Notes on Galois Cohomology—Modularity seminar

Rebecca Bellovin

1 Introduction

We've seen that the tangent space to a deformation functor is a Galois cohomology group H^1, and we'll see that obstructions to a deformation problem will be in H^2. So if we want to know things like the dimension of R or whether a deformation functor is smooth, we need to be able to get our hands on the cohomology groups. Secondarily, if we want to "deform subject to conditions", we'll want to express the tangent space and obstruction space of those functors as cohomology groups, and cohomology groups we can compute in terms of an unrestricted deformation problem.

For the most part, we will assume the contents of Serre's *Local Fields* and *Galois Cohomology*. These cover the cases when G is finite (and discrete) and M is discrete, and G is profinite and M is discrete, respectively.

References:
Serre's *Galois Cohomology*
Neukirch's *Cohomology of Number Fields*
Appendix B of Rubin's *Euler Systems*
Washington's article in CSS
Darmon, Diamond, and Taylor (preprint on Darmon's website)

2 Generalities

Let G be a group, and let M be a module with an action by G. Both G and M have topologies; often both will be discrete (and G will be finite),

or G will be profinite with M discrete; or both will be profinite. We always require the action of G on M to be continuous.

Let's review group cohomology, using inhomogenous cocycles.

For a topological group G and a topological G-module M, the ith group of continuous cochains $C^i(G, M)$ is the group of continuous maps $G^i \to M$. There is a differential $d : C^i(G, M) \to C^{i+1}(G, M)$ given by

$$\begin{aligned}(df)(g_1, \ldots, g_{i+1}) = \; & g_1 \cdot f(g_2, \ldots, g_{i+1}) \\ & + \sum_{j=1}^{n} (-1)^j f(g_1, \ldots, g_j g_{j+1}, \ldots, g_{i+1}) \\ & + (-1)^{i+1} f(g_1, \ldots, g_i)\end{aligned}$$

It is easy to check that d^2 is zero, so we have a complex $C^\bullet(G, M)$. Then we define $H^i(G, M) := \ker d / \operatorname{im} d$.

If G is finite and M is discrete, this is just ordinary group cohomology, see for example [3]. But for G or M profinite, taking the algebraic group cohomology gives the "wrong" answer. For example, if L/K is a finite Galois extension of fields and M is a module equipped with a trivial action of $G := \mathrm{Gal}(L/K)$, then the algebraic cohomology group $H^1(G, M) = \mathrm{Hom}(G, M)$ classifies subextensions $K \subset K' \subset L$ with $\mathrm{Gal}(K'/K)$ isomorphic to a subgroup of M. It would be nice if we could relax the finiteness hypothesis on the extension L/K and still have H^1 meaningfully classify subextensions. But infinite Galois theory tells us that only *closed* subgroups of $\mathrm{Gal}(L/K)$ correspond to subextensions $K \subset K' \subset L$, so our definition of H^1 will have to take topological information into account somehow.

For an explicit example where algebraic and continuous group cohomology differ, see Brian's notes from Hawaii, exercise 2.5.2.

2.1 Functorial properties

As we have defined it, Galois cohomology is functorial in the coefficients, that is, given a morphism $M \to M'$ of G-modules, there is are morphisms $H^i(G, M) \to H^i(G, M')$. Suppose $0 \to M' \to M \to M'' \to 0$ is an exact sequence of topological modules, and there is continuous section $M'' \to M$ (as sets, not modules!). Then $0 \to C^i(G, M') \to C^i(G, M) \to C^i(G, M'') \to 0$ is

exact for every i, and by homological algebra nonsense, we get a long exact sequence

$$\cdots \to H^i(G, M') \to H^i(G, M) \to H^i(G, M'') \to H^{i+1}(G, M') \to \cdots$$

In all the cases we will care about, this hypothesis will be satisfied, because surjective maps of discrete topological spaces have continuous sections, and proposition 1, chapter 1 of *Galois Cohomology* tells us that continuous surjections of profinite groups have continuous sections. In particular, if M is a finitely-generated $\mathbb{Z}_p$-module or a finite-dimensional $\mathbb{Q}_p$-vector space, we will have a long exact sequence.

For finite groups G and discrete G-modules M, recall that for all subgroups $H \subset G$, we have a restriction map

$$\text{res} : H^i(G, M) \to H^i(H, M)$$

and a corestriction map

$$\text{cor} : H^i(H, M) \to H^i(G, M)$$

If H is normal in G, we also have an inflation map

$$\text{inf} : H^i(G/H, M^H) \to H^i(G, M)$$

For G profinite and M discrete, we still have a restriction map

$$\text{res} : H^i(G, M) \to H^i(H, M)$$

If H is a closed, normal subgroup of G (so that the quotient G/H makes sense), we also still have an inflation map

$$\text{inf} : H^i(G/H, M^H) \to H^i(G, M)$$

However, to define a corestriction map, we need to assume H is open in G with finite index. In that case, we define it "at finite level" (as discussed in section 2.2) using the definition from finite group cohomology, and take the limit.

When G is a finite group, or G is profinite and M is discrete, for any normal subgroup H there is a spectral sequence $H^p(G/H, H^q(H, M)) \to$

$H^{p+q}(G, M)$. This is because cohomology groups $H^q(G, M)$ are the derived functors (taken in the category of all G modules if G is finite, but taken in the category of discrete G-modules if G is profinite) of the functor $M \mapsto M^G$, and $M \mapsto M^G$ is the composition of $M \mapsto M^H$ and $M^G \mapsto (M^H)^{G/H}$. In particular, the low-degree terms of the spectral sequence give us the Hochschild-Serre exact sequence

$$0 \to H^1(G/H, M^H) \overset{\text{inf}}{\to} H^1(G, M) \overset{\text{res}}{\to} H^1(H, M)^{G/H} \to H^2(G/H, M^H) \overset{\text{inf}}{\to} H^2(G, M)$$

The first four terms are the usual inflation-restriction exact sequence.

Recall also that in finite group cohomology, there is a cup-product pairing $H^p(G, M) \times H^q(G, N) \overset{\cup}{\to} H^{p+q}(G, M \otimes N)$ given on the level of cochains by $(\varphi \cup \psi)(g_1, \ldots, g_p, g_{p+1}, \ldots, g_{p+q}) = \varphi(g_1, \ldots, g_p) \otimes g_1 \cdots g_p \psi(g_{p+1}, \ldots, g_{p+q})$. The same applies for profinite groups G and discrete G-modules. However, if we want to allow more interesting topologies on the coefficient modules, we may not be able to define the tensor product of modules. Instead, we use the same formula to say that whenever there are (continuous) maps of G-modules $M \to P, N \to P$, there is a cup-product $H^p(G, M) \times H^1(G, N) \overset{\cup}{\to} H^{p+q}(G, P)$.

2.2 Reducing to the Finite/Discrete Case

Now let's allow G to be profinite (still assuming M to be discrete).

Theorem 2.1. *Let (G_i) be a projective system of profinite groups, and let (M_i) be an inductive system of discrete G_i-modules (the maps are all compatible). If $G = \varprojlim G_i$ and $M = \varinjlim M_i$, then $H^q(G, M) = \varinjlim H^q(G_i, M_i)$.*

In particular,

Corollary 2.2. *For profinite G, $H^q(G, M) = \varinjlim H^q(G/U, M^U)$ for $q \geq 0$, where the limit is taken over all open normal subgroups of G.*

This corollary lets us reduce many statements to the equivalent statements at finite level. For example, classical group cohomology tells us that for a finite group G, $H^q(G, M)$ is torsion for $q \geq 1$, so for profinite G, $H^q(G, M)$ is the colimit of torsion groups, so is itself torsion.

It also lets us make definitions at finite level, and then take a direct limit. For example, in order to define corestriction for profinite groups, we recall the definition of the corestriction map $\mathrm{cor} : H^q(H/(H \cap U), M) \to H^q(G/U, M)$ for open normal subgroups $U \subset G$ of finite index. By applying the above corollary, we obtain a homomorphism $\mathrm{cor} : H^q(H, M) \to H^q(G, M)$.

Now let's relax the assumption that M is discrete. Then we have the following results due to Tate (see [4] or Appendix B of [1]):

Proposition 2.3. *For $T = \varprojlim T_n$, T_n finite, if $i > 0$ and $H^{i-1}(G, T_n)$ is finite for every n, then $H^i(G, T) = \varprojlim H^i(G, T_n)$.*

Proposition 2.4. *If T is a finitely generated $\mathbb{Z}_p$-module and $i \geq 0$, then $H^i(G, T)$ has no divisible elements, and $H^i(G, T) \otimes \mathbb{Q}_p \tilde{\to} H^i(G, T \otimes \mathbb{Q}_p)$.*

If we wanted, we could have first defined group cohomology for discrete G-modules, and then defined $H^i(G, T)$ by $\varprojlim H^i(G, T_n)$ and $H^i(G, T \otimes \mathbb{Q}_p)$ by $H^i(G, T) \otimes \mathbb{Q}_p$, instead of via continuous cochains. Then these propositions show we would end up with the same theory (at least for the coefficient modules we care about).

These propositions also give us generalizations of the inflation-restriction exact sequence and the five-term exact sequence associated to the Hochschild-Serre spectral sequence.

Proposition 2.5. *Suppose H is a closed normal subgroup of G.*

1. *There is an inflation-restriction exact sequence*

$$0 \to H^1(G/H, T^H) \to H^1(G, T) \to H^1(H, T)$$

2. *Suppose that p is a prime and for every G-module (resp. H-module) N of finite p-power order, $H^1(G, N)$ and $H^2(G, N)$ (resp. $H^1(H, N)$) is finite. If M is discrete or a finitely generated $\mathbb{Z}_p$-module or a finite-dimensional $\mathbb{Q}_p$-vector space, then there is a Hochschild-Serre exact sequence*

$$0 \to H^1(G/H, M^H) \to H^1(G, M) \to H^1(H, M)^{G/H} \to H^2(G/H, M^H) \to H^2(G, T)$$

2.3 New Phenomena

However, there are some genuinely new phenomena when our groups are profinite, even if our coefficients are still discrete. For example, there is the notion of cohomological dimension:

Definition 2.6. *Let p be a prime and G a profinite group. If for every discrete torsion G-module M and for every $q > n$, the p-primary component of $H^q(G, M)$ is zero, and n is the smallest integer with these properties, we say that n is the p-cohomological dimension of G and denote it by $\mathrm{cd}_p(G)$.*

Removing the requirement that the coefficients be torsion, we make the following definition:

Definition 2.7. *Let p be a prime and G a profinite group. If for every discrete G-module M and for every $q > n$, the p-primary component of $H^q(G, M)$ is zero, and n is the smallest integer with this property, we say that n is the strict p-cohomological dimension of G and denote it by $\mathrm{scd}_p(G)$.*

Of course, we could have infinite cohomological dimension or strict cohomological dimension.

Note that these are not interesting concepts when G is assumed finite! Recall that for any finite cyclic group G, $H^0_T(G, \mathbb{Z}) = \mathbb{Z}/\#G\mathbb{Z}$ and $H^r_T(G, \mathbb{Z}) \cong H^{r+2}_T(G, \mathbb{Z})$ for all $r \in \mathbb{Z}$.

Examples:

- Let $G = \hat{Z}$. Then for every p, $\mathrm{cd}_p(G) = 1$ (see [3, Ch. XIII, Prop. 2]). But $H^2(G, \mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$, so $\mathrm{scd}_p(G) = 2$.
- Let G_ℓ be the absolute Galois group of $\mathbb{Q}_\ell$. Then for all p, $\mathrm{cd}_p(G_\ell) = \mathrm{scd}_p(G_\ell) = 2$. This is a manifestation of the general fact that if k is the residue field of K, then $\mathrm{cd}_p(G_K) \leq 1 + \mathrm{cd}_p(G_k)$, with equality when $\mathrm{cd}_p(G_k) < \infty$ and p is different than the characteristic.

3 Local Duality

Now let's try to say something about group cohomology we care about as number theorists. Let K be a p-adic field, i.e., a finite extension of $\mathbb{Q}_p$ and let μ_n be the group of nth roots of unity in $\overline{K}$.

From now on, we will be considering Galois cohomology, that is, group cohomology where the groups in question are Galois groups. If K is a field, we will write $H^i(K, M)$ to mean $H^i(G_K, M)$, and if K'/K is a Galois extension of fields, we will write $H^i(K'/K, M)$ to mean $H^i(\mathrm{Gal}(K'/K), M)$.

Proposition 3.1.

- $H^0(K, \mu_n) = \mu_n \cap K$
- $H^1(K, \mu_n) = K^\times/(K^\times)^n$
- $H^2(K, \mu_n) = \mathbb{Z}/n\mathbb{Z}$
- $H^i(K, \mu_n) = 0$ *for* $i \geq 3$

Proof. The first assertion follows by definition. For the cases $i = 1$ and $i = 2$, use the exact sequence $0 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 0$ and look at the long exact sequence in cohomology:

$$\begin{aligned} 0 \;\to\; & H^0(K, \mu_n) \to H^0(K, \mathbb{G}_m) \xrightarrow{n} H^0(K, \mathbb{G}_m) \to \\ \to\; & H^1(K, \mu_n) \to H^1(K, \mathbb{G}_m) \xrightarrow{n} H^1(K, \mathbb{G}_m) \to \\ \to\; & H^2(K, \mu_n) \to H^2(K, \mathbb{G}_m) \xrightarrow{n} H^2(K, \mathbb{G}_m) \end{aligned}$$

By Hilbert's Satz 90, $H^1(K, \mathbb{G}_m) = 0$, which implies that $H^1(K, \mu_n) = K^\times/(K^\times)^n$. In addition, $H^2(K, \mathbb{G}_m) = \mathbb{Q}/\mathbb{Z}$, with the isomorphism given by the inv map, by the theory of Brauer groups. This implies $H^2(K, \mu_n) = \mathbb{Z}/n\mathbb{Z}$. For $i \geq 3$, the assertion is a theorem of Tate, and is proved in ([2, §4.3, Prop. 12]). □

In particular, this has the striking corollary

Corollary 3.2. *For M a finite G_K-module, $H^i(K, M)$ is finite as well.*

Proof. Over a finite extension K'/K, M becomes a $G_{K'}$-module isomorphic to a direct sum of μ_n's. We have a spectral sequence $H^i(\mathrm{Gal}(K'/K), H^j(K', M)) \Rightarrow H^{i+j}(K, M)$, so by the proposition, $H^{i+j}(K, M)$ is finite. □

Now we can state Tate's local duality theorem:

Theorem 3.3. *Let M be a finite G_K-module and set $M' = \mathrm{Hom}(M, \mu) = \mathrm{Hom}(M, \mathbb{G}_m)$. Then for $0 \leq i \leq 2$, the cup-product*

$$H^i(K, M) \times H^{2-i}(K, M') \to H^2(K, \mu) = \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing.

One of the consequences is the Euler-Poincaré characteristic. For a finite G_K-module M, we define the Euler-Poincaré characteristic to be

$$\chi(M) := \frac{\#H^0(K,M)\#H^2(K,M)}{\#H^1(K,M)}$$

Then one can show that $\chi(M) = p^{-v_p(\#M)\cdot N} = 1/(\mathcal{O} : \#M\mathcal{O})$, where $N = [K : \mathbb{Q}_p]$ and $\mathcal{O}$ is the ring of integers of K. In particular, if the order of A is relatively prime to p, then $\chi(A) = 1$.

We can extend the concept to the case where M is a finite free $\mathbb{Z}_\ell$-module or a finite-dimensional $\mathbb{Q}_\ell$-vector space by making the more familiar definition

$$\chi(M) := h^0(M) - h^1(M) + h^2(M)$$

where $h^i(M) := \operatorname{rk} H^i(K,M)$. If M is a free $\mathbb{Z}_\ell$-module of rank k, take $M_n = M/\ell^n M$, so that $\chi(M) = \varprojlim \frac{1}{n}\log_\ell \chi(M_n) = -kNv_p(\ell)$. In particular, if $\ell \neq p$, then $\chi(M) = 0$.

Here are some interesting special cases:

- Take $M = \mathbb{Z}/n\mathbb{Z}$ and $i = 1$. Then this theorem says we have a perfect pairing $H^1(K, \mathbb{Z}/n\mathbb{Z}) \times H^1(K, \mu_n) \to \mathbb{Q}/\mathbb{Z}$, which in particular says that $\operatorname{Hom}(G_K, \mathbb{Z}/n\mathbb{Z})$ is dual to $K^\times/(K^\times)^n$. This is the duality given by local class field theory, and if K contains the nth roots of unity, Tate duality becomes the Hilbert symbol $K^\times/(K^\times)^n \times K^\times/(K^\times)^n \to \mathbb{Q}/\mathbb{Z}$.
- If E is an elliptic curve (or A is an abelian variety) over K, there is an action of G_K on the torsion $E(\overline{K})[m]$, so we have the perfect pairing

  $$H^1(K, E(\overline{K})[m]) \times H^1(K, E(\overline{K})[m]') \to \mathbb{Q}/\mathbb{Z}$$

  But the Weil pairing tells us that $E(\overline{K})[m]$ is dual to $\hat{E}(\overline{K})[m]$, which for elliptic curves implies we have a pairing

  $$H^1(K, E(\overline{K})[m]) \times H^1(K, E(\overline{K})[m]) \to \mathbb{Q}/\mathbb{Z}$$

3.1 Unramified Cohomology

We're going to be interested in a subgroup of H^1 called the unramified cohomology. We define

$$H^i_{nr}(K,M) := H^i(K^{nr}/K, M^I)$$

to be the cohomology classes vanishing on inertia. For example,

- $H^0_{nr}(K,M) = H^0(K,M)$
- $H^1_{nr}(K,M) = \ker(H^1(K,M) \to H^1(K^{nr},M))$—this is by inflation-restriction. If M is finite, the order of $H^1_{nr}(K,M)$ is the same as the order of $H^0(K,M)$, because there is an exact sequence

  $$0 \to M^{G_K} \to M^I \stackrel{\mathrm{Frob}-\mathrm{id}}{\to} M^I/(\mathrm{Frob}-\mathrm{id})M^I \to 0$$

  The lefthand term is $H^0(K,M)$ and the righthand term is $H^1_{nr}(K,M)$.
- $H^i_{nr}(K,M) = 0$ for $i \geq 2$ because $\mathrm{Gal}(K^{nr}/K) = \hat{\mathbb{Z}}$ has cohomological dimension 1.

Why do we care? For one thing, suppose ρ is an unramified representation and $c \in H^1_{nr}(K,M)$, and consider the corresponding deformation ρ'. Then ρ' restricted to I is the trivial deformation, so ρ' is still unramified.

Going back to elliptic curves, let's briefly make K a global field with E an elliptic curve (or abelian variety) defined over it. Define the finite set of places S to be the union of the archimedean places, the places where E has bad reduction, and the places v where $v(m) \neq 0$, and define K_S to the be the maximal extension of K unramified outside of S. Then $E[m]$ is a G_K-module, so we have the exact sequence

$$0 \to E(\overline{K})[m] \to E(\overline{K}) \stackrel{m}{\to} E(\overline{K}) \to 0$$

The long exact sequence in cohomology gives us

$$0 \to E(K)[m] \to E(K) \stackrel{m}{\to} E(K) \to H^1(G_K, E(\overline{K})[m])$$

so

$$0 \to E(K)/mE(K) \to H^1(G_K, E(\overline{K})[m])$$

We are interested in $E(K)/mE(K)$ because of its role in the proof of the Mordell-Weil theorem. In fact, its image in $H^1(K_S, E(\overline{K})[m])$ is exactly the subgroup of cohomology classes unramified outside S.

Going back to the general theory, let's look at what happens in the Tate pairing. I claim that if $\#M$ is relatively prime to p, then $H^1_{nr}(K,M)$ and

$H^1_{nr}(K, M')$ exactly annhilate each other. To see this, note that the inclusion $H^1_{nr}(K, M) \hookrightarrow H^1(K, M)$ is compatible with cup-product, so the cup-product map

$$H^1_{nr}(K, M) \times H^1_{nr}(K, M') \to H^2(K, \overline{K}^\times)$$

factors through $H^2_{ur}(K, \overline{K}^\times)$, which is zero. So we only need to check that the orders of $H^1_{nr}(K, M)$ and $H^1_{nr}(K, M')$ match up, i.e., that $\#H^1(K, M)/\#H^1_{nr}(K, M) = \#H^1_{nr}(K, M')$. By the argument above, $H^1_{nr}(K, M)$ has the same number of elements as $H^0(K, M)$, and $H^1_{nr}(K, M')$ has the same number of elements as $H^0(K, M')$, which is identified with $H^2(K, M)$ by Tate duality. Since $\#M$ is relatively prime to p, the Euler characteristic of M is 1, which implies the desired equality.

4 Global Euler Characteristic and Poitou-Tate Long Exact Sequence

4.1 Local Conditions

We are going to care about deformation problems more restricted than "all deformations to A", and we'll want to identify tangent spaces of restricted problems with cohomology groups, ideally subgroups of the cohomological tangent spaces we already know about. For example, if we ask for deformations preserving the determinant, we find that the tangent space is $H^1(G, \mathrm{ad}^0 \rho)$: let $C : G \to \mathrm{ad}\,\rho$ be the cocycle representing an infinitesimal deformation, i.e., the deformation is $\rho'(g) = (I + \varepsilon C(g))\rho(g)$. Then $\det(\rho') = (1 + \varepsilon \operatorname{Tr}(C)) \det \rho$, so keeping the determinant unchanged is equivalent to $\operatorname{Tr}(C) = 0$, that is, C is actually a cocycle valued in $\mathrm{ad}^0 \rho$.

Since we're interested in deformations of global Galois groups, we're also going to be interested in deformations satisfying local conditions. That is, if v is a place of F, there is a homomorphism $G_v \hookrightarrow G$, so by contravariance, we have a restriction map $H^i(G, M) \to H^i(G_v, M)$. This lets us try to understand global cohomology classes in terms of their restrictions to the local Galois groups. For example, we could look at the subgroup of everywhere uramified cohomology classes:

$$\{c \in H^i(G, M) \mid \mathrm{res}_v(c) \text{ is unramified}\}$$

We make the following definition:

Definition 4.1. *Let $\mathcal{L} = (L_v)$ be a collection of subgroups $L_v \subset H^1(G_v, M)$ such that for almost all places v, $L_v = H^1_{nr}(G_v, M)$ (this is called a family of local conditions). The generalized Selmer group is*

$$H^1_{\mathcal{L}}(G_F, M) := \{c \in H^1(G_F, M) \mid \mathrm{res}_v(c) \in L_v \forall v\}$$

We also let $\mathcal{L}^D$ (the dual) denote the family of local conditions (L_v^D), where L_v^D is the annhilator of L_v under the Tate local duality pairing.

Here's an example of a family of local conditions: Fix a finite set $S \supset S_\infty$ of places of a global field F, and let $\rho : G_F \to \mathrm{GL}_n(R)$ be a representation of the absolute Galois group of F. Then we set

- $L_\ell = H^1_{nr}(G_\ell, \mathrm{ad}^0\,\rho)$ if $\ell \notin S$, $\ell \neq p$
- $L_\ell = H^1(G_\ell, \mathrm{ad}^0\,\rho)$ if $\ell \in S$
- L_p the conditions for ordinary deformations

4.2 Global Euler-Poincaré characteristic and Poitou-Tate

The Poitou-Tate nine-term exact sequence is the following: Let F be a number field, and let S be any set of places containing the archimedean places and the places v with $v(\#M) \neq 0$,

$$\begin{aligned} 0 \;&\to\; H^0(F_S, M) \to P^0(F_S, M) \to H^2(F_S, A')^\vee \\ &\to\; H^1(F_S, M) \to P^1(F_S, M) \to H^1(F_S, A')^\vee \\ &\to\; H^2(F_S, M) \to P^2(F_S, M) \to H^0(F_S, A')^\vee \end{aligned}$$

This bears some explanation, since we haven't defined the groups P^i, or the maps in the sequence. Let A be a finite G_F-module. We define

$$P^i(F_S, M) := \prod_{v \in S}{}' H^i(F_v, M)$$

Here the restricted product is taken with respect to the unramified cohomology classes, that is,

$$P^i(F_S, M) = \{(c_v)_{v\in S} \in \prod_{v\in S} H^i(F_v, M) \mid c_v \in H^i_{nr}(F_v, M) \text{ for almost all } v \in S\}$$

Moreover, for archimedean places $v \in S$, we replace H^0 by the modified Tate cohomology group $\hat{H}^0$. In particular,

$$\begin{aligned} P^0(F_S, M) &= \prod_{v\in S\smallsetminus S_\infty} H^0(F_v, M) \times \prod_{v\in S_\infty} \hat{H}^0(F_v, M) \\ P^1(F_S, M) &= \prod_{v\in S}{}' H^1(F_v, M) \\ P^2(F_S, M) &= \bigoplus_{v\in S} H^2(F_v, M) \end{aligned}$$

(by passing to a finite extension where A is unramified).

These groups have topologies: in order, excluding the zero terms, they are finite discrete, compact, compact, discrete, locally compact, compact, discrete, discrete, finite.

Now we want to say what the maps are. The maps $H^i \to P^i$ are evident. For the maps $P^i \to H^{2-i}$, note that local duality gives an isomorphism $P^i \xrightarrow{\sim} (P^{2-i})^\vee$ for $0 \le i \le 2$; composing with the (Pontryagin) dual of the homomorphism $H^{2-i} \to P^{2-i}$ gives the desired map. That leaves the maps $(H^2)^\vee \to H^1$ and $(H^1)^\vee \to H^2$. Denoting the maps $H^i \to P^i$ by α_i, there is a non-degenerate pairing $\ker\alpha_1 \times \ker\alpha_2 \to \mathbb{Q}/\mathbb{Z}$, which defines the desired maps.

A theorem due to Poitou and Tate (independently) states that this sequence is exact, and all of the maps are continuous.

Now we would like an analogue of the local Euler-Poincaré characteristic, for global Galois cohomology. We need to assume that S is a finite set, containing S_∞ and the places v with $v(\#M) \neq 0$. First of all, we show that if M is a finite G_S-module, then $H^1(F_S, M)$ is finite. It is also true that $H^i(F_S, A)$ is finite for $i \neq 1$, but this is harder (this is Theorem 8.3.19 in Neukirch)

Proof. We can pass to a finite Galois extension F'/F such that $G_{F',S}$ acts trivially on M. Then $H^1(G_{F',S}, M)$ is finite, because it's equal to $\mathrm{Hom}(F'^\times_S, M)$,

which classifies Galois extensions of F' unramified outside S with Galois group a subgroup of M, and there are finitely many of these (Hermite-Minkowski). Then use the spectral sequence or inflation-restriction to say that $H^1(F_S, M)$ itself is finite. $\square$

Now we define the global Euler-Poincaré characteristic to be

$$\chi(F_S, M) := \frac{\#H^0(F_S, M)\#H^2(F_S, M)}{\#H^1(F_S, M)}$$

We have the formula

$$\chi(F_S, M) = \prod_{v \in S_\infty} \frac{\#H^0(F_v, M)}{\|\#M\|} = \prod_{v \in S_\infty} \frac{\#\hat{H}^0(F_v, M)}{\#H^0(F_v, M')} \tag{4.1}$$

Note that this formula is in terms of the cardinality of the cohomology groups. In this seminar, we will be interested in the case where the cohomology coefficients are vector spaces (either over finite fields or over p-adic fields), so we would like a formula in terms of the dimensions of cohomology groups as vector spaces.

So suppose that M is a finite dimensional vector space over a finite field $k = \mathbb{F}_q$. Then the cohomology groups $H^i(G_S, M)$ are vector spaces over k, so we may take the base q logarithm of 4.1 to get

$$\log_q \chi(F_S, M) = \sum_{v \in S_\infty} \left(h^0(F_v, M) - \log_q \|\#M\|\right) = \sum_{v \in S_\infty} \left(\hat{h}^0(F_v, M) - h^0(F_v, M')\right)$$

5 Product formula

The formula we want to prove is due to Wiles: Let M be a finite G_F-module and let $\mathcal{L}$ be a collection of local conditions. Then

$$\frac{\#H^1_{\mathcal{L}}(F, M)}{H^1_{\mathcal{L}^D}(F, M')} = \frac{\#H^0(F, M)}{\#H^0(F, M')} \cdot \prod_v \frac{\#\mathcal{L}_v}{\#H^0(F_v, M)}$$

where the product runs over all places of F.

We choose a finite set S of places of F as follows: S contains all archimedean places of F, all non-archimedean places whose residue characteristic divides

$\#M$, all places where M is ramified, and all places $\mathfrak{p}$ where $L_\mathfrak{p} \neq \#H^1(G_\mathfrak{p}/I_\mathfrak{p}, M^{I_\mathfrak{p}})$. Let F_S be the maximal extension of F unramified outside S, and let G_S be $\mathrm{Gal}(F_S/F)$.

For any finite discrete G_F-module M, we have an exact sequence

$$0 \to H^1_{\mathcal{L}}(F, M) \to H^1(G_S, M) \to \oplus_{v \in S} H^1(G_v, M)/L_v$$

Taking this exact sequence for M^* and hitting it with $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$, we get

$$\prod_{v \in S} L_v \to H^1(G_S, M^*)^\vee \to H^1_{\mathcal{L}^D}(F, M^*)^\vee \to 0$$

Here the $\vee$ refers to Pontryagin dual. The identity $(H^1(G_v, M^*)/L_v^D)^\vee = L_v$ follows from local duality: $\mathrm{Hom}(H^1(G_v, M^*)/L_v^D, \mathbb{Q}/\mathbb{Z})$ is the subset of $H^1(G_v, M)$ killing L_v^D under the Tate pairing, which is to say that it is L_v again.

Next we want to merge this exact sequence into the Poitou-Tate exact sequence:

$$\begin{aligned} 0 \quad &\to \quad H^0(G_S, M) \to P^0(G_S, M) \to H^2(G_S, A')^\vee \to \\ &\to \quad H^1_{\mathcal{L}}(F, M) \to \prod_{v \in S} L_v \to H^1(G_S, M^*)^\vee \to H^1_{\mathcal{L}^D}(F, M^*)^\vee \to 0 \end{aligned}$$

If this sequence is exact, we have

$$\frac{\#H^1_{\mathcal{L}}(F, M)}{\#H^1_{\mathcal{L}^D}(F, M')} = \frac{\#H^0(G_S, M)\#H^2(G_S, M')}{\#H^1(G_S, M')\#P^0(G_S, M)} \cdot \prod_{v \in S} \#L_v$$

because $H^2(G_S, M')^\vee$ has the same number of elements as $H^2(G_S, M')$. The formula for $\chi(G_S, M')$ is $\chi(G_S, M') = \prod_{v \in S_\infty} \frac{\hat{h}^0(F_v, M')}{h^0(F_v, M)}$, which yields

$$\begin{aligned} \frac{\#H^1_{\mathcal{L}}(F, M)}{\#H^1_{\mathcal{L}^D}(F, M')} &= \frac{\#H^0(G_S, M)}{\#H^0(G_S, M')} \cdot \frac{1}{\#P^0(G_S, M)} \cdot \prod_{v \in S_\infty} \frac{\#\hat{H}^0(F_v, M')}{\#H^0(F_v, M)} \prod_{v \in S} \#L_v \\ &= \frac{\#H^0(G_S, M)}{\#H^0(G_S, M')} \prod_{v \in S} \frac{\#L_v}{\#H^0(F_v, M)} \text{ by the definition of } P^0 \\ &= \frac{\#H^0(G_S, M)}{\#H^0(G_S, M')} \prod_{v} \frac{\#L_v}{\#H^0(F_v, M)} \end{aligned}$$

The last line follows because outside of S, $L_v = H^1_{nr}(F_v, M)$ and M is unramified, so we can apply the argument that $\#H^1_{nr} = \#H^0$ to say the quotient is 1.

References

[1] Karl Rubin, *Euler Systems*, Princeton University Press, New York: 2000.

[2] J-P. Serre and P. Ion (trans.), *Galois Cohomology*, Springer-Verlag, New York: 1997.

[3] J-P. Serre and M.J. Ion (trans.), *Local Fields*, Springer-Verlag, New York: 1979.

[4] John Tate, "Relations between K_2 and Galois cohomology". *Invent. Math.*. 36 (1976), 257–274.