GALOIS COHOMOLOGY

Lawrence C. Washington

In these lectures, we give a very utilitarian description of the Galois cohomology needed in Wiles' proof. For a more general approach, see any of the references.

First we fix some notation. For a field K, let $\bar{K}$ be a separable closure of K and let G_K =Gal$(\bar{K}/K)$. For a prime p, let $G_p = G_{\mathbb{Q}_p}$, where $\mathbb{Q}_p$ is the field of p-adic numbers, and let $I_p \subset G_p$ be the inertia group.

Let G be a group, usually either finite or profinite, and let X be an abelian group on which G acts. Such an X will be called a G-module. If there are topologies to consider, we assume the action is continuous, though we shall mostly ignore continuity questions except to say that all maps, actions, etc. are continuous when they should be.

§1. H^0, H^1, and H^2.

We start with

$$H^0(G, X) = X^G = \{x \in X | gx = x \text{ for all } g \in G\}.$$

For example, G_K acts on $\bar{K}^\times$ and

$$H^0(G_K,\, \bar{K}^\times) = K^\times.$$

For another example, let μ_n denote the group of n-th roots of unity. Then

$$H^0(G_{\mathbb{Q}},\, \mu_n) = \{\pm 1\} \text{ if } 2|n, = 1 \text{ if } 2 \nmid n.$$

Occasionally, for a finite group G, we will need the modified Tate cohomology group

$$\hat{H}^0(G, X) = X^G/\text{Norm}(X),$$

where $\text{Norm}(x) = \sum_{g\in G} gx$ (if X is written additively). For example, if X is an abelian group of odd order on which Gal$(\mathbb{C}/\mathbb{R})$ acts, then $\text{Norm}(X) \supseteq 2(X^G) = X^G$, so $\hat{H}^0(\text{Gal}(\mathbb{C}/\mathbb{R}),\, X) = 0$.

We now skip $H^1(G, X)$ in order to give a brief description of $H^2(G, X)$. Define

$$H^2(G, X) = \text{ cocycles/coboundaries},$$

where a cocycle is a map (of sets) $f : G \times G \to X$ satisfying

$$\delta f = f(g_1, g_2g_3) - f(g_1g_2, g_3) + g_1 \cdot f(g_2, g_3) - f(g_1, g_2) = 0,$$

and where f is a coboundary if there is a map $h : G \to X$ such that

$$f(g_1, g_2) = g_1 \cdot h(g_2) - h(g_1g_2) + h(g_1) = \delta h.$$

This definition might seem a little strange; we will give a slightly different form of it later after we define $H^1(G, X)$.

Here is an example. Let p be an odd prime and let $G = G_p$. Let $a, b \in \mathbb{Q}_p^\times$ with a not a square. Define

$$\begin{aligned} f(g_1, g_2) =& b \text{ if } g_1\sqrt{a} = -\sqrt{a} \text{ and } g_2\sqrt{a} = -\sqrt{a} \\ =& 1 \text{ otherwise.} \end{aligned}$$

It is easy to check that $f : G_p \times G_p \to \mathbb{Q}_p^\times$ satisfies the cocycle condition, hence yields an element of $H^2(G_p,\, \mathbb{Q}_p^\times)$. Suppose b is a norm from $\mathbb{Q}_p(\sqrt{a})$, so $b = x^2 - ay^2$ for some $x, y \in \mathbb{Q}_p$. Let $h(g) = x + y\sqrt{a}$ if $g\sqrt{a} = -\sqrt{a}$ and $h(g) = 1$ otherwise. Then

$$f(g_1, g_2) = (g_1h(g_2))h(g_1)/h(g_1g_2),$$

so the element of H^2 we obtain is trivial. Conversely, it can be shown that if this element is trivial, then b is a norm from $\mathbb{Q}_p(\sqrt{a})$. Recall the Hilbert symbol $(a, b)_p$, which equals 1 if b is a norm from $\mathbb{Q}_p(\sqrt{a})$ and equals -1 otherwise. Thus the above cohomology class we obtain is essentially the same as the Hilbert symbol. We also have $(a, b)_p = 1$ if and only if $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 0$ has a non-zero solution in $\mathbb{Q}_p$. Equivalently, $(a, b)_p = 1$ if and only if the generalized quaternion algebra $\mathbb{Q}_p[i, j, k]$, with $i^2 = a$, $j^2 = b$, $k^2 = -ab$, $ij = k$, etc., is isomorphic to the algebra of two-by-two matrices over $\mathbb{Q}_p$ (rather than being a division algebra). In general, $H^2(G_K,\, \bar{K}^\times)$ is known as the Brauer group and classifies central simple algebras over the field K. We will need the following result.

Proposition 1. *Let p be a prime number. Then $H^2(G_p,\, \bar{\mathbb{Q}}_p^{\times}) \simeq \mathbb{Q}/\mathbb{Z}$.*

This result is an important result in local class field theory. For a proof, see [Se]. In our example, the cohomology class of f is 0 if $(a,b)_p = 1$ and is $\frac{1}{2}$ mod $\mathbb{Z}$ if $(a,b)_p = -1$.

We now turn our attention to H^1, which is the most important for us. Define

$$H^1(G,X) = \text{ cocycles/coboundaries},$$

where a cocycle is a map $f : G \to X$ satisfying $f(g_1 g_2) = f(g_1) + g_1 f(g_2)$ (a "crossed homomorphism") and where f is a coboundary if there exists $x \in X$ such that $f(g) = gx - x$.

Before continuing, we write the cocycle conditions in a different form that perhaps seems more natural. For a 2-cocycle f, let $F(a,b,c) = a \cdot f(a^{-1}b, a^{-1}c)$, where $a,b,c \in G$. Then $F(ga,gb,gc) = g \cdot F(a,b,c)$ and the cocycle condition becomes

$$F(a,b,c) - F(a,b,d) + F(a,c,d) - F(b,c,d) = 0.$$

For a 1-cocycle f, let $F(a,b) = a \cdot f(a^{-1}b)$. Then $F(ga,gb) = g \cdot F(a,b)$ and the cocycle condition reads

$$F(a,b) - F(a,c) + F(b,c) = 0.$$

We can even describe H^0 in this manner: a 0-cocycle is a map f from the one point set to X, hence simply an element x of X, that satisfies $gx - x = 0$. If we let $F(a) = ax$, then $F(ga) = g \cdot F(a)$ and $F(a) - F(b) = 0$ for all $a, b \in G$. In all three cases, the coboundary condition says that F is the coboundary of a function from the next lower dimension. For example, the function F for a 2-coboundary is of the form $H(a,b) - H(a,c) + H(b,c)$ for a function H satisfying $H(ga,gb) = g \cdot H(a,b)$ (explicitly, $H(a,b) = a \cdot h(a^{-1}b)$ in the above notation). It should now be clear how to define higher cohomology groups $H^n(G,X)$ for $n \geq 3$. With one exception, we will not need these higher groups, and in this one exception, the element we need will be 0; therefore, we may safely ignore them for the present exposition.

A fundamental fact that will be used quite often is the following. Suppose

$$0 \to A \to B \to C \to 0$$

is a short exact sequence of G-modules. Then there is a long exact sequence of cohomology groups (write $H^r(X)$ for $H^r(G,X)$)

$$0 \to H^0(A) \to H^0(B) \to H^0(C) \to H^1(A) \to H^1(B) \to H^1(C) \to H^2(A) \to \cdots .$$

The proof is a standard exercise in homological algebra.

Let's return to $H^1(G,X)$. Suppose the action of G is trivial, so $gx = x$ for all g and x. Then cocycles are simply homomorphisms $G \to X$. A coboundary $f(g) = gx - x$ is the 0-map. Therefore we have proved the useful fact that

$$H^1(G,X) = \text{ Hom}(G,X) \text{ if the action of } G \text{ is trivial.}$$

Here "Hom" means (continuous) homomorphisms of groups. For example, let K be a field and let $G = G_K$. Then G_K acts trivially on $\mathbb{Z}/2\mathbb{Z}$, so $H^1(G_K, \mathbb{Z}/2\mathbb{Z}) = \text{Hom}(G_K, \mathbb{Z}/2\mathbb{Z})$, which corresponds to the separable quadratic (or trivial) extensions of K; namely, if f is a non-trivial homomorphism, then the fixed field of the kernel of f is a quadratic extension. The trivial homomorphism corresponds to the trivial extension K/K.

Suppose now that G is a finite cyclic group: $G =< g >$ with $g^n = 1$. The cocycle relation yields by induction that

$$f(g^i) = (1 + g + g^2 + \cdots + g^{i-1}) f(g).$$

Therefore $f(1) = f(g^n) =$Norm$(f(g))$. The cocycle condition easily implies that $f(1) = 0$, so $f(g)$ is in the kernel of Norm. Any such choice for $f(g)$ yields a cocycle via the above formula. A coboundary corresponds to $f(g) = (g-1)x$ for some $x \in X$. Therefore

$$H^1(G,X) \simeq \text{ (Kernel of Norm)}/(g-1)X \qquad \text{for a finite cyclic group } G.$$

As an example, consider a $G_{\mathbb{R}}$-module X of odd order. Let c be complex conjugation. Write $X = \frac{1+c}{2} X \oplus \frac{1-c}{2} X$. Note that $\frac{1-c}{2} X$ is the kernel of Norm $= 1 + c$, and is also equal to $(c-1)X$. Therefore $H^1(G_{\mathbb{R}}, X) = 0$. More generally, it can be shown that if G and X are finite with relatively prime orders, then $H^i(G,X)=0$ for all $i>0$, and also for $i=0$ if we use the modified groups $\hat{H}^0(G,X)$.

When G is infinite cyclic, or is the profinite completion of an infinite cyclic group, and X is finite, then there is a similar description. Let g be a (topological) generator. Let $x\in X$ be arbitrary. There are $k,n>0$ such that $g^n x=x$ and $kx=0$. Define a cocycle by $f(g^i)=(1+g+\cdots+g^{i-1})x$ for $i>0$. If $i>j$ and $i\equiv j \mod kn$, then $g^j+\cdots g^{i-1}$ is a multiple of $1+g^n+\cdots+g^{n(k-1)}$, which kills x. Therefore $f(g^i)$ depends only on $i \mod kn$, so f extends to a continuous cocycle on all of G. Since, as above, every cocycle must be of this form, we have

$$H^1(G,X)\simeq X/(g-1)X \text{ when } G \text{ is (the profinite closure of) an infinite cyclic group and } X \text{ is finite.}$$

This result will be applied later to the case where $\mathbb{F}$ is a finite field and $G=$Gal$(\bar{\mathbb{F}}/\mathbb{F})$, which is generated by the Frobenius map.

Let L/K be a finite extension of fields with cyclic Galois group G generated by g. Then G acts on $L^\times$. The famous Hilbert Theorem 90 says that if $x\in L^\times$ has Norm 1 then $x=gy/y$ for some $y\in L^\times$. This is precisely the statement that $H^1(G,L^\times)=0$. More generally, we have

$$H^1(\mathrm{Gal}(L/K),\, L^\times)=0$$

for any Galois extension of fields L/K ([Se]).

Let $n\geq 1$ be prime to the characteristic of the field K and consider the exact sequence of G_K-modules

$$1\to\mu_n\to\bar{K}^\times\to\bar{K}^\times\to 1$$

induced by the n-th power map. The long exact sequence of cohomology groups includes the portion

$$H^0(G_K,\bar{K}^\times)\to H^0(G_K,\bar{K}^\times)\to H^1(G_K,\mu_n)\to H^1(G_K,\bar{K}^\times),$$

where the first map is the n-th power map. Since the last group is 0, we find that

$$H^1(G_K,\mu_n)\simeq K^\times/(K^\times)^n.$$

Explicitly, let $a\in K^\times$ and fix an nth root α of a. Then $g\mapsto g\alpha/\alpha$ defines a cocycle and hence an element of $H^1(G_K,\mu_n)$. When $\mu_n\subseteq K$, $H^1(G_K,\mu_n)$ becomes $\mathrm{Hom}(G_K,\mu_n)$, which corresponds (in an obvious many to one fashion) to cyclic extensions of K of degree dividing n, and α is a Kummer generator for this extension (and, correspondingly, there are several Kummer generators mod nth powers for each extension). When $n=2$, note that $\mathbb{Z}/2\mathbb{Z}$ and μ_2 are isomorphic as G_K-modules, and we find that $H^1(G_K,\mu_2)$ classifies quadratic extensions of K, though in a slightly different manner than $H^1(G_K,\mathbb{Z}/2\mathbb{Z})$.

§2. Preliminary results.

Suppose H is a (closed) normal subgroup of a group G and X is a G-module. Then X^H is a module for G/H in the obvious way. A cocycle for G/H can also be regarded as a cocycle for G ("inflation") by composing with the map $G\to G/H$. A cocycle for G can be regarded as a cocycle for H by restriction. Also, G/H acts on $H^1(H,X)$ by the formula $f^g(h)=g\cdot f(g^{-1}hg)$, where f is a cocycle and g is a representative of a coset in G/H. An easy calculation shows that if g' is another representative of the coset of g then $f^{g'}$ and f^g differ by a coboundary, so the action is well-defined.

Proposition 2 (Inflation-Restriction). *There is an exact sequence*

$$0\to H^1(G/H,X^H)\to H^1(G,X)\to H^1(H,X)^{G/H}\to H^2(G/H,X^H)\to H^2(G,X).$$

This is the exact sequence of terms of low degree in the Hochschild-Serre spectral sequence, hence is sometimes referred to by that name. For a proof, and the definition of the map from H^1 to H^2, see [Sh].

For example, let p be a prime and let $G=G_p$. Let $H=I_p=\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{unr}})$, where $\mathbb{Q}_p^{\mathrm{unr}}$ is the maximal unramified extension of $\mathbb{Q}_p$, so I_p is the inertia subgroup of G_p, and $G_p/I_p\simeq$ Gal$(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. The beginning of the above sequence implies that

$$H^1(G_p/I_p,X^{I_p})\simeq \mathrm{Ker}\Big(H^1(G_p,X)\to H^1(I_p,X)\Big).$$

In other words, we can regard $H^1(G_p/I_p,X^{I_p})$ as the subgroup of $H^1(G_p,X)$ consisting of those cohomology classes that become trivial when restricted to the inertia subgroup; hence, we call these the unramified classes. For example, when $X=\mathbb{Z}/2\mathbb{Z}$, the unramified classes are those homomorphisms from G_p to $\mathbb{Z}/2\mathbb{Z}$ that are 0 on I_p, hence that can be identified with homomorphisms from G_p/I_p to $\mathbb{Z}/2\mathbb{Z}$. There are two such homomorphisms, the 0 homomorphism and the one corresponding to the unique unramified quadratic extension of $\mathbb{Q}_p$ (or of $\mathbb{F}_p$). This is well-known, but is also a consequence of the following, which often allows us to calculate the order of the group of unramified classes, since $H^0(G_p,X)=X^{G_p}$.

Lemma 1. *Let X be finite. Then $\#H^1(G_p/I_p, X^{I_p}) = \#H^0(G_p, X)$ (and both are finite).*

Proof. There is an exact sequence

$$0 \to X^{G_p} \to X^{I_p} \xrightarrow{(\text{Frob}-1)} X^{I_p} \to X^{I_p}/(\text{Frob}-1)X^{I_p} \to 0.$$

The exactness at the first X^{I_p} follows from the fact that if $x \in X^{I_p}$ and $(\text{Frob}-1)x = 0$, then x is fixed by both I_p and Frob, which (topologically) generate G_p. The first term gives $H^0(G_p, X)$ and the last term gives $H^1(G_p/I_p, X^{I_p})$. The result follows easily. □

The last preliminary topic that we need is cup products. In general, suppose X_1, X_2, and X_3 are G-modules, and there is a G-module homomorphism $\Phi : X_1 \otimes X_2 \to X_3$. The cup product is a map $H^i(G, X_1) \times H^j(G, X_2) \to H^{i+j}(G, X_3)$. We define the cup product only when $i+j = 2$, since this is the main case we need. Let $f_1 \in H^2(G, X_1)$, so we may regard f_1 as (being represented by) a map $f_1 : G \times G \to X_1$. Let $x_2 \in X_2^G = H^0(G, X_2)$. Then $f_3 = f_1 \cup x_2$ is the 2-cocycle satisfying $f_3(g_1, g_2) = \Phi(f_1(g_1, g_2) \otimes x_2)$. The cup product of H^0 and H^2 is defined similarly. Now let $\phi_k \in H^1(G, X_k)$ for $k = 1, 2$. Define

$$(\phi_1 \cup \phi_2)(g_1, g_2) = \Phi\big(\phi_1(g_1) \otimes g_1\, \phi_2(g_2)\big).$$

It is easy to see that this defines a 2-cocycle, hence an element of $H^2(G, X_3)$.

For example, let $a, b \in \mathbb{Q}_p^\times$. Let $\phi \in H^1(G_p, \mathbb{Z}/2\mathbb{Z})$ be defined by $\phi(g) = 0$ if $g(\sqrt{a}) = \sqrt{a}$ and $\phi(g) = 1$ otherwise. Define $\psi \in H^1(G_p, \mu_2)$ by $\psi(g) = g(\sqrt{b})/\sqrt{b}$. We may regard $\mu_2 \simeq \text{Hom}(\mathbb{Z}/2\mathbb{Z},\, \mu_2)$ as the dual of $\mathbb{Z}/2\mathbb{Z}$; hence there is a map $\mathbb{Z}/2\mathbb{Z} \otimes \mu_2 \to \mu_2 \subset \bar{\mathbb{Q}}_p^\times$. Therefore $\phi \cup \psi \in H^2(\mathbb{Q}_p, \bar{\mathbb{Q}}_p^\times)$. Fix a square root $\sqrt{b}$ and let $h(g) = (g\sqrt{b})^{\phi(g)}$. A calculation shows that $\phi \cup \psi$ multiplied times the coboundary $h(g_1) \cdot g_1 h(g_2)/h(g_1 g_2)$ equals the cocycle f defined earlier, the one corresponding to the Hilbert symbol $(a, b)_p$. In fact, this cup product is one way to define the Hilbert symbol; see [Se]. We now have a pairing

$$H^1(G_p, \mathbb{Z}/2\mathbb{Z}) \times H^1(G_p, \mu_2) \longrightarrow H^2(G_p, \bar{\mathbb{Q}}_p^\times) \simeq \mathbb{Q}/\mathbb{Z}.$$

The non-degeneracy of this pairing is equivalent to the non-degeneracy of the Hilbert symbol.

Now let p be odd and consider the group $H^1(G_p/I_p,\, \mathbb{Z}/2\mathbb{Z})$ of unramified classes. Assume a is not a square. The element ϕ is in this group if $\sqrt{a}$ generates an unramified extension (in fact, the unique quadratic extension) of $\mathbb{Q}_p$, which means we may assume a is a p-adic unit. We have $(a, b)_p = 1 \iff b$ is a norm from $\mathbb{Q}_p(\sqrt{a}) \iff b$ is a square times a p-adic unit (this follows from the fact that p is a uniformizer for $\mathbb{Q}_p(\sqrt{a})$) $\iff$ the cocycle ψ is unramified. Therefore, the unramified classes in $H^1(\mathbb{Q}_p, \mu_2)$ form the annihilator of the unramified classes in $H^1(\mathbb{Q}_p, \mathbb{Z}/2\mathbb{Z})$ under the above pairing. All of this will be greatly generalized in the next section.

§3. Local Tate Duality.

Let p be prime and let X be a G_p-module of finite cardinality n. Let

$$X^* = \text{Hom}_{\mathbb{Z}}(X,\, \mu_n),$$

where G_p acts on X^* by $(g\, x^*)(x) = g(x^*(g^{-1}x))$. Note that $X \otimes X^* \simeq \mu_n \subseteq \bar{\mathbb{Q}}_p^\times$ as G_p-modules.

Theorem 1 (Local Tate Duality). *(a) The groups $H^i(G_p, X)$ are finite for all $i \geq 0$, and $=0$ for $i \geq 3$.*
(b) For $i = 0, 1, 2$, the cup product gives a non-degenerate pairing

$$H^i(G_p, X) \times H^{2-i}(G_p, X^*) \to H^2(G_p, \bar{\mathbb{Q}}_p^\times) \simeq \mathbb{Q}/\mathbb{Z}.$$

(c) If p does not divide the order of X then the unramified classes $H^1(G_p/I_p, X^{I_p})$ and $H^1(G_p/I_p, (X^*)^{I_p})$ are the exact annihilators of each other under the pairing $H^1(G_p, X) \times H^1(G_p, X^*) \to \mathbb{Q}/\mathbb{Z}$.

For a proof, see [Mi].

For the archimedean prime, the groups $H^i(G_{\mathbb{R}}, X)$ are finite for all i. If we use the modified group $\hat{H}^0$ in place of H^0, then we have $\#\hat{H}^0(G_{\mathbb{R}}, X) = \#H^i(G_{\mathbb{R}}, X)$ for all $i > 0$. There is a non-degenerate pairing

$$H^1(G_{\mathbb{R}}, X) \times H^1(G_{\mathbb{R}}, X^*) \to \mathbb{Q}/\mathbb{Z},$$

and also

$$\hat{H}^0(G_{\mathbb{R}}, X) \times H^2(G_{\mathbb{R}}, X^*) \to \mathbb{Q}/\mathbb{Z}$$

(and with $\hat{H}^0$ and H^2 reversed); note that we use the modified $\hat{H}^0$ here also.

Another result we need evaluates Euler characteristics.

Proposition 3. *Let p be prime and let X be a finite G_p-module. Then*

$$\frac{\#H^1(G_p,X)}{\#H^0(G_p,X)\cdot\#H^2(G_p,X)}=\frac{\#H^1(G_p,X)}{\#H^0(G_p,X)\cdot\#H^0(G_p,X^*)}=p^{v_p(\#X)}.$$

The first equality follows from Theorem 1. For a proof of the proposition, see [Mi].

By using Theorem 1 and Proposition 3, we can evaluate $\#H^1(G_p,X)$ and $\#H^2(G_p,X)$ in terms of $\#H^0(G_p,X)$ and $\#H^0(G_p,X^*)$. These are much easier to calculate in most cases.

§4. Extensions and deformations.

The main reason that Galois cohomology arises in Wiles' work is that certain cohomology groups can be used to classify deformations of Galois representations. In order to explain this, we need a few concepts.

Suppose G is a group acting on an abelian group M, and assume in addition that M is a free module of rank n over a ring R (commutative with 1), and the action of G commutes with the action of R. The action of G is then given by a homomorphism

$$\rho: G\to \mathrm{GL}_n(R).$$

This yields an action of G on $M_n(R)$, the ring of $n\times n$ matrices, via $x\mapsto\rho(g)x\rho(g)^{-1}$. Let $\mathrm{Ad}\rho$ denote $M_n(R)$ (or $\mathrm{End}_R(M)$) with this action. We also will need the submodule $\mathrm{Ad}^0\rho$ consisting of matrices with trace 0.

An *extension* of M by M will mean a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\alpha"] & E \arrow[r, "\beta"] & M \arrow[r] & 0, \end{tikzcd}$$

where E is an $R[G]$-module and α and β are $R[G]$-homomorphisms. The equivalence of two extensions is given by a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\alpha_1"] \arrow[d, "="'] & E_1 \arrow[r, "\beta_1"] \arrow[d, "\gamma"'] & M \arrow[r] \arrow[d, "="'] & 0 \\ 0 \arrow[r] & M \arrow[r, "\alpha_2"] & E_2 \arrow[r, "\beta_2"] & M \arrow[r] & 0, \end{tikzcd}$$

where γ is an $R[G]$-isomorphism. The set of equivalence classes of such extensions is denoted $\mathrm{Ext}^1(M,M)$.

Let $R[\epsilon]$ denote the ring $R[T]/(T^2)$ (so $\epsilon^2=0$). An *infinitesimal deformation* of ρ is an extension of ρ to

$$\rho': G\to\mathrm{GL}_n(R[\epsilon])$$

such that ρ' maps to ρ under the map $\epsilon\mapsto 0$. Two such infinitesimal deformations ρ' and ρ'' are equivalent if there is a matrix $A\equiv I \mod \epsilon$ such that $A\rho'A^{-1}=\rho''$. The idea behind this is that we want to fit ρ into a family of representations. Suppose, for example, that R is a local ring with maximal ideal $\mathcal{M}$, and that we can extend ρ to $\tilde\rho: G\to\mathrm{GL}_n(R[T])$ (or $R[[T]]$ if R is complete). Then we can evaluate T at anything in the maximal ideal $\mathcal{M}$ and get a representation congruent to $\rho \mod \mathcal{M}$. The infinitesimal deformations are the first steps in the direction of constructing such families.

Proposition 4. *The following sets are in one-one correspondence.*
(a) $H^1(G,Ad\rho)$
(b) $Ext^1(M,M)$
(c) Equivalence classes of infinitesimal deformations of ρ.

Proof. Consider an extension $0\to M\xrightarrow{\alpha}E\xrightarrow{\beta}M\to 0$. Since M is free over R, there is an R-module homomorphism $\phi: M\to E$ such that $\beta\circ\phi=\mathrm{id}_M$. Let $g\in G$ and $m\in M$. Since β is an $R[G]$-homomorphism, $g\phi(g^{-1}m)-\phi(m)$ is in $\mathrm{Ker}(\beta)$. Let $T_g: M\to M$ be defined by

$$T_g(m)=\alpha^{-1}\big(g\phi(g^{-1}m)-\phi(m)\big).$$

It is easy to check that $T_{g_1g_2}=T_{g_1}+g_1T_{g_2}$, where the action of G is the one on $\mathrm{Ad}\rho$. Therefore $g\mapsto T_g$ gives an element of $H^1(G,\mathrm{Ad}\rho)$. If we have two equivalent extensions and ϕ_1 and ϕ_2 are the corresponding maps, and T_1 and T_2 are the corresponding cocycles, then $(T_2)_g-(T_1)_g=g\psi-\psi$, where $\psi=\alpha^{-1}\gamma^{-1}(\phi_2-\gamma\phi_1): M\to M$. Therefore

$T_2 - T_1$ is a coboundary for $\mathrm{Ad}\rho$, hence T_1 and T_2 represent the same class in $H^1(G, \mathrm{Ad}\rho)$. Therefore we have a well-defined map $\mathrm{Ext}^1(M, M) \to H^1(G, \mathrm{Ad}\rho)$.

Note that the trivial extension $E = M \oplus M$ (as $R[G]$-modules) yields the trivial cohomology class.

We remark that this method of obtaining cocycles is fairly standard; namely, take an element, such as ϕ, in a bigger set, in this case $\mathrm{Hom}(M, E)$, and form $g\phi - \phi$. Something of this form will automatically satisfy the cocycle condition, but of course we also want $g\phi - \phi$ to be in the original set. When ϕ itself is in the original set, in this case $\mathrm{Ad}\rho$, the cocycle is a coboundary.

Now suppose we have two extensions E_1 and E_2 and corresponding cohomology classes T_1 and T_2, and suppose these classes are equal. Then there exists an R-map $\psi : M \to M$ such that $(T_2)_g - (T_1)_g = g\psi - \psi$. Let $e_1 \in E_1$. We can uniquely write $e_1 = \alpha_1(m) + \phi_1(m')$ with $m, m' \in M$. Define $\gamma(e_1) = \alpha_2(m) + \phi_2(m') - \alpha_2(\psi(m'))$. A calculation shows that $\gamma : E_1 \to E_2$ is an $R[G]$-homomorphism that makes the appropriate diagram commute (and is therefore an isomorphism, by the Snake Lemma); hence the extensions are equivalent. We have proved that the map $\mathrm{Ext}^1(M, M) \to H^1(G, \mathrm{Ad}\rho)$ is an injection.

Finally, let $g \to C(g) \in \mathrm{Ad}\rho$ be a cocycle. Let $E = M \otimes_R R[\epsilon] = \epsilon M \oplus M$. We regard $\rho(g)$ as an element of $\mathrm{GL}_n(R[\epsilon])$ via the natural containment $\mathrm{GL}_n(R) \subseteq \mathrm{GL}_n(R[\epsilon])$. The matrix $I + \epsilon C(g)$ is also in $\mathrm{GL}_n(R[\epsilon])$, so we define

$$\rho'(g) = \big(I + \epsilon C(g)\big)\rho(g).$$

This is easily seen to be a homomorphism, and gives an action of G on E. We have the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\epsilon"] & E \arrow[r] & M \arrow[r] & 0. \end{tikzcd}$$

Let $\phi : M \to E = \epsilon M \oplus M$ be the map to the second summand. Then the above recipe gives

$$T_g(m) = \epsilon^{-1}\Big(\big(1 + \epsilon C(g)\big)\rho(g)\,\phi\big(\rho(g)^{-1}m\big) - \phi(m)\Big) = C(g)(m).$$

Therefore this extension yields the cocycle C, so the map $\mathrm{Ext}^1(M, M) \to H^1(G, \mathrm{Ad}\rho)$ is surjective.

The above shows that a cocycle yields an infinitesimal deformation. Conversely, if $\rho' : G \to \mathrm{GL}_n(R[\epsilon])$ extends ρ, define $C(g)$ by $I + \epsilon C(g) = \rho'(g)\rho(g)^{-1}$. An easy calculation shows that C is a cocycle. The identity

$$(I + \epsilon A)(I + \epsilon C)\,\rho\,(I - \epsilon A) = \big(I + \epsilon(A - \rho A \rho^{-1} + C)\big)\rho$$

shows that equivalence of deformations corresponds to equivalence of cohomology classes. Note that the trivial cohomology class corresponds to the trivial deformation $\rho' = \rho$. This completes the proof. □

One of the themes in Wiles' work is to consider deformations with various restrictions imposed. By the above, this corresponds to considering cohomology classes lying in certain subsets of $H^1(G, \mathrm{Ad}\rho)$. For the moment, we consider two such examples.

1. Suppose we want to consider deformations where the determinant remains unchanged. Note that $\det((I + \epsilon C)\rho) = (1 + \epsilon\mathrm{Tr(C)})\mathrm{det}\rho$. Keeping the determinant unchanged is equivalent to having $C \in \mathrm{Ad}^0\rho$. Since $\mathrm{Ad}(\rho) = \mathrm{Ad}^0\rho \oplus R$, where R represents the scalar matrices with trivial action of G, we have $H^1(G, \mathrm{Ad}\rho) = H^1(G, \mathrm{Ad}^0\rho) \oplus H^1(G, R)$. From the above, $H^1(G, \mathrm{Ad}^0\rho)$ gives the classes of infinitesimal deformations with fixed determinant.

2. Let p be prime and consider a cohomology class C in $H^1(G_p/I_p, (\mathrm{Ad}\rho)^{I_p})$, which is the kernel of the restriction map $H^1(G_p, \mathrm{Ad}\rho) \to H^1(I_p, \mathrm{Ad}\rho)$. Let ρ' be the corresponding deformation. Then ρ' restricted to I_p is (equivalent to) the trivial deformation: $\rho'|_{I_p} = \rho|_{I_p}$. Therefore ρ' is unramified at p if and only if ρ is unramified at p (i.e., $\rho|_{I_p}$ is trivial). Moreover, if ρ is ramified, all the ramification of the deformation ρ' comes from that of ρ. We will often require certain cohomology classes to be unramified in order to control the ramification of the corresponding deformations of ρ.

§5. Generalized Selmer groups.

Let X be a $G_{\mathbb{Q}}$-module. Eventually, X will be $\mathrm{Ad}^0\rho$, but for the moment we do not need to make this restriction. As indicated above, we want to study cohomology classes in $H^1(G_{\mathbb{Q}}, X)$ with various local restrictions. For each place ℓ of $\mathbb{Q}$, including the archimedean one, we may regard the group G_ℓ as a subgroup of $G_{\mathbb{Q}}$. There are many ways to do this, but all the results we obtain will be independent of these choices. We have the restriction maps

$$\mathrm{res}_\ell : H^1(G_{\mathbb{Q}}, X) \to H^1(G_\ell, X).$$

Let $\mathcal{L} = \{L_\ell\}$ be a family of subgroups $L_\ell \subseteq H^1(G_\ell, X)$ as ℓ runs through all places of $\mathbb{Q}$, with $L_\ell = H^1(G_\ell/I_\ell, X^{I_\ell})$ for all but finitely many ℓ. Such a family will be called a collection of local conditions. Define the generalized Selmer group

$$H^1_{\mathcal{L}}(\mathbb{Q}, X) = \{x \in H^1(G_{\mathbb{Q}}, X) | \text{res}_\ell(x) \in L_\ell \text{ for all } \ell\}.$$

Let $\mathcal{L}^* = \{L_\ell^\perp\}$, where $L_\ell^\perp$ is the annihilator of L_ℓ under the Tate pairing. By Theorem 1, $L_\ell^\perp = H^1(G_\ell/I_\ell, X^{*I_\ell})$ for all but finitely many ℓ. The following result is crucial in Wiles' proof. It was inspired by work of Ralph Greenberg [Gr].

Theorem 2. *The group $H^1_{\mathcal{L}}(\mathbb{Q}, X)$ is finite, and*

$$\frac{\# H^1_{\mathcal{L}}(\mathbb{Q}, X)}{\# H^1_{\mathcal{L}^*}(\mathbb{Q}, X^*)} = \frac{\# H^0(G_{\mathbb{Q}}, X)}{\# H^0(G_{\mathbb{Q}}, X^*)} \prod_{\ell \le \infty} \frac{\# L_\ell}{\# H^0(G_\ell, X)}.$$

Note that $\# H^0(G_\ell, X) = \# H^1(G_\ell/I_\ell, X^{I_\ell})$ by Lemma 1, so almost all factors in the product are 1. The formulation of the theorem is that of [DDT], which differs slightly from that of [Wi]. An easy exercise, using Theorem 1 and Proposition 3, shows that the two versions are equivalent.

We sketch the proof of the theorem at the end of the paper.

In the applications, $\mathcal{L}$ is chosen so that $H^1_{\mathcal{L}^*} = 0$. Since the terms on the right are fairly easy to work with, we obtain information about the group $H^1_{\mathcal{L}}$, which for appropriate X describes deformations of representations with certain local conditions.

To show how the formula may be used, we now give an application in a fairly concrete setting. The techniques are much in the spirit of those used by Wiles. Let $X = \mathbb{Z}/p^n\mathbb{Z}$ (with trivial Galois action), where p is an odd prime. Let S be a finite set of primes containing p and ∞. For $\ell \in S$, let $L_\ell = H^1(G_\ell, \mathbb{Z}/p^n\mathbb{Z})$. For $\ell \notin S$, let $L_\ell = H^1(G_\ell/I_\ell, \mathbb{Z}/p^n\mathbb{Z})$. Then $L_\ell^\perp = 0$ for $\ell \in S$ and $L_\ell^\perp = H^1(G_\ell/I_\ell, \mu_{p^n})$ for $\ell \notin S$. Consider $H^1_{\mathcal{L}^*}(\mathbb{Q}, \mu_{p^n})$. From above, we know that every element of $H^1(G_{\mathbb{Q}}, \mu_{p^n})$ is represented by a cocycle of the form $g \mapsto g\alpha/\alpha$, where $\alpha^{p^n} = a \in \mathbb{Q}^\times$. To be in $H^1_{\mathcal{L}^*}$, it must be unramified everywhere. Since

$$H^1(I_\ell, \mu_{p^n}) = H^1(G_{\mathbb{Q}_\ell^{unr}}, \mu_{p^n}) \simeq (\mathbb{Q}_\ell^{unr})^\times/((\mathbb{Q}_\ell^{unr})^\times)^{p^n},$$

where $\mathbb{Q}_\ell^{unr}$ is the maximal unramified extension of $\mathbb{Q}_\ell$, this implies that $v_\ell(\alpha) \equiv 0 \mod p^n$ for all ℓ. Therefore $a = p^n$th power in $\mathbb{Q}$ (we can ignore ± 1 since p is odd) and the cocycle represents the trivial cohomology class. It follows that $H^1_{\mathcal{L}^*}(\mathbb{Q}, \mu_{p^n}) = 0$.

We now evaluate the right side of the formula. First, $\# H^0(G_{\mathbb{Q}}, \mathbb{Z}/p^n\mathbb{Z}) = \# \mathbb{Z}/p^n\mathbb{Z} = p^n$. Since we chose p to be odd, $H^0(G_{\mathbb{Q}}, \mu_{p^n}) = 0$. In the product, the terms for $\ell \notin S$ are all 1. When $\ell \neq \infty$ is in S, the factor is

$$\frac{\# H^1(G_\ell, \mathbb{Z}/p^n\mathbb{Z})}{\# H^0(G_\ell, \mathbb{Z}/p^n\mathbb{Z})} = \# H^0(G_\ell, \mu_{p^n}) \cdot \ell^{v_\ell(p^n)}$$

by Proposition 3. The number of p^nth roots of unity in $\mathbb{Q}_\ell$ is $(\ell - 1, p^n)$, so this is the order of $H^0(G_\ell, \mu_{p^n})$. Since $\# \text{Hom}(G_{\mathbb{R}}, \mathbb{Z}/p^n\mathbb{Z}) = 1$, the factor for $\ell = \infty$ is $1/p^n$. Putting everything together, we find

$$\# H^1_{\mathcal{L}}(\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z}) = p^n \prod_{\ell \in S \setminus \infty} (\ell - 1, p^n).$$

Note that $H^1(G_{\mathbb{Q}}, \mathbb{Z}/p^n\mathbb{Z}) = \text{Hom}(G_{\mathbb{Q}}, \mathbb{Z}/p^n\mathbb{Z})$ classifies cyclic extensions of degree dividing p^n, and $H^1_{\mathcal{L}}(\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z})$ gives those extensions that are unramified outside S.

We already have a good supply of such extensions coming from subfields of cyclotomic fields. For each finite prime $\ell \in S$, there is a cyclic extension of degree $(\ell - 1, p^n)$ contained in the ℓ-th cyclotomic field. There is also a cyclic extension of degree p^n contained in the p^{n+1}st cyclotomic field. These extensions are disjoint, so we obtain an abelian extension of exponent p^n and degree $p^n \prod_{\ell \in S} (\ell - 1, p^n)$. The Galois group of this extension has this many homomorphisms into $\mathbb{Z}/p^n\mathbb{Z}$, so all homomorphisms of $G_{\mathbb{Q}}$ into $\mathbb{Z}/p^n\mathbb{Z}$ unramified outside S are obtained from subfields of cyclotomic fields. By enlarging S arbitrarily, we find that every cyclic extension of $\mathbb{Q}$ of degree dividing p^n is contained in a cyclotomic field. The same analysis may be done for powers of 2 with the same result. Since every finite abelian group is a product of cyclic groups of prime power order, we obtain the Kronecker-Weber theorem that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. (Of course, this proof is by no means elementary, since the full power of class field theory is used in the proof of Theorem 2.)

As in the proof of the Kronecker-Weber theorem just given, it will sometimes be necessary to enlarge the set of primes at which ramification is allowed. The following estimates how much the Selmer group increases.

Proposition 5. *Let p be prime and suppose $\#X$ is a power of p. Let $\mathcal{L} = \{L_\ell\}$ be a collection of local conditions and let $q \neq p$ be a prime for which $L_q = H^1(G_q/I_q, X^{I_q})$. Define a new collection $\mathcal{L}' = \{L'_\ell\}$ of local conditions by $L'_\ell = L_\ell$ if $\ell \neq q$ and $L'_q = H^1(G_q, X)$. Then*

$$\frac{\#H^1_{\mathcal{L}'}(\mathbb{Q}, X)}{\#H^1_{\mathcal{L}}(\mathbb{Q}, X)} \leq \#H^0(G_q, X^*).$$

Proof. Since ${L'_q}^\perp = 0$, the conditions defining $H^1_{\mathcal{L}'^*}$ are more restrictive than those defining $H^1_{\mathcal{L}^*}$, so $H^1_{\mathcal{L}'^*}$ has order less than or equal to that of $H^1_{\mathcal{L}^*}$. When $\mathcal{L}$ is changed to $\mathcal{L}'$ in Theorem 2, all factors on the right remain the same except the one for q, which changes from 1 to $\#H^1(G_q, X)/\#H^0(G_p, X)$. By Proposition 3, this equals $\#H^0(G_q, X^*)$, since $q \nmid \#X$. The result follows easily. □

§6. Local conditions.

From now on, fix a finite set Σ of primes (including ∞, though this will not be important). Let p be an odd prime and assume R is a finite ring of cardinality a power of p. We will work with $X = \mathrm{Ad}^0\rho$, where $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ is a 2-dimensional representation. We also assume ρ is an odd representation. For our present purposes, we take this to mean that if c is (any choice of) complex conjugation, then the matrix $\rho(c)$ is similar to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Define a collection of local conditions as follows:

$$\begin{aligned} &L_\ell = H^1(G_\ell/I_\ell, (\mathrm{Ad}^0\rho)^{I_\ell}) \text{ for } \ell \notin \Sigma,\ \ell \neq p \\ &L_\ell = H^1(G_\ell, \mathrm{Ad}^0\rho) \text{ for } \ell \in \Sigma,\ \ell \neq p \\ &L_p \text{ will be specified later.} \end{aligned}$$

In other words, if we think in terms of infinitesimal deformations, we allow as little ramification as possible at the primes $\neq p$ outside Σ, the ramification at those places being due to ramification in ρ. At the primes $\ell \neq p$ in Σ we allow arbitrary ramification. At p we want to control what happens a little more carefully, depending on properties of ρ.

In the formula of Theorem 2, we need to evaluate, or at least estimate, the factors $\#L_\ell/\#H^0(G_\ell, \mathrm{Ad}^0\rho)$ corresponding to the various primes.

- The factors for the primes $\ell \notin \Sigma$ with $\ell \neq p$ are all 1 by Lemma 1
- The factor for the infinite prime is easy. Since $G_{\mathbb{R}}$ has order 2 and $\mathrm{Ad}^0\rho$ has odd order, $H^1(G_{\mathbb{R}}, \mathrm{Ad}^0\rho) = 0$. Therefore L_∞ is a subgroup of the trivial group, hence trivial. We may assume that $\rho(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Since $\rho(c)A\rho(c)^{-1} = A$ is equivalent to A being diagonal, we see that $H^0(G_{\mathbb{R}}, \mathrm{Ad}^0\rho)$ has order $\#R$. Therefore the factor for ∞ is $1/\#R$.
- Let $\ell \in \Sigma$, $\ell \neq p$, ∞. Then, as in the proof of Proposition 5, we have

$$\frac{\#H^1(G_\ell, \mathrm{Ad}^0\rho)}{\#H^0(G_\ell, \mathrm{Ad}^0\rho)} = \#H^0(G_\ell, (\mathrm{Ad}^0\rho)^*).$$

§7. Conditions at p.

Ordinary representations. Suppose $\rho|_{G_p}$ has the form (for some choice of basis) $\begin{pmatrix} \psi_1\epsilon & * \\ 0 & \psi_2 \end{pmatrix}$, where ψ_1 and ψ_2 are unramified characters (with values in $R^\times$), and ϵ is now the cyclotomic character (not the infinitesimal element from above) giving the action of G_p on the p-power roots of unity. Let W^0 be the additive subgroup of $\mathrm{Ad}^0\rho$ given by matrices of the form $\begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}$.

Lemma 2. *G_p acts on W^0 by multiplication by $\psi_1\epsilon/\psi_2$.*

Proof.

$$\begin{pmatrix} \psi_1\epsilon & * \\ 0 & \psi_2 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \psi_1\epsilon & * \\ 0 & \psi_2 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & \psi_1\epsilon b/\psi_2 \\ 0 & 0 \end{pmatrix}. \quad \square$$

Lemma 3. $\#H^0(G_p,(W^0)^*) = \#R/\big(\frac{\psi_1}{\psi_2}(Frob_p)-1\big)R.$

Proof. An element of $(W^0)^*$ is a group homomorphism $\phi : R \to \mu_{p^n}$ (for some sufficiently large n), and ϕ is fixed by G_p if and only if $\phi(gr) = g\phi(r)$ for all $g \in G_p$ and $r \in R$. By Lemma 2, this means $\phi(\frac{\psi_1\epsilon}{\psi_2}r) = \epsilon\phi(r)$. Note that ϵ takes values in the image of $\mathbb{Z}_p$ in R, which is the same as the image of $\mathbb{Z}$ in R. Therefore we can regard ϵ as an integer that is also a unit in R, and consequently obtain $\phi(\frac{\psi_1}{\psi_2}r) = \phi(r)$. Since ψ_1 and ψ_2 are unramified, it suffices to check this for $g = \mathrm{Frob}_p$, so we let $\alpha = \frac{\psi_1}{\psi_2}(\mathrm{Frob}_p)$. We need ϕ to satisfy $\phi((\alpha-1)r) = 0$ for all r. This says that ϕ is a group homomorphism from $R/(\alpha-1)R$ to $\mu_{p^n}\mathbb{Z}$. The number of such homomorphisms is $\#R/(\alpha-1)R$. □

We now look at two choices for L_p.

1. $L_p = \mathrm{Ker}\Big(H^1(G_p, \mathrm{Ad}^0\rho) \to H^1(I_p, \mathrm{Ad}^0\rho/W^0)\Big)$.

In terms of infinitesimal deformations ρ', this requires $\rho'|_{I_p}$ always to be equivalent to the form $\begin{pmatrix} \epsilon & * \\ 0 & 1 \end{pmatrix}$. This case will be used, for example, in the case of an elliptic curve with good ordinary reduction at p.

Consider the diagram

$$\begin{tikzcd}
 & & H^1(G_p, \mathrm{Ad}^0\rho) \arrow[d, "u"] & \\
0 \arrow[r] & H^1(G_p/I_p, (\mathrm{Ad}^0\rho/W^0)^{I_p}) \arrow[r] & H^1(G_p, \mathrm{Ad}^0\rho/W^0) \arrow[r, "\mathrm{res}"] & H^1(I_p, \mathrm{Ad}^0\rho/W^0)^{G_p/I_p}.
\end{tikzcd}$$

Then $L_p = \mathrm{Ker}(\mathrm{res}\circ u)$ and $H^1(G_p, \mathrm{Ad}^0\rho)/L_p \simeq \mathrm{Im}\ (\mathrm{res}\circ u)$. From the exact sequence,

$$\#\mathrm{Im}\ (\mathrm{res}\circ u) \geq \#\mathrm{Im}\ u/\#H^1(G_p/I_p, (\mathrm{Ad}^0\rho/W^0)^{I_p}) = \#\mathrm{Im}\ u/\#H^0(G_p, \mathrm{Ad}^0\rho/W^0),$$

the last equality following from Lemma 1. The exact sequence (with $H^i(X) = H^i(G_p, X)$)

$$0 \to H^0(W^0) \to H^0(\mathrm{Ad}^0\rho) \to H^0(\mathrm{Ad}^0\rho/W^0) \to H^1(W^0) \to H^1(\mathrm{Ad}^0\rho) \to \mathrm{Im}\ u \to 0$$

yields $\#\mathrm{Im}\ u$ as the alternating product of the orders of the other terms, and we obtain

$$\begin{aligned}\frac{\#L_p}{\#H^0(G_p,\mathrm{Ad}^0\rho)} &= \frac{\#H^1(G_p,\mathrm{Ad}^0\rho)}{\#H^0(G_p,\mathrm{Ad}^0\rho)\,\#\mathrm{Im}\ (\mathrm{res}\circ u)} \leq \frac{\#H^1(G_p,\mathrm{Ad}^0\rho)\#H^0(G_p,\mathrm{Ad}^0\rho/W^0)}{\#H^0(G_p,\mathrm{Ad}^0\rho)\,\#\mathrm{Im}\ u} \\ &= \frac{\#H^1(G_p,W^0)}{\#H^0(G_p,W^0)} = \#R\cdot\#H^0(G_p,(W^0)^*).\end{aligned}$$

The last equality follows from Proposition 3. Combining this with Lemma 3, we obtain

$$\frac{\#L_p}{\#H^0(G_p,\mathrm{Ad}^0\rho)} \leq \#R\cdot\#\left[R/(\frac{\psi_1}{\psi_2}(\mathrm{Frob}_p)-1)R\right].$$

2. $L_p = \mathrm{Ker}\Big(H^1(G_p, \mathrm{Ad}^0\rho) \to H^1(G_p, \mathrm{Ad}^0\rho/W^0)\Big)$.

This is used when working with an elliptic curve that has bad multiplicative reduction at p. It is similar to the previous case, except that it specifies what happens on all of G_p. Actually, in this case ("ordinary but not flat" [DDT], or "strict" [Wi]) we could use the same L_p as before, by a result of Diamond [Wi, Proposition 1.1], but the present choice is more convenient for our calculations. By the calculations just completed, but with the new choice of L_p, we have $H^1(G_p, \mathrm{Ad}^0\rho)/L_p \simeq \mathrm{Im}\ u$ and

$$\frac{\#L_p}{\#H^0(G_p,\mathrm{Ad}^0\rho)} = \frac{\#R\cdot\#H^0(G_p,(W^0)^*)}{\#H^0(G_p,\mathrm{Ad}^0\rho/W^0)}.$$

In the case where this will be applied, we will have

$$\psi_1 = \psi_2,$$

so $\#H^0(G_p,(W^0)^*) = \#R$ by Lemma 3. Also, we will have a matrix

$$\rho(g) = \begin{pmatrix} \psi_1\epsilon & y \\ 0 & \psi_2 \end{pmatrix} \text{ with } y \in R^\times$$

in the image of $\rho|_{G_p}$. Since

$$\begin{pmatrix} \psi_1\epsilon & y \\ 0 & \psi_2 \end{pmatrix} \begin{pmatrix} a & * \\ c & -a \end{pmatrix} \begin{pmatrix} \psi_1\epsilon & y \\ 0 & \psi_2 \end{pmatrix}^{-1} = \begin{pmatrix} a + \frac{cy}{\psi_1\epsilon} & * \\ \frac{\psi_2 c}{\psi_1\epsilon} & -a - \frac{cy}{\psi_1\epsilon} \end{pmatrix},$$

it follows that an element of $\mathrm{Ad}^0\rho/W^0$ fixed by G_p is represented by a diagonal matrix. Therefore $\#H^0(G_p, \mathrm{Ad}^0\rho/W^0) = \#R$. Putting things together, we obtain

$$\frac{\#L_p}{\#H^0(G_p, \mathrm{Ad}^0\rho)} = \#R.$$

Flat representations. This is a more technical situation that must be used in the case of an elliptic curve with good supersingular reduction. Let $L_p = H^1_f(G_p, \mathrm{Ad}^0\rho)$ be those cohomology classes in $H^1(G_p, \mathrm{Ad}^0\rho)$ representing extensions $0 \to M \to E \to M \to 0$ in the category of $R[G_p]$-modules attached to finite flat group schemes over $\mathbb{Z}_p$. We also assume that $R = \mathcal{O}/\lambda^n$, where $\mathcal{O}$ is the ring of integers in a finite extension of $\mathbb{Q}_p$ and λ generates the maximal ideal. The theory of Fontaine-Lafaille implies that

$$\frac{\#L_p}{\#H^0(G_p, \mathrm{Ad}^0\rho)} = \#R.$$

§8. Proof of Theorem 2.

We first address a technical point. Let Σ be the finite set of primes and let $\mathbb{Q}_\Sigma$ be the maximal extension of $\mathbb{Q}$ unramified at the primes not in Σ. Let X be a module for G_Σ =Gal$(\mathbb{Q}_\Sigma/\mathbb{Q})$. Then X is also a module for $G_\mathbb{Q}$ that is unramified outside Σ. Some papers, for example [Wi], consider $H^1(G_\Sigma, X)$, while others, for example [DDT], consider the classes of $H^1(G_\mathbb{Q}, X)$ unramified outside Σ. Fortunately, the two groups are isomorphic. In the following, we will find it more convenient to work with $H^1(G_\Sigma, X)$.

Proposition 6. *$H^1(G_\Sigma, X) \simeq Ker\Big(H^1(G_\mathbb{Q}, X) \to \prod_{\ell \notin \Sigma} H^1(I_\ell, X)\Big)$.*

Proof. The following diagram commutes (the top row is inflation-restriction).

$$\begin{tikzcd}
0 \arrow[r] & H^1(G_\Sigma, X) \arrow[r] & H^1(G_\mathbb{Q}, X) \arrow[r] \arrow[d] & H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_\Sigma), X) \arrow[d, "="] \\
 & & \prod_{\ell \notin \Sigma} \mathrm{Hom}(I_\ell, X) & \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_\Sigma), X). \arrow[l, "\phi"']
\end{tikzcd}$$

The map ϕ is injective since a homomorphism that is 0 on I_ℓ for all $\ell \notin \Sigma$ must vanish on the smallest normal subgroup generated by all such I_ℓ, which is Gal$(\bar{\mathbb{Q}}/\mathbb{Q}_\Sigma)$. The result follows easily. □

Proposition 7. *If X is finite then $H^1(G_\Sigma, X)$ is finite.*

Proof. Choose an open normal subgroup H of G_Σ such that H acts trivially on X. Let K be the fixed field of H. The group $H^1(H, X) = \mathrm{Hom}(H, X)$ is finite since it classifies Galois extensions of K, unramified outside Σ, with Galois group isomorphic to a subgroup of X, and there are only finitely many such extensions by a theorem of Hermite-Minkowski. Since G_Σ/H is finite, the group $H^1(G_\Sigma/H, X)$ is finite by its definition. The result now follows from the inflation-restriction sequence. □

Corollary. *$H^1_\mathcal{L}(\mathbb{Q}, X)$ is finite.*

Proof. The group is isomorphic to a subgroup of $H^1(G_\Sigma, X)$. □

Let X be a finite module for $G_\mathbb{Q}$. Fix a set Σ containing ∞, all the prime divisors of $\#X$, and all primes such that I_p does not act trivially on X. There exists an open subgroup that acts trivially on X. This subgroup corresponds to some finite extension $K/\mathbb{Q}$, and the inertia group of any prime not ramifying in K acts trivially on X. Therefore we can take Σ to be finite. Let Σ_f be the set of finite primes in Σ. For an integer $r = 0, 1, 2$, let

$$\alpha_r : H^r(G_\Sigma, X) \longrightarrow \hat{H}^r(G_\mathbb{R}, X) \times \prod_{\ell \in \Sigma_f} H^r(G_\ell, X)$$

be induced by the restriction maps, where $\hat{H}^r(G_\mathbb{R}, X)$ is the modified Tate cohomology group (when $r > 0$, let $\hat{H}^r = H^r$). By Theorem 1, $\hat{H}^r(G_\mathbb{R}, X) \times \prod H^r(G_\ell, X)$ is the dual of $\hat{H}^{2-r}(G_\mathbb{R}, X^*) \times \prod H^{2-r}(G_\ell, X^*)$, so we may dualize the map $H^{2-r}(G_\Sigma, X^*) \to \hat{H}^{2-r}(G_\mathbb{R}, X^*) \times \prod H^{2-r}(G_\ell, X^*)$ to obtain

$$\beta_r : \hat{H}^r(G_\mathbb{R}, X) \times \prod_{\ell \in \Sigma_f} H^r(G_\ell, X) \longrightarrow H^{2-r}(G_\Sigma, X^*)^\vee,$$

where $A^\vee = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ is the dual of an abelian group A. Let $\mathrm{Ker}^r(G_\Sigma, X) = \mathrm{Ker}\ \alpha_r$.

Proposition 8. *There is a non-degenerate canonical pairing*

$$Ker^2(G_\Sigma, X) \times Ker^1(G_\Sigma, X^*) \to \mathbb{Q}/\mathbb{Z}.$$

Proof. The pairing can be defined as follows. Let $f \in \mathrm{Ker}^2$ and $g \in \mathrm{Ker}^1$. For $\ell \in \Sigma$, we can write $\mathrm{res}_\ell f = \delta\phi_\ell$ and $\mathrm{res}_\ell g = \delta\psi_\ell$, where $\phi_\ell : G_\ell \to X$, $\psi_\ell \in X^*$, and δ is the coboundary map of the appropriate dimension. It can be shown that the cup product $f \cup g = 0 \in H^3(G_\Sigma, \mathbb{Q}_\Sigma^\times)$, so $f \cup g = \delta h$ for an appropriate h. Then

$$(f \cup \psi_\ell) - h = (\phi_\ell \cup g) - h + \delta(\phi_\ell \cup \psi_\ell),$$

hence $(f \cup \psi_\ell) - h$ and $(\phi_\ell \cup g) - h$ represent the same class $x_\ell \in H^2(G_l, \mathbb{Q}_\ell^\times) \simeq \mathbb{Q}/\mathbb{Z}$, and it is independent of the choices involved. Define

$$< f, g >= \sum_{\ell \in \Sigma} x_\ell \in \mathbb{Q}/\mathbb{Z}.$$

The proof of the non-degeneracy is much more difficult. See [Mi]. □

Proposition 9. *α_0 is injective, β_2 is surjective, and for $r = 0, 1, 2$, we have Im α_r = Ker β_r.*

For a proof, see [Mi].

This can all be summarized in the following.

Proposition 10 (Poitou-Tate). *The following nine-term sequence is exact:*

$$\begin{tikzcd}
0 \arrow[r] & H^0(G_\Sigma, X) \arrow[r, "\alpha_0"] & \hat{H}^0(G_\mathbb{R}, X) \times \prod_{\ell \in \Sigma_f} H^0(G_\ell, X) \arrow[r, "\beta_0"] & H^2(G_\Sigma, X^*)^\vee \arrow[r] & H^1(G_\Sigma, X) \arrow[d, "\alpha_1"] \\
 & & & & \prod_{\ell \in \Sigma} H^1(G_\ell, X) \arrow[d, "\beta_1"] \\
0 & H^0(G_\Sigma, X^*)^\vee \arrow[l] & \prod_{\ell \in \Sigma} H^2(G_\ell, X) \arrow[l, "\beta_2"'] & H^2(G_\Sigma, X) \arrow[l, "\alpha_2"'] & H^1(G_\Sigma, X^*)^\vee \arrow[l]
\end{tikzcd}$$

where the unlabeled arrows are maps defined by the non-degeneracy of the pairing in Proposition 8.

It is also possible to work with infinite sets Σ, but then some restrictions need to be made on the direct products involved.

We can now prove Theorem 2. The definition of the Selmer group yields the exact sequence

$$0 \to H^1_{\mathcal{L}^*}(\mathbb{Q}, X^*) \to H^1(G_\Sigma, X^*) \to \prod_\Sigma H^1(G_\ell, X^*)/L_\ell^\perp.$$

Dualizing (i.e., $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$) and using the pairing of Theorem 1 yields

$$0 \leftarrow H^1_{\mathcal{L}^*}(\mathbb{Q}, X^*)^\vee \leftarrow H^1(G_\Sigma, X^*)^\vee \leftarrow \prod L_\ell.$$

Splicing this into the nine-term sequence yields

$$\begin{tikzcd}
0 \arrow[r] & H^0(G_\Sigma, X) \arrow[r, "\alpha_0"] & \hat{H}^0(G_\mathbb{R}, X) \times \prod_{\ell \in \Sigma_f} H^0(G_\ell, X) \arrow[r, "\beta_0"] & H^2(G_\Sigma, X^*)^\vee \arrow[r] & H^1_{\mathcal{L}}(\mathbb{Q}, X) \arrow[d, "\alpha_1"] \\
 & & & & \prod_{\ell \in \Sigma} L_\ell \arrow[d, "\beta_1"] \\
 & & 0 & H^1_{\mathcal{L}^*}(\mathbb{Q}, X^*)^\vee \arrow[l] & H^1(G_\Sigma, X^*)^\vee . \arrow[l]
\end{tikzcd}$$

Therefore

$$\frac{\# H^1_{\mathcal{L}}(\mathbb{Q}, X)}{\# H^1_{\mathcal{L}^*}(\mathbb{Q}, X^*)} = \frac{\# H^0(G_\Sigma, X)\, \# H^2(G_\Sigma, X^*)^\vee\, \#(1+c)X}{\# H^1(G_\Sigma, X^*)} \prod_{\ell \in \Sigma} \frac{\# L_\ell}{\# H^0(G_\ell, X)},$$

where we have used the fact for $\ell = \infty$ that $\hat{H}^0(G_\mathbb{R}, X) = H^0(G_\mathbb{R}, X)/(1+c)X$. We now need the following formula for what may be regarded as a global Euler characteristic.

Proposition 11. *Let X be finite. The groups $H^r(G_\Sigma, X)$, $r = 0, 1, 2$, are finite, and*

$$\frac{\# H^0(G_\Sigma, X)\, \# H^2(G_\Sigma, X)}{\# H^1(G_\Sigma, X)} = \frac{\# H^0(G_\mathbb{R}, X)}{\# X}.$$

For a proof, see [Mi, p. 82].

Since $H^2(G_\Sigma, X^*)$ is finite, it has the same order as its dual. Also, $H^0(G_\Sigma, X) = X^{G_\Sigma} = X^{G_\mathbb{Q}} = H^0(G_\mathbb{Q}, X)$. Therefore the proposition, applied to X^*, reduces the proof to the following.

Lemma 4. $\#(1+c)X \cdot \# H^0(G_\mathbb{R}, X^*) = \# X^*$.

Proof. The (non-degenerate) pairing $X \times X^* \to \mu_n$ satisfies $\langle cx, cx^* \rangle = c\langle x, x^* \rangle = \langle x, x^* \rangle^{-1}$, from which it follows that $\langle (1+c)x, x^* \rangle = \langle x, (1-c)x^* \rangle$. Therefore x^* is fixed by $c \iff (1-c)x^* = 0 \iff \langle x, (1-c)x^* \rangle = 0$ for all $x \iff \langle (1+c)x, x^* \rangle = 0$ for all x. Therefore $H^0(G_\mathbb{R}, X^*)$ is the exact annihilator of $(1+c)X$, hence is dual to $X/(1+c)X$. The result follows easily. □

References

[CF] J.W.S. Cassels andA. Fröhlich, *Algebraic number theory*, Acad. Press, New York, 1967.

[DDT] H. Darmon, F. Diamond, and R. Taylor, *Fermat's Last Theorem*, preprint.

[Gr] R. Greenberg, *Iwasawa theory for p-adic representations*, Algebraic number theory - in honor of K. Iwasawa (J. Coates et al., eds.), Advanced studies in pure mathematics **17**, Academic Press, Boston, 1989.

[Ha] K. Haberland, *Galois cohomology of algebraic number fields*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.

[Mi] J.S. Milne, *Arithmetic duality theorems,* Perspectives in Mathematics **1**, Academic Press, Boston, 1986.

[Po] G. Poitou, *Cohomologie galoisienne des modules finis*, Dunod, Paris, 1967.

[Se] J-P. Serre, *Local fields* (translated by M. Greenberg), Springer-Verlag, New York-Heidelberg-Berlin, 1979.

[Sh] S. Shatz, *Profinite groups, arithmetic, and geometry*, Annals of Mathematics Studies **67**, Princeton Univ. Press, 1972.

[Ta] J. Tate, *Duality theorems in Galois cohomology over number fields*, *Proc. International Cong. Math., Stockholm, 1962*, pp. 234–241.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

Department of Mathematics, University of Maryland, College Park, MD 20742