We leave this as an exercise. The proof relies on the theorem for finite Galois extensions and some bookkeeping.

Example 1.4. Let $K = \mathbb{Q}$, and let L be the cyclotomic extension of \mathbb{Q} (\mathbb{Q} (all roots of unity)). $L = \bigcup \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n -th root of unity. we get the picture



We know that $\text{Gal} \mathbb{Q}[\zeta_n]/\mathbb{Q} = (\mathbb{Z}/n\mathbb{Z})^*$. So $\text{Gal}(\mathbb{Q}_{\text{cycl}}/\mathbb{Q})$ is given by the inverse limit of



As before, $(\mathbb{Z}/n\mathbb{Z})^* = \prod (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$. So $\varprojlim (\mathbb{Z}/n\mathbb{Z})^* = \prod_p (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^* = \prod_p \mathbb{Z}_p^*$. This is equal to $\bar{\mathbb{Z}}^*$, where $\bar{\mathbb{Z}}$ is the profinite completion of the ring \mathbb{Z} . Nicely enough, it is abelian.

Example 1.5. Let $K = \mathbb{Q}$ and $L = \bar{\mathbb{Q}}$, the algebraic closure of \mathbb{Q} . Let $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. G is not known. The abelianization of G is known. This is $\varprojlim (\mathbb{Z}/n\mathbb{Z})^* = \text{Gal}(\mathbb{Q}_{\text{cycl}}/\mathbb{Q})$. We have the exact sequence

$$0 \rightarrow \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_{\text{cycl}}) \rightarrow \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}_{\text{cycl}}/\mathbb{Q}) \rightarrow 0.$$

What is $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_{\text{cycl}})$? This is unknown. There is a conjecture of Shafarevich that this is isomorphic to the profinite completion of a countable free group. $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is related to the Langlands program and “automorphic forms.”³ Part of Andrew Wiles’ proof of Fermat’s last theorem is about understanding some of the structure of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

1.3 Abelian Kummer theory

We want to find abelian extensions of K , given that K has enough roots of unity. Let \bar{K} be the separable algebraic closure of K , the largest separable extension in the algebraic closure. Look at

$$1 \rightarrow \mu_n \rightarrow \bar{K}^* \rightarrow \bar{K}^* \rightarrow 1,$$

where μ_n is the n -th roots of unity in K . This is an exact sequence of groups acted on by $\text{Gal}(\bar{K}/K)$. Take the invariants under $\text{Gal}(\bar{K}/K)$.

$$1 \rightarrow \mu_n \rightarrow K^* \xrightarrow{x \mapsto x^n} K^* \rightarrow H^1(G, \mu_n) \rightarrow \underbrace{H^1(G, \bar{K}^*)}_{=1} \rightarrow \underbrace{H^1(G, \bar{K})}_{=1} \rightarrow \dots$$

where these last two are 1 by Hilbert’s theorem 90. The definition of the first homomology is the same as for when G is finite, except cocycles must be continuous.

So we get

$$K^* \xrightarrow{x \mapsto x^n} K^* \rightarrow \text{Hom}(G, \mu_n) \rightarrow 1,$$

and $\text{Hom}(G, \mu_n) = H^*/(K^*)^n$, which is cyclic of order n . The kernels of homomorphisms in this group are isomorphic to subgroups H of G with G/H cyclic and of order dividing n . This is isomorphic to extensions L of K with $\text{Gal}(L/K)$ cyclic and of order n . This is the same as our previous description: cyclic extensions of the form $K(\sqrt[n]{*})$.

1.4 Artin-Schrier extensions

Let L/K be cyclic of order p , where p is the characteristic of K . Then $L = K(\alpha)$, where α is a root of $x^p - x - b = 0$ for $b \in K$. Rewrite this in terms of infinite extensions and Galois cohomology. Let \bar{K} be the separable closure of K . Use

$$0 \rightarrow F_p \rightarrow \bar{K} \xrightarrow{x \mapsto x^p - x} \bar{K} \rightarrow 0,$$

the exact sequence of modules acted on by $\text{Gal}(\bar{K}/K)$. Take the invariants

$$0 \rightarrow F_p \rightarrow K \xrightarrow{x \mapsto x^p - x} K \rightarrow \underbrace{H^1(G, F_p)}_{=\text{Hom}(G, F_p)} \rightarrow \underbrace{H^1(G, \bar{K})}_{=0} \rightarrow \underbrace{H^1(G, \bar{K})}_{=0} \rightarrow \dots$$

³Professor Borchers says that to understand what automorphic forms are, it takes a semester, and to understand what “related to” means, it takes a lifetime of study.

$H^i(G, \bar{K}) = 0$ for $i > 0$ by the normal basis theorem.

So $\text{Hom}(G, F_p) = K/\text{im}(x^p - x)$ correspond to normal subgroups of index p in $\text{Gal}(\bar{K}/K)$. which correspond to cyclic extensions of degree p .

What about extensions L/K with group $\mathbb{Z}/p^n\mathbb{Z}$ and $n > 1$? The answer is to use *Witt vectors*; see the exercises in Lang. We get

$$0 \rightarrow \mathbb{Z}/p^n\mathbb{Z} \rightarrow W \rightarrow W \rightarrow 0,$$

where W is the ring of Witt vectors.