Euler Systems and Arithmetic Geometry

Barry Mazur and Tom Weston

Contents

Chapter 1. Lecture 1 5
1. Galois Modules 5
2. Example : Quasi-Finite Fields 6
3. Local Fields 10

Chapter 2. Lecture 2 13
1. Discrete Valuation Rings 13
2. Local Fields 14
3. The Galois Theory of Local Fields 16

Chapter 3. Lecture 3 19
1. Ramification Groups 19
2. Witt Vectors 23
3. Projective Limits of Groups of Units of Finite Fields 24

Chapter 4. Lecture 4 27
1. The Absolute Galois Group of a Local Field 27
2. Galois Representations 31

Chapter 5. Lecture 5 35
1. Group Cohomology 35
2. Galois Cohomology 38
3. Tate Local Duality 42

Chapter 6. Lecture 6 45
1. Duality Preliminaries 45
2. Tate Local Duality 49

Chapter 7. Lecture 7 53
1. Finite/Singular Structures 53
2. Generalized Selmer Groups 57
3. Brauer Groups 60

Chapter 8. Lecture 8 65
1. Notation for Generalized Selmer Groups 65
2. A Global Pairing 67
3. The Finiteness of the Selmer Group 69

Chapter 9. Lecture 9 75
1. Abelian Varieties 75
2. Selmer Groups of Abelian Varieties 77

Chapter 10. Lecture 10 81
1. Kummer Theory 81
2. Cohomology of Abelian Varieties 86

Chapter 11. Lecture 11 93
1. L/K Forms 93
2. Cohomological Interpretations 95

Chapter 12. Lecture 12 99
1. Torsors for Algebraic Groups 99

Chapter 13. Lecture 13 103
1. The Picard Group of a Curve 103
2. Direct Limits of Selmer Groups 107
3. Conditions on Galois Representations 108

Chapter 14. Lecture 14 115
1. Structures on Galois Representations 115
2. Depth and Kolyvagin-Flach Systems 119

Chapter 15. Lecture 15 121
1. The Main Theorem 121
2. The Main Theorem for Rank 1 Modules 124

Chapter 16. Lecture 16 127
1. Other Versions of the Main Theorem 127

Chapter 17. Lecture 17 135
1. Modular Curves 135
2. Operators on Modular Curves 138

Chapter 18. Lecture 18 143
1. Representations on Torsion Points 143
2. Heegner Points 146

Chapter 19. Lecture 19 149
1. Hecke Operators on Heegner Points 149

Chapter 20. Lecture 20 155
1. The Euler System for $X_0(11)$ 155

Chapter 21. Lecture 21 159
1. Local Behavior of Cohomology Classes 159

Chapter 22. Lecture 22 163
1. Completion of the Proofs 163

Bibliography 169

CHAPTER 1

Lecture 1

This lecture will be a summary of the material to be covered in the next few lectures; many details will be left until then.

1. Galois Modules

Let K be a field, and fix a separable closure K_s. Set

$$G_K = \mathrm{Gal}(K_s/K) = \varprojlim_{K \subseteq K' \subseteq K_s} \mathrm{Gal}(K'/K)$$

where the projective limit is over all finite Galois extensions K' of K contained in K_s. We give G_K its usual profinite (Krull) topology.

Let M be a G_K-module; that is, M is an abelian group with a left G_K-action. We will say that M is a *G_K-Galois module* if this action is continuous with respect to the profinite topology on G_K and the discrete topology on M. (These are called *topological G_K-modules* in [**Se-LF**].) Equivalently, for each $m \in M$ there must be an open subgroup H of G_K which fixes m; that is,

$$M = \bigcup_{H \text{ open subgroup of } G_K} M^H.$$

(Recall that M^H is the subgroup of M of elements invariant under H.)

In particular, if M is a finitely generated G_K-Galois module, then there is an open subgroup H of G_K which fixes all of M. (H is just the intersection of the open subgroups fixing each of the finitely many generators of M.) Since open subgroups of G are just $\mathrm{Gal}(K_s/K')$ for finite extensions K' of K, replacing K' by its normal closure we see that the G_K-action on M factors through $\mathrm{Gal}(K'/K)$ for some finite Galois extension K' of K.

For future reference we will briefly clarify the relationship between G_K-Galois modules and abelian sheaves for the étale topology on $\operatorname{Spec} K$. (See [**Mi-EC**, p. 53] for more details.) In fact, there is an equivalence of categories between the two, although certain objects often belong more naturally in one category than the other. Specifically, set $x = \operatorname{Spec} K$ and $\overline{x} = \operatorname{Spec} K_s$. Then given an abelian sheaf $\mathcal{F}$ we associate to $\mathcal{F}$ the G_K-Galois module

$$M_{\mathcal{F}} = \mathcal{F}(\overline{x}) = \varinjlim_{x' \to x} \mathcal{F}(x')$$

where the direct limit is over $x' = \operatorname{Spec} K'$ for all finite Galois extensions K' of K in K_s.

[0]Last modified September 4, 2003

In the other direction, we first recall that for any x-scheme U which is connected and étale we can associate a G_K-set (that is, a set with a G_K-action) by

$$U \mapsto \mathrm{Hom}_x(\overline{x}, U),$$

the K_s-valued points of U. Given a G_K-Galois module M, we now associate to it the étale sheaf $\mathcal{F}_M$ such that

$$\mathcal{F}_M(U) = \mathrm{Hom}_{G_K}(\mathrm{Hom}_x(\overline{x}, U), M)$$

for any finite étale U over x. We leave it to the reader to check that these associations give the asserted equivalence of categories. (In particular in the first direction one must check that $M_{\mathcal{F}}$ really is a discrete G_K-module. In the second direction, one must check that $\mathcal{F}_M$ really is a sheaf and that $\mathcal{F}_m(\overline{x}) = M$.)

If M is a G_K-Galois module the Galois cohomology groups

$$H^q(G_K, M) = \varinjlim_{H \lhd G_K, H \text{ open}} H^q(G_K/H, M^H)$$

are defined. (Note that if H is open and normal in G_K then G_K/H is finite. For generalities on the cohomology of finite groups see [**Se-LF**, Chapters 7 and 8].) In particular,

$$H^0(G_K, M) = M^{G_K} = \mathrm{Hom}_{G_K}(\mathbb{Z}, M),$$

the G_K-invariants of M. More generally, for any $q \geq 0$

$$H^q(G_K, M) = \mathrm{Ext}^q_{G_K}(\mathbb{Z}, M).$$

2. Example : Quasi-Finite Fields

2.1. Cohomology Groups. We now specialize the notions of the previous section to the case of a quasi-finite field k. (See [**Se-LF**, Chapter 13, Section 2] for the definition of a quasi-finite field.) When working with a quasi-finite field (which for us will almost always actually be finite), we will usually write $\mathfrak{g}_k$ or even just $\mathfrak{g}$ for its absolute Galois group $\mathrm{Gal}(k_s/k)$. We then have an isomorphism

$$\mathfrak{g}_k \cong \widehat{\mathbb{Z}},$$

where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$ with respect to its subgroups of finite index; that is,

$$\widehat{\mathbb{Z}} = \varprojlim_N \mathbb{Z}/N\mathbb{Z}.$$

(If k is actually finite, then there is a canonical choice for this isomorphism; namely, we want $1 \in \widehat{\mathbb{Z}}$ to correspond to the Frobenius automorphism. For general quasi-finite fields we do not have such a canonical choice.) Fix one such isomorphism and let $\varphi \in \mathfrak{g}_k$ correspond to 1. In this setting a $\mathfrak{g}_k$-Galois module M is simply an abelian group M with an automorphism φ such that every orbit of φ is finite.

The cohomology theory in this case is quite simple, at least when M is torsion. It is determined by the exact sequence

$$0 \longrightarrow M^{\mathfrak{g}_k} \longrightarrow M \xrightarrow{1-\varphi} M \longrightarrow M_{\mathfrak{g}_k} \longrightarrow 0$$

where $M_{\mathfrak{g}_k}$ is the $\mathfrak{g}_k$-coinvariants $M/(1-\varphi)M$. (This is the largest quotient of M on which $\mathfrak{g}_k$ acts trivially, just as $M^{\mathfrak{g}_k}$ is the largest submodule of M on which $\mathfrak{g}_k$ acts trivially.) In fact, these give the only non-zero cohomology groups.

THEOREM 2.1. *If k is a quasi-finite field and M is a torsion $\mathfrak{g}_k$-Galois module, then there are natural isomorphisms*

$$H^q(\mathfrak{g}_k, M) = \begin{cases} M^{\mathfrak{g}_k} & q = 0; \\ M_{\mathfrak{g}_k} & q = 1; \\ 0 & q \geq 2. \end{cases}$$

In particular, given a $\mathfrak{g}_k$-module map $f : M \to N$ the following diagrams commute:

$$\begin{array}{ccc} H^0(\mathfrak{g}_k, M) & \xrightarrow{f} & H^0(\mathfrak{g}_k, N) \\ \cong\downarrow & & \downarrow\cong \\ M^{\mathfrak{g}_k} & \xrightarrow{f} & N^{\mathfrak{g}_k} \end{array}$$

$$\begin{array}{ccc} H^1(\mathfrak{g}_k, M) & \xrightarrow{f} & H^1(\mathfrak{g}_k, N) \\ \cong\downarrow & & \downarrow\cong \\ M_{\mathfrak{g}_k} & \xrightarrow{f} & N_{\mathfrak{g}_k} \end{array}$$

where the horizontal maps in each case are the natural maps induced by f.

PROOF. See [**Se-LF**, Chapter 13, Section 1]. □

In fact, somewhat more is true: suppose we are given an exact sequence

$$0 \to M \to N \to P \to 0$$

of $\mathfrak{g}_k$-Galois modules. Consider the exact commutative diagram

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M^{\mathfrak{g}_k} & \to & N^{\mathfrak{g}_k} & \to & P^{\mathfrak{g}_k} & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M & \to & N & \to & P & \to & 0 \\ & & \downarrow{\scriptstyle 1-\varphi} & & \downarrow{\scriptstyle 1-\varphi} & & \downarrow{\scriptstyle 1-\varphi} & & \\ 0 & \to & M & \to & N & \to & P & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & M_{\mathfrak{g}_k} & \to & N_{\mathfrak{g}_k} & \to & P_{\mathfrak{g}_k} & \to & 0. \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

The horizontal arrows in the first and last rows are either obvious or come from functoriality, depending on which you prefer. The snake lemma now yields an exact sequence

$$0 \to M^{\mathfrak{g}_k} \to N^{\mathfrak{g}_k} \to P^{\mathfrak{g}_k} \to M_{\mathfrak{g}_k} \to N_{\mathfrak{g}_k} \to P_{\mathfrak{g}_k} \to 0.$$

In particular, we obtain a boundary map $P^{\mathfrak{g}_k} \to M_{\mathfrak{g}_k}$.

PROPOSITION 2.2. *In the situation above, the diagram*

$$\begin{array}{ccc} H^0(\mathfrak{g}_k, P) & \longrightarrow & H^1(\mathfrak{g}_k, M) \\ \cong\downarrow & & \downarrow\cong \\ P^{\mathfrak{g}_k} & \longrightarrow & M_{\mathfrak{g}_k} \end{array}$$

commutes, where the top and bottom maps are the boundary map in cohomology and the map constructed above respectively.

PROOF. This follows easily from the explicit isomorphisms of [**Se-LF**, Chapter 13, Section 1]. □

2.2. Cup Products. We continue to assume that k is a quasi-finite field (with a fixed topological generator φ of $\mathfrak{g}_k$) and that M is a torsion $\mathfrak{g}_k$-module. Since most of the cohomology groups of M are trivial, the cup product structure must be particularly simple. (Recall that for any profinite group G and discrete G-modules M and N, the cup product is a pairing

$$H^i(G, M) \otimes H^j(G, N) \to H^{i+j}(G, M \otimes N)$$

for any $i, j \geq 0$. See [**AW**, Section 7]. Recall that if M and N are G-modules, then $M \otimes N$ is made into a G-module by setting $g(m \otimes n) = gm \otimes gn$.) Using Theorem 2.1 it is easy to describe the non-trivial cup product pairings for $\mathfrak{g}_k$.

PROPOSITION 2.3. *For $i = j = 0$ the cup product is simply the natural map*

$$M^{\mathfrak{g}_k} \otimes N^{\mathfrak{g}_k} \to (M \otimes N)^{\mathfrak{g}_k}.$$

Similarly, for $i = 1, j = 0$ the cup product is the natural map

$$M_{\mathfrak{g}_k} \otimes N^{\mathfrak{g}_k} \to (M \otimes N)_{\mathfrak{g}_k}.$$

PROOF. This follows easily from the definition of cup product and the usual isomorphisms. □

We can use the above proposition to determine the Pontrjagin dual of M. Recall that this is defined to be

$$M^\vee = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z}).$$

(As always, if G is a group and M and N are G-modules, $\mathrm{Hom}(M, N)$ is given a G-module structure by $(gf)(m) = gf(g^{-1}m)$, $f \in \mathrm{Hom}(M, N)$, $g \in G$, $m \in M$. In particular, the G-invariants of $\mathrm{Hom}(M, N)$ are precisely the G-equivariant homomorphisms.)

PROPOSITION 2.4. *Let M and N be finite $\mathfrak{g}_k$-Galois modules. Suppose that there is a perfect pairing*

$$M \otimes N \to \mathbb{Q}/\mathbb{Z}.$$

(This is equivalent to $N \cong M^\vee$.) Then the induced cup product pairings

$$H^i(\mathfrak{g}_k, M) \otimes H^{1-i}(\mathfrak{g}_k, N) \to H^1(\mathfrak{g}_k, M \otimes N) \to H^1(\mathfrak{g}_k, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$$

are also perfect pairings for $i = 0, 1$.

PROOF. This follows easily from Proposition 2.3. □

2.3. Finite Fields. We now specialize to the case where k is a finite field. Set $p = \operatorname{char} k$ and $q = p^f = |k|$. Since k is finite it is perfect and we have $k_s = \overline{k}$, the algebraic closure of k. Furthermore, in this case we have a canonical isomorphism

$$\mathfrak{g}_k \to \widehat{\mathbb{Z}}$$

given by sending the Frobenius automorphism φ to 1. (We normalize φ so that it sends x to x^q.) For every $n \geq 1$ there is a unique extension k_n of k of degree n; we will write $\mathfrak{g}_n$ for the Galois group $\operatorname{Gal}(k_n/k)$. It is the unique (cyclic) quotient of $\mathfrak{g}_k$ of order n.

We have $|k_n| = q^n$; set $w_n = |k_n^*| = q^n - 1$. For any m dividing n we have norm maps

$$k_n^* \xrightarrow{\mathbf{N}} k_m^*;$$

these are in fact surjective. (See [**Fr**, Section 7, Corollary to Proposition 3].) Define Δ_k to be the projective limit of the k_n^* under these maps. Δ_k is a $\mathfrak{g}_k$-module, although it is not a $\mathfrak{g}_k$-Galois module in the sense of Section 1.

PROPOSITION 2.5. *Δ_k is (very non-canonically) isomorphic to $\prod_{l \neq p} \mathbb{Z}_l$, where the product is over all primes l not equal to p.*

PROOF. First note that the Chinese remainder theorem shows that the above product is simply the projective limit

$$\varprojlim_{N,(N,p)=1} \mathbb{Z}/N\mathbb{Z},$$

the limit taken over only those N relatively prime to p. Further, note that for any N relatively prime to p we can find a w_n with N dividing w_n. The proposition now follows easily from the fact that Δ_k is a projective limit of cyclic groups of all orders prime to p by surjective maps. □

The proposition implies that for any finite extension k' of k, $\Delta_{k'}$ and Δ_k are abstractly isomorphic. In fact, a canonical isomorphism is given by the norm map. (This is one case where it is much more natural to think of things in terms of étale abelian sheaves.) They are even isomorphic as $\mathfrak{g}_{k'}$-modules; since $\mathfrak{g}_k$ doesn't act on $\Delta_{k'}$, this is the best we could hope for. In any event, this leads one to consider $\Delta_{\mathbb{F}_p}$. Here one is able to use roots of unity to construct a canonical isomorphism

$$\Delta_{\mathbb{F}_p} \cong \prod_{l \neq p} \mathbb{Z}_l(1),$$

where $\mathbb{Z}_l(1)$ is the *Tate module* of the l-power roots of unity. That is,

$$\mathbb{Z}_l(1) = \varprojlim_n \mu_{l^n},$$

the maps

$$\mu_{l^{n+1}} \to \mu_{l^n}$$

being the l^{th}-power map. Note that the $\mathbb{Z}_l(1)$ notation is slightly misleading; $\mathbb{Z}_l(1)$ is *not* canonically isomorphic to $\mathbb{Z}_l$ as an abelian group. $\mathbb{Z}_l(1)$ is called the *Tate twist* of $\mathbb{Z}_l$; $\mathfrak{g}_k$ acts on it simply by the cyclotomic action.

3. Local Fields

We continue with the notation of the previous section: k is a finite field of characteristic p and order q. Recall that to k one can associate the ring of *Witt vectors*

$$W(k) = \{(a_0, a_1, a_2, \ldots) \mid a_i \in k\}$$

which is made into a ring using certain universal polynomials. (See [**Se-LF**, Chapter 2, Section 6]. With some effort they can be reconstructed by attempting to model the operations in $\mathbb{Z}_p$.) $W(k)$ has two natural operators F and V given by

$$\begin{array}{rcccl} F & : & (a_0, a_1, a_2, \ldots) & \mapsto & (a_0^p, a_1^p, a_2^p, \ldots); \\ V & : & (a_0, a_1, a_2, \ldots) & \mapsto & (0, a_0, a_1, a_2, \ldots). \end{array}$$

Clearly F and V commute, and in fact $VF = FV$ is simply multiplication by p in $W(k)$. It turns out that $W(k)$ is a complete, absolutely unramified (that is, with uniformizer p) discrete valuation ring with residue field k.

Now, consider the units $W(k)^*$. They naturally sit in an exact sequence

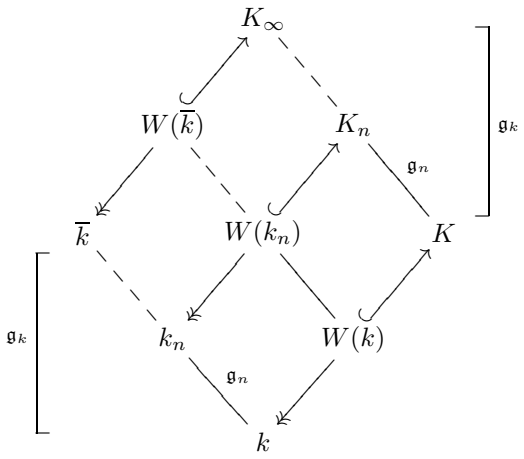
$$0 \to 1 + pW(k) \to W(k)^* \to k^* \to 0,$$

where the map $W(k)^* \to k^*$ is reduction modulo p. Since $1 + pW(k)$ is pro-p and k^* has order prime to p it follows that the sequence splits, so that k^* lifts uniquely to $W(k)^*$ and

$$W(k)^* \cong k^* \times (1 + pW(k)).$$

The splitting map $k^* \to W(k)^*$ is called the *Teichmuller character* and denoted ω. (Its existence can also be seen more directly; for example, it follows easily from Hensel's lemma. (See [**Se-LF**, Chapter 2, Section 2.2, Lemma] or [**Cas**, Appendix C].) Alternatively, one can check that k^* is simply the roots of unity $\mu(W(k))$.)

The same construction applies to k_n; $W(k_n)$ is also an absolutely unramified complete discrete valuation ring. Letting K be the quotient field of $W(k)$, K_n the quotient field of $W(k_n)$, $W(\overline{k})$ the union of all of the $W(k_n)$'s and K_∞ its fraction field, we obtain a diagram



This construction can be shown to give all of the unramified extensions of K. (See [**Se-LF**, Chapter 3, Section 5]. Note that this approach only works for absolutely unramified K.)

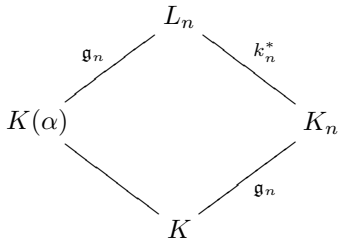
The next step from K to $\bar{K}$ is the tamely ramified piece. For this we use Kummer extensions. We adjoin to the field K_n the w_n^{th} roots of p. More precisely, set

$$L_n = K_n[x]/(x^{w_n} - p).$$

Since K_n contains μ_{w_n} this is indeed a Kummer extension. Also, $x^{w_n} - p$ is an Eisenstein polynomial, so L_n is totally ramified of degree w_n over K_n; since p does not divide w_n the ramification is tame. Furthermore, if we let V be the subgroup of $K_n^*/K_n^{*w_n}$ generated by p, then Kummer theory (as in Lecture 8, Section 3.1) identifies $\mathrm{Gal}(L_n/K_n)$ with $\mathrm{Hom}(V, \mu_{w_n})$ as $\mathrm{Gal}(K_n/K)$-modules. (Recall that $\mathrm{Gal}(K_n/K)$ acts on $\mathrm{Gal}(L_n/K_n)$ by extending an automorphism of K_n to L_n and then using it to conjugate $\mathrm{Gal}(L_n/K_n)$; this is well-defined since $\mathrm{Gal}(L_n/K_n)$ is abelian.) In fact, since K_n is absolutely unramified and $p \in K$, V is isomorphic to $\mathbb{Z}/w_n\mathbb{Z}$ with trivial Galois action. Furthermore, we know that $\mu_{w_n} \cong k_n^*$, so finally we can identify $\mathrm{Gal}(L_n/K_n)$ with k_n^* as $\mathrm{Gal}(K_n/K)$-modules. Thus, if we let $T_n = \mathrm{Gal}(L_n/K)$, we see that it sits in an exact sequence

$$1 \to k_n^* \to T_n \to \mathfrak{g}_n \to 1.$$

This sequence does not in general split; however, since $p \in K$ we can take a single w_n^{th} root of p, say α, and adjoin it to K:



This does allow us to identify a (non-canonical) lifting of $\mathfrak{g}_n$ to T_n, and thus to identify T_n with the semi-direct product of k_n^* and $\mathfrak{g}_n$. We have shown above that the action of $\mathfrak{g}_n$ for this semi-direct product is simply its natural action on k_n^*.

Now, define L_∞ to be the union of all of the L_n, and let $T = \mathrm{Gal}(L_\infty/K)$. That L_∞ is the maximal tamely ramified extension of K_∞ can be seen easily from Kummer theory. $\mathrm{Gal}(L_\infty/K_\infty)$ is the projective limit of the k_n^*'s; one can check that the maps (m divides n)

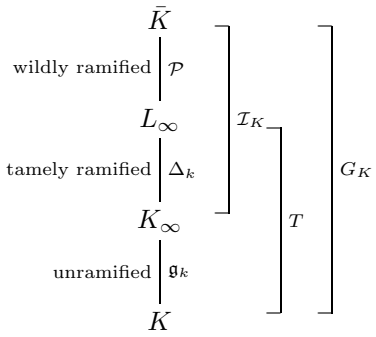
$$\mathrm{Gal}(L_n/K_n) \to \mathrm{Gal}(L_m/K_m)$$

for this projective system are simply the norm maps

$$k_n^* \xrightarrow{\mathbf{N}} k_m^*.$$

Thus $\mathrm{Gal}(L_\infty/K_\infty) \cong \Delta_k$.

We summarize our constructions to this point in the following diagram.



Here $\mathcal{I}_K$ is the inertia group of K. Also, $\mathfrak{g}_k \cong \widehat{\mathbb{Z}}$ (canonically) and $\Delta_k \cong \prod_{l \neq p} \mathbb{Z}_l$ (non-canonically). $\mathcal{P}$ is a pro-p group which is quite complicated.

CHAPTER 2

Lecture 2

1. Discrete Valuation Rings

1.1. Definitions. Let A be a commutative ring with unit. We recall six equivalent characterizations of discrete valuation rings. (As a general convention, for any local ring A we let $\mathfrak{m}_A$ denote its maximal ideal.)

(a) A is a noetherian local ring and $\mathfrak{m}_A$ is principal, generated by a non-nilpotent.
(b) A is a noetherian, integrally closed integral domain with only one non-zero prime ideal.
(c) A is a principal ideal domain with a unique non-zero prime ideal.
(d) Let A be an integral domain with field of fractions K. Then K possesses a surjective *valuation homomorphism*

$$v : K^* \twoheadrightarrow \mathbb{Z},$$

for which, if we set $v(0) = +\infty$, we have

$$v(x + y) \geq \min\{v(x), v(y)\}$$

for all $x, y \in K$, and A can be recovered as

$$A = \{x \in K \mid v(x) \geq 0\}.$$

(e) A has a non-nilpotent element π such that every non-zero element $a \in A$ can be written uniquely as $a = u\pi^n$ for some $u \in A^*$, $n \geq 0$.
(f) A is a discrete valuation ring.

For proofs of the equivalences see [**Se-LF**, Chapter 1, Section 2]. These proofs are essentially a sort of "resolution of singularities" in Krull dimension 1; that is, the implication (b) implies (a) shows that taking the integral closure of a local domain of dimension 1 gives a regular local ring of dimension 1. Geometrically, this corresponds to replacing a possibly non-regular point with a regular point.

Any element $\pi \in A$ of valuation 1 is called a *uniformizer* or a *local parameter*; these are precisely the generators of $\mathfrak{m}_A$. This name also has a geometric interpretation: if A is the local ring of a smooth k-rational point x of an algebraic curve X over k, then a "local parameter" in the above sense is simply a rational function on X which provides a local parameter for X about the point x.

If A is a discrete valuation ring, we will write k_A (or simply k if it is clear from context) for its residue field $A/\mathfrak{m}_A$.

[0]Last modified September 4, 2003

1.2. Completions. There are two different, yet equivalent, points of view on completions. We begin with the algebraic approach. (See [**Ma**, Chapter 8] for the details.) For any noetherian local ring A, we define its $\mathfrak{m}_A$-*adic completion* (or just *completion*) to be the ring

$$\hat{A} = \varprojlim_n A/\mathfrak{m}_A^n.$$

$\hat{A}$ is again a local ring, with maximal ideal $\mathfrak{m}_{\hat{A}} = \mathfrak{m}_A\hat{A}$. There is a natural injection

$$A \hookrightarrow \hat{A}$$

since by Krull's theorem $\cap_n \mathfrak{m}_A^n = 0$. If A is a discrete valuation ring, then $\hat{A}$ is also a discrete valuation ring, and any uniformizer of A is again a uniformizer of $\hat{A}$ (although there are of course many uniformizers of $\hat{A}$ which do not lie in A). We let K and $\hat{K}$ be the field of fractions of A and $\hat{A}$ respectively; we now have a diagram as below.

$$\begin{array}{ccc} A & \hookrightarrow & \hat{A} \\ & \searrow \quad \swarrow & \\ K & \hookrightarrow & \hat{K} \end{array}$$

The topological approach begins with the fraction field K; we define a metric on K by

$$\| x \| = e^{-v(x)}$$

for $x \in K$. (The choice for the base of the exponent is irrelevant for our purposes.) The properties of v make K into a topological field with respect to this metric, and we define $\hat{K}$ to be the topological completion of K with respect to the induced metric topology. We recover the ring $\hat{A}$ simply as

$$\hat{A} = \{x \in \hat{K}; \| x \| \leq 1\}.$$

For more details on this approach, see [**Se-LF**, Chapter 2]. For more details on the comparison of the two methods, see [**Wes-Ide**, Sections 1 and 2].

One easily sees that the residue fields of A and $\hat{A}$ coincide; that is, the natural map $A \hookrightarrow \hat{A}$ induces an isomorphism

$$k_A \xrightarrow{\sim} k_{\hat{A}}.$$

2. Local Fields

2.1. Definitions. Let A be a complete discrete valuation ring (that is, $A = \hat{A}$) with fraction field K and residue field k. If K has characteristic 0 and k is finite, we will call such a K a *local field*. (This is not the usual definition of local field, but it will suffice for our present purposes.)

Since A is complete, we have

$$A = \varprojlim_n A/\mathfrak{m}_A^n.$$

By assumption $A/\mathfrak{m}_A = k$ is finite, and it follows easily that each $A/\mathfrak{m}_A^n$ is finite, since it has finite length over k. Specifically, if k has order q, then $A/\mathfrak{m}_A^n$ has order q^n. In particular, each A is a profinite topological ring (since it is an inverse limit of finite rings) and thus is compact in its natural profinite (i.e., $\mathfrak{m}_A$-adic) topology.

The fraction field K can be written as

$$K = \bigcup_{n \in \mathbb{Z}} \pi^{-n} A$$

for any uniformizer π. Each $\pi^{-n}A$ is easily seen to be both an open and closed subset of K (since the metric on K is discrete), and each $\pi^{-n}A$ is a homeomorphic image of a compact set and thus compact. Thus K is a locally compact topological field.

Given only the topology on K, we can recover A and its maximal ideal $\mathfrak{m}_A$ as

$$A = \{x \in K \mid \{x^\nu\}_{\nu=1}^{\infty} \text{ is contained in a compact set}\}$$

and

$$\mathfrak{m}_A = \{x \in K \mid \lim_{\nu \to \infty} x^\nu = 0\}.$$

From this we also recover $A^* = A - \mathfrak{m}_A$ and the valuation homomorphism, since we know $\mathfrak{m}_A$. Again, for more details on the topology of local fields see [**Wes-Ide**].

2.2. Construction of Local Fields. Let F be a number field with ring of integers $\mathcal{O}_F$. (Recall that this means that F is a finite extension of $\mathbb{Q}$ and $\mathcal{O}_F$ is the integral closure of $\mathbb{Z}$ in F.) Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$, and consider

$$\mathcal{O}_{F,\mathfrak{p}} = \varprojlim_n \mathcal{O}_F/\mathfrak{p}^n.$$

Then $\mathcal{O}_{F,\mathfrak{p}}$ is a complete discrete valuation ring (see [**Se-LF**, Chapter 1, Section 3]). In fact, it can be shown that any local field (as we have defined them) arises in this way.

There is another approach which is in some sense more self-contained. The basic result is the following theorem.

THEOREM 2.1. *Let K be a local field and let L be a finite extension of K. Then there is a unique local field structure on L extending that of K. (That is, there is a unique topology on L giving it the structure of a local field which restrictson K to the given topology.)*

PROOF. (Sketch. For details, see [**Se-LF**, Chapter 2, Section 2].) Let B be the integral closure of A in L.

$$\begin{array}{ccc} B & \hookrightarrow & L \\ \uparrow & & \uparrow \\ A & \hookrightarrow & K \end{array}$$

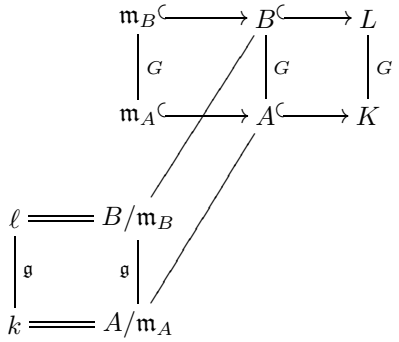
L is a finite dimensional vector space over K, so there is only one compatible topology on L. (See [**Cas**, Section 10].) Now let $\mathfrak{p}$ be a prime ideal of B. Suppose $\mathfrak{p} \cap A = 0$. Then one can use the integrality of B over A to show that $\mathfrak{p}$ must be 0. Thus, for any non-zero prime $\mathfrak{p}$ of B we must have $\mathfrak{p} \cap A = \mathfrak{m}_A$. Again, integrality insures that some such prime must exist. Furthermore, $\mathfrak{p}$ is unique; for if it weren't, each $\mathfrak{p}$ could be used to define a different topology on L compatible with that on K (since $\mathfrak{p} \cap A = \mathfrak{m}_A$). It then follows from the equivalent characterizations of discrete valuation rings that B is a discrete valuation ring, and thus that L is a local field. □

Now, choose a rational prime p. We start with the field $\mathbb{Q}_p$, which is a local field with ring of integers $\mathbb{Z}_p$. Take K to be any finite extension of $\mathbb{Q}_p$; by the theorem it is a local field in a unique way, with ring of integers A the integral closure of $\mathbb{Z}_p$ in K. Again, it can be shown that these are all of the possible local fields (as we have defined them) with residue field of characteristic p.

3. The Galois Theory of Local Fields

Let L/K be a finite Galois extension of local fields. Set $G = \mathrm{Gal}(L/K)$. Note first that G stabilizes B; that is, if $s \in G$, then $s(B) = B$. This is essentially because B is integral over A and s fixes A and thus integral equations over A as well. Further, G stabilizes $\mathfrak{m}_B$. (For this use the topological characterization of $\mathfrak{m}_B$ and the fact that elements of G are homeomorphisms.)

It follows that G induces an action on $B/\mathfrak{m}_B = k_B$. To unify notation, let $\ell = k_B$ for the remainder of this section. Since ℓ/k is a finite extension of finite fields it is automatically Galois. Set $\mathfrak{g} = \mathrm{Gal}(\ell/k)$. We now have a diagram



Since we have shown that G acts on ℓ, and since it obviously fixes k, we have constructed a natural map

$$G \to \mathfrak{g}$$

which is obviously a group homomorphism. We define the *inertia group* $\mathcal{I}$ to be the kernel of this map; it is a subgroup of G.

THEOREM 3.1. *The natural map $G \to \mathfrak{g}$ is surjective; thus we have an exact sequence*

$$0 \to \mathcal{I} \to G \to \mathfrak{g} \to 0.$$

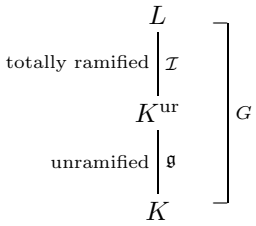
PROOF. k is finite and thus perfect, so the primitive element theorem implies that we can write $\ell = k[\bar{b}]$ for some $\bar{b} \in \ell$. Consider the set of k-conjugates of $\bar{b}$ in ℓ. $\mathfrak{g}$ acts on this set, by definition, and it acts simply transitively since $\bar{b}$ is a primitive element. Now lift $\bar{b}$ to an element b of B. Let $P_b(T)$ be the minimal polynomial of b over A; it has the form

$$P_b(T) = \prod_{s \in S \subseteq G} \big(T - s(b)\big) \in A[T]$$

where S is a subset of G such that S acts simply transitively on the K-conjugates of b. Consider the reduction of $P_b(T)$, say $\bar{P}_b(T) \in k[T]$. By construction $\bar{b}$ is a root of $\bar{P}_b(T)$. Since $\bar{P}_b(T)$ has coefficients in k, it follows that any k-conjugate of $\bar{b}$ is also a root of $\bar{P}_b(T)$; that is, for any $\sigma \in \mathfrak{g}$ there exists an $s \in G$ such that

$\sigma(\bar{b}) = \overline{s(b)}$. Since $\bar{b}$ generates the entire extension ℓ over k, it follows that s maps to σ under the natural map $G \to \mathfrak{g}$, and thus that this map is surjective. □

Let n, f and e be the number of elements in G, $\mathfrak{g}$ and $\mathcal{I}$ respectively. n is simply the degree of L/K; we call f the *residue degree* and e the *inertial degree* or *ramification index* of the extension L/K. By Theorem 3.1 we have $n = ef$. If we set (temporarily) $K^{\mathrm{ur}} = L^{\mathcal{I}}$, the subfield of L fixed by $\mathcal{I}$, we have a diagram



CHAPTER 3

Lecture 3

1. Ramification Groups

1.1. Definitions. In an effort to further understand the ramification in Galois extensions of local fields we will now define a certain filtration of the Galois group. As before let L/K be a finite Galois extension of local fields with ring of integers B and A respectively. Let ℓ and k be their residue fields, and let p be the residue characteristic. For any $i \geq 0$ and $s \in G$, consider the following two equivalent conditions:

(a) s is the identity on $B/\mathfrak{m}_B^{i+1}$;
(b) $v_L(s(b) - b) \geq i + 1$ for all $b \in B$.

Here v_L is the valuation on L, normalized so that

$$v_L : L^* \twoheadrightarrow \mathbb{Z}.$$

If in addition we have that $B = A[\beta]$ for some $\beta \in B$, then we have a third condition equivalent to the previous two.

(c) $v_L(s(\beta) - \beta) \geq i + 1$.

The proof of the equivalence is easy; see [**Se-LF**, Chapter 4, Section 1, Lemma 1]. We define G_i to be the subgroup of G of elements s satisfying any of the above conditions. G_i is called the i^{th} *ramification group* of the extension L/K. It follows easily from condition (a) that each G_i is normal in G. By (b) we also see that for sufficiently large i we must have $G_i = \{1\}$. Thus we have a filtration

$$\{1\} \lhd \cdots \lhd G_i \lhd G_{i-1} \lhd \cdots \lhd G_1 \lhd G_0 \lhd G.$$

We note that $G_0 = \mathcal{I}$ by definition, where $\mathcal{I}$ is the inertia group for the extension L/K. This means that the rest of the group G is irrelevant for the computation of the ramification groups; in particular, we may as well replace K by K^{ur} (recall that this is the maximal unramified extension of K in L; that is, $K^{\mathrm{ur}} = L^{\mathcal{I}}$) and thus assume that L/K is totally ramified. We make this assumption for the remainder of our discussion of ramification groups.

We now investigate the quotients G_i/G_{i+1}. We begin with the special case of $i = 0$. By definition G_0 stabilizes $\mathfrak{m}_B$ and G_1 stabilizes $\mathfrak{m}_B^2$. Thus the natural action of G_0 on $\mathfrak{m}_B/\mathfrak{m}_B^2$ factors through G_0/G_1; in fact, G_0/G_1 acts faithfully on $\mathfrak{m}_B/\mathfrak{m}_B^2$, since any element of G_0 which fixes all of $\mathfrak{m}_B/\mathfrak{m}_B^2$ actually lies in G_1. Since $\mathfrak{m}_B$ is principal, $\mathfrak{m}_B/\mathfrak{m}_B^2$ is free of rank 1 over $B/\mathfrak{m}_B = \ell$. Further, the action of G_0/G_1 on $\mathfrak{m}_B/\mathfrak{m}_B^2$ is l-linear; this is easy to check using the fact that if $b \in B$ lifts an element of ℓ then $s(b) \equiv b \pmod{\mathfrak{m}_B}$ for any $s \in G_0$. Combining all of this we have the following proposition.

[0]Last modified September 4, 2003

PROPOSITION 1.1. *There is a natural injection*

$$G_0/G_1 \hookrightarrow \mathrm{Aut}_l(\mathfrak{m}_B/\mathfrak{m}_B^2) \cong \ell^*.$$

COROLLARY 1.2. *G_0/G_1 is cyclic of order dividing $q_B - 1$, where q_B is the order of ℓ; in particular, it is prime to p.*

We now go off on a complete digression before considering the higher quotients.

1.2. Digression : Filtrations of Matrix Groups. Let R be an arbitrary commutative, noetherian, complete local ring with finite residue field k and maximal ideal $\mathfrak{m}_R$. Thus

$$R = \varprojlim_n R/\mathfrak{m}_R^n$$

and we have an exact sequence

$$0 \to \mathfrak{m}_R \to R \to k \to 0.$$

R is profinite, and thus a compact topological ring. There is also a multiplicative version of the above exact sequence:

$$1 \to 1 + \mathfrak{m}_R \to R^* \to k^* \to 1.$$

This is essentially the exact sequence comparing $\mathrm{GL}_1(R)$ with $\mathrm{GL}_1(k)$, where for any ring R, $\mathrm{GL}_N(R)$ is the group of invertible N by N matrices with entries in R. (Recall that a necessary and sufficient condition for such a matrix to be invertible is that its determinant lies in R^*.)

Fix some positive integer N. Consider the group $\mathrm{GL}_N(R)$. It follows from the completeness of R that we have

$$\mathrm{GL}_N(R) = \varprojlim_n \mathrm{GL}_N(R/\mathfrak{m}_R^n);$$

thus $\mathrm{GL}_N(R)$ is a compact topological group. For any $i \geq 1$, we consider the surjection

$$\mathrm{GL}_N(R) \twoheadrightarrow \mathrm{GL}_N(R/\mathfrak{m}_R^i).$$

(This is easily seen to be a surjection; since R is local, any lifting to R of the entries of a matrix in $\mathrm{GL}_N(R/\mathfrak{m}_R^i)$ will work.) Let Γ_i be the kernel; it is a normal subgroup of $\mathrm{GL}_N(R)$ which is closed and of finite index, and thus open. Thus there is an exact sequence

$$1 \to \Gamma_i \to \mathrm{GL}_N(R) \to \mathrm{GL}_N(R/\mathfrak{m}_R^i) \to 1,$$

and we have defined a filtration

$$\cdots \Gamma_{i+1} \lhd \Gamma_i \lhd \cdots \lhd \Gamma_1 \lhd \mathrm{GL}_N(R)$$

of $\mathrm{GL}_N(R)$.

We now consider the quotients Γ_i/Γ_{i+1}. The first one, $\mathrm{GL}_N(R)/\Gamma_1$, is just $\mathrm{GL}_N(k)$, which is an interesting group. Next consider the higher quotients. It is easy to write down Γ_i explicitly; it is just the set of matrices of the form $1 + (A_{\alpha\beta})$, with each entry $A_{\alpha\beta} \in \mathfrak{m}_R^i$. (Here by 1 we mean the $N \times N$ identity matrix and by $(A_{\alpha\beta})$ we mean the $N \times N$ matrix with (α, β) entry $A_{\alpha\beta}$.) Now, define a map

$$\Gamma_i/\Gamma_{i+1} \to \{(\bar{A}_{\alpha\beta}) \mid \bar{A}_{\alpha\beta} \in \mathfrak{m}_R^i/\mathfrak{m}_R^{i+1}\}$$

by sending $1 + (A_{\alpha\beta})$ to the reduction of $(A_{\alpha\beta})$ modulo $\mathfrak{m}_R^{i+1}$. (Here the second set is made into a group by *addition* of matrices.) The fact that this is a group homomorphism comes from the calculation

$$\big(1 + (A_{\alpha\beta})\big)\big(1 + (B_{\alpha\beta})\big) = 1 + (A_{\alpha\beta} + B_{\alpha\beta}) + (A_{\alpha\beta})(B_{\alpha\beta}) = 1 + (A_{\alpha\beta} + B_{\alpha\beta})$$

since $(A_{\alpha\beta})(B_{\alpha\beta})$ has all entries in $\mathfrak{m}_R^{2i}$, which vanishes modulo $\mathfrak{m}_R^{i+1}$. It is easy to see that this map is actually an isomorphism. The group structure of the second group is quite simple; it is just isomorphic to

$$\overbrace{\mathfrak{m}_R^i/\mathfrak{m}_R^{i+1} \times \cdots \times \mathfrak{m}_R^i/\mathfrak{m}_R^{i+1}}^{n^2},$$

n^2 copies of the additive group $\mathfrak{m}_R^i/\mathfrak{m}_R^{i+1}$. This in turn is an abelian group of exponent p.

We now look at the simplest case of this; take $N = 1$. Our Γ_i's are thus defined by the exact sequences

$$1 \to \Gamma_i \to R^* \to (R/\mathfrak{m}_R^i)^* \to 1.$$

If we apply our above results with the ring B from earlier in this section, we obtain a filtration of the topological group B^*. The usual notation for the Γ_i in this situation is $\mathcal{U}_i$; B^* is denoted by $\mathcal{U}$. We thus have a filtration

$$\cdots \subseteq \mathcal{U}_{i+1} \subseteq \mathcal{U}_i \subseteq \cdots \subseteq \mathcal{U}_1 \subseteq \mathcal{U}.$$

Our above results show that each $\mathcal{U}_i/\mathcal{U}_{i+1}$ is a finite p-group, and thus that $\mathcal{U}_1$ is a pro-p group; that is, $\mathcal{U}_1$ is an inverse limit of finite p-groups.

1.3. The Higher Ramification Groups. We now compare the two filtrations

$$\{1\} \lhd \cdots \lhd G_i \lhd G_{i-1} \lhd \cdots \lhd G_1 \lhd G_0$$

and

$$\cdots \subseteq \mathcal{U}_{i+1} \subseteq \mathcal{U}_i \subseteq \cdots \subseteq \mathcal{U}_1 \subseteq \mathcal{U}$$

that we have constructed. As before, we assume that L/K is totally ramified, so that $G_0 = \mathcal{I} = \mathrm{Gal}(L/K)$. Choose a uniformizer $\pi = \pi_B$ for B. One can easily check that $B = A[\pi]$. (See [**Se-LF**, Chapter 1, Section 6].) So in this case for any $s \in G_0$ we have $s \in G_i$ if and only if

$$s(\pi) \equiv \pi \pmod{\mathfrak{m}_B^{i+1}}.$$

This is in turn is equivalent to

$$\frac{s(\pi)}{\pi} \equiv 1 \pmod{\mathfrak{m}_B^i},$$

since π has exact valuation 1. That is, $s \in G_i$ if and only if

$$\frac{s(\pi)}{\pi} \in \mathcal{U}_i.$$

Now consider the map

$$\theta_i : G_i \to \mathcal{U}_i/\mathcal{U}_{i+1}$$

defined by

$$s \mapsto \frac{s(\pi)}{\pi}.$$

We claim first that θ_i is independent of the choice of π. To see this, let π' be another uniformizer for B; then $\pi' = u\pi$ for some $u \in \mathcal{U}$. We compute

$$\frac{s(\pi')}{\pi'} = \frac{s(u\pi)}{u\pi} = \frac{s(u)}{u}\frac{s(\pi)}{\pi} = \frac{u + m_{i+1}}{u}\frac{s(\pi)}{\pi}$$

for some $m_{i+1} \in \mathfrak{m}_B^{i+1}$, since $s \in G_i$. But

$$\frac{u + m_{i+1}}{u}\frac{s(\pi)}{\pi} \equiv \frac{s(\pi)}{\pi} \pmod{\mathcal{U}_{i+1}}$$

since u is a unit. This shows that θ_i is well-defined independent of π. In fact, it also shows that θ_i is a group homomorphism. To see this, let $s, t \in G_i$. Note that $\pi' = t(\pi)$ is also a uniformizer. Thus

$$\frac{st(\pi)}{\pi} = \frac{st(\pi)}{t(\pi)}\frac{t(\pi)}{\pi} = \frac{s(\pi')}{\pi'}\frac{t(\pi)}{\pi},$$

which shows that θ_i is a homomorphism, since in $\mathcal{U}_i/\mathcal{U}_{i+1}$ we have $s(\pi')/\pi' = s(\pi)/\pi$.

θ_i clearly vanishes on G_{i+1}, so we obtain a map

$$G_i/G_{i+1} \to \mathcal{U}_i/\mathcal{U}_{i+1}$$

which we shall hereafter refer to as θ_i. It is easy to see that θ_i is now injective, using criterion (c) for lying in G_{i+1}. Thus, by the determination of $\mathcal{U}_i/\mathcal{U}_{i+1}$ earlier we now see that G_i/G_{i+1} is abelian of exponent p, for $i \geq 1$. This yields two important corollaries.

COROLLARY 1.3. *The group G_1 is a p-group.*

COROLLARY 1.4. *If L/K is tamely ramified, then $G_1 = \{1\}$. (Recall that an extension L/K is tamely ramified if its ramification index e is prime to p, the residue characteristic.)*

We now summarize our investigation of ramification. So assume L/K is any finite Galois extension of local fields (in particular, we no longer assume that it is totally ramified) with Galois group G and residue Galois group $\mathfrak{g}$. Set $\mathcal{P} = G_1$ and $\Delta = G_0/G_1$. Then $\mathcal{P}$ is a p-group (the wildly ramified inertia subgroup), Δ is cyclic of order prime to p, and we have an exact sequence

$$1 \to \mathcal{P} \to \mathcal{I} \to \Delta \to 1.$$

Next, if we let T be the Galois group of the maximal tamely ramified extension of K in L (that is, the extension $L^{\mathcal{P}}$), then we have exact sequences

$$1 \to \mathcal{P} \to G \to T \to 1$$

and

$$1 \to \Delta \to T \to \mathfrak{g} \to 1.$$

Δ was previously identified with a subgroup of ℓ^*, and one can check that the conjugation action of $\mathfrak{g}$ on Δ is just the usual action of $\mathfrak{g}$ on ℓ^*.

1.4. The Upper Indexing. To this point we have been using the *lower indexing* of ramification groups. This is the simplest to define, but it unfortunately behaves very poorly with respect to extensions. To correct for this, one is led to introduce the upper indexing as follows. (For more details, see [**Se-LF**, Chapter 4].) First, we extend the definition of G_i to real indices by saying that $s \in G_u$ if and only if $v_L(s(b) - b) \geq u + 1$ for all $b \in B$. Now define

$$\varphi(u) = \int_0^u \frac{dt}{(G_0 : G_t)}.$$

(The integrand is piecewise constant, so this is really just a sum; the integral notation is more convenient.) This can be checked to give a bijection from the positive reals to itself. We define the *upper indexing* by

$$G_u = G^{\varphi(u)}.$$

The inverse function of φ can be determined to be

$$\psi(v) = \int_0^v (G^0 : G^w) dw.$$

Thus

$$G^v = G_{\psi(v)}.$$

It turns out that this upper indexing is compatible with extensions, in the sense that if we have a diagram

$$\begin{array}{c} M \\ | \\ L \\ | \; G_{L/K} \\ K \end{array} \Bigg\rceil \; G_{M/K}$$

then under the natural surjection

$$G_{M/K} \twoheadrightarrow G_{L/K}$$

each $G^v_{M/K}$ maps onto $G^v_{L/K}$.

2. Witt Vectors

Let R be a perfect ring of characteristic p. We define the *Witt vectors* over R to be the set

$$W(R) = \{(a_0, a_1, \ldots) \mid a_i \in R\},$$

which is turned into a ring using certain universal polynomials. (See [**Se-LF**, Chapter 2, Section 6] for all references for this section.) The fundamental example is $W(\mathbb{F}_p) = \mathbb{Z}_p$, which is really used to define the univeral polynomials in general. In this case the Witt vector of $\alpha \in \mathbb{Z}_p$ is just the p-adic expansion of α; that is,

$$(a_0, a_1, \cdots) \leftrightarrow \alpha = a_0 + a_1 p + a_2 p^2 + \cdots.$$

In general the relationship is not this simple; it involves twisting by Frobenius.

Now let k be a finite field of characteristic p. Then $W(k)$ is is a complete discrete valuation ring with residue field k. Further, $W(k)$ is *absolutely unramified*;

that is, it has p as a uniformizer. The construction of Witt vectors is also functorial, so we get a map

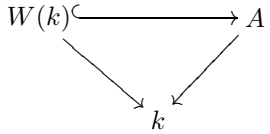
$$\mathbb{Z}_p = W(\mathbb{F}_p) \hookrightarrow W(k).$$

The Galois group $\mathfrak{g} = \mathrm{Gal}(k/\mathbb{F}_p)$ acts on $W(k)$, and one has a canonical isomorphism

$$\mathfrak{g} \cong \mathrm{Gal}(K/\mathbb{Q}_p),$$

where K is the fraction field of $W(k)$. More generally, we have the following proposition.

PROPOSITION 2.1. *Let A be a complete discrete valuation ring with residue field k and fraction field K of characteristic 0. Then there is a unique ring homomorphism*



making this diagram commute, where both maps to k are the natural map.

A is in fact a free $W(k)$-module of rank equal to the absolute ramification index of K. Specifically, one can write $A = W(k)[\pi_A]$, where π_A is any uniformizer for A.

3. Projective Limits of Groups of Units of Finite Fields

3.1. Topologically Cyclic Profinite Groups. Let Γ be a profinite group which is topologically cyclic; that is, there is a $\gamma \in \Gamma$ such that Γ is the closure of the group generated by γ. We further assume that γ has infinite order; this merely excludes the case where Γ is cyclic of finite order. Thus we have a map

$$\gamma^{\mathbb{Z}} \hookrightarrow \Gamma$$

with dense image. Morally speaking, any such Γ ought to be some sort of profinite completion of the infinite cyclic group $\mathbb{Z}$. We will now attempt to make that statement more precise in certain special cases of interest to us.

First of all, we recall the standard examples. We have the full profinite completion of $\mathbb{Z}$,

$$\hat{\mathbb{Z}} = \varprojlim_N \mathbb{Z}/N\mathbb{Z},$$

the inverse system being defined by divisibilities. We also have

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \varprojlim_{N,(N,l)=1 \text{ for } l \neq p} \mathbb{Z}/N\mathbb{Z}.$$

The first inverse system is with respect to the usual ordering of $\mathbb{Z}$, the second with respect to the multiplicative ordering. More generally, if $\mathcal{L}$ is any set of prime numbers of $\mathbb{Z}$, we have

$$\prod_{l \in \mathcal{L}} \mathbb{Z}_l \cong \varprojlim_{N,\ N \text{ has all prime divisors in } \mathcal{L}} \mathbb{Z}/N\mathbb{Z}.$$

This isomorphism comes from the Chinese remainder theorem. All of these groups are topologically cyclic, with canonical generator the image of $1 \in \mathbb{Z}$.

Conversely, suppose that

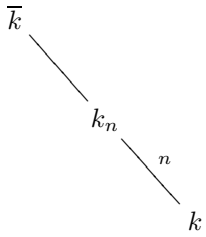
$$\Gamma = \varprojlim_N C_N,$$

where each C_N is cyclic of order w_N and the maps of the inverse system are surjective. In particular Γ is topologically cyclic, as one can lift generators via the surjective maps. Suppose further that every integer M prime to a fixed prime number p divides some w_N, and that all of the w_N are prime to p. Then one can easily show that

$$\Gamma \cong \prod_{l \neq p} \mathbb{Z}_l,$$

although the isomorphism is horribly non-canonical.

3.2. Example : Units of Finite Fields. Let k be a finite field of order q and characteristic p, let $\overline{k}$ be a fixed algebraic closure of k, and let k_n be the unique subfield of $\overline{k}$ of degree n over k.



Set $C_n = k_n^*$ and $w_n = |C_n| = q^n - 1$. This defines an inverse system via norm maps

$$k_{n'} \xrightarrow{\mathbf{N}} k_n$$

for n dividing n'. These maps can be shown to be surjective (see [**Fr**, Section 7, Corollary to Proposition 3]), and one easily checks that the w_n satisfy the conditions at the end of the previous section. Thus, if we define

$$\Delta_k = \varprojlim_n k_n^*,$$

then

$$\Delta_k \cong \prod_{l \neq p} \mathbb{Z}_l,$$

although the isomorphism is non-canonical. (Each factor $\mathbb{Z}_l$ is canonical, but the choice of generator and thus the identification with $\mathbb{Z}_l$ is not.) This is actually a $\mathfrak{g}$-module, where $\mathfrak{g} = \mathrm{Gal}(\overline{k}/k)$, and the action is continuous when Δ_k is given the profinite topology. (It is not continuous if Δ_k is given the discrete topology; thus Δ_k is not a $\mathfrak{g}$-Galois module.)

Now let k' be any finite extension of k in $\overline{k}$. Then

$$\Delta_{k'} \cong \Delta_k$$

since $\Delta_{k'}$ is defined to be an inverse limit of a cofinal subsystem of the inverse system defining Δ_k. In fact, this is a $\mathfrak{g}'$-isomorphism, where $\mathfrak{g}' = \mathrm{Gal}(\overline{k}/k')$. This suggests that we should look at the $\mathrm{Gal}(\overline{k}/\mathbb{F}_p)$-module $\Delta_{\mathbb{F}_p}$. We use this module to define $\mathrm{Gal}(\overline{k}/\mathbb{F}_p)$ modules $\mathbb{Z}_l(1)$ by

$$\Delta_{\mathbb{F}_p} = \prod_{l \neq p} \mathbb{Z}_l(1).$$

This notation is slightly misleading, in that $\mathbb{Z}_l(1)$ is not canonically isomorphic to $\mathbb{Z}_l$. It can actually be realized as the Tate module of the l-power roots of unity; that is,

$$\mathbb{Z}_l(1) = \varprojlim_n \mu_{l^n}.$$

In fact, Δ_k can also be realized as this same product, via our earlier isomorphism. Here $\mathfrak{g}$ acts on each $\mathbb{Z}_l(1)$ simply as it would as a subgroup of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

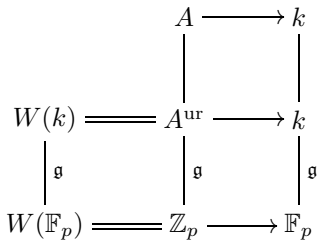
CHAPTER 4

Lecture 4

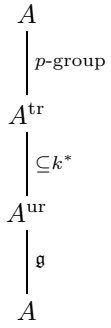
1. The Absolute Galois Group of a Local Field

1.1. Finite Galois Extensions. We continue to let K be a local field, in the sense defined previously, with ring of integers $\mathcal{O}_K$ and residue field $k = k_A = \mathcal{O}_K/\mathfrak{m}_A$ of characteristic p. For this section we will feel free to think of Galois groups as belonging to extensions of rings of integers; this will simplify notation, and no confusion should result.

Let $\mathfrak{g} = \mathrm{Gal}(k/\mathbb{F}_p)$. Using our construction of Witt vectors, we get a diagram



In fact, using our study of ramification groups we know that we can further decompose the extension as



where the notation above is supposed to indicate that we know that $\mathrm{Gal}(A^{\mathrm{tr}}/A^{\mathrm{ur}})$ is isomorphic to the ramification quotient G_0/G_1, which canonically embeds in k^*. (See Lecture 3, Section 1.1.)

1.2. Passage to the Limit. We now generalize the above construction. Let k_n be the unique extension of k of degree n, and let $\mathfrak{g}_n = \mathrm{Gal}(k_n/k)$. Let q_n be the order of k_n and let $w_n = q_n - 1$ be the order of k_n^*. Then Hensel's lemma (see [**Cas**, Appendix C]) shows that the elements of k_n^* lift to $W(k_n)$ as roots of unity;

[0]Last modified September 4, 2003

more precisely, there is an isomorphism

$$\omega : k_n^* \xrightarrow{\cong} \mu(W(k_n)),$$

called the *Teichmuller character*, such that

$$\omega(a) \equiv a \pmod{\mathfrak{m}}$$

for all $a \in k_n^*$, where $\mathfrak{m}$ is the maximal ideal of $W(k_n)$. Somewhat more explicitly, one can define $\omega(a)$ by

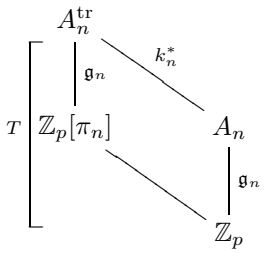
$$\omega(a) = \lim_{\nu \to \infty} \tilde{a}^{q_n^\nu}$$

where $\tilde{a}$ is any choice of lifting of a to $W(k_n)$. (The basic idea here is that exponentiating by powers of q_n will not affect the root of unity part of $\tilde{a}$, while it will "push" the non-root of unity part off to infinity. It is still congruent to a since exponentiating by q_n is the identity on the residue field.)

Let us now construct the maximal totally tamely ramified extension of $A_n = W(k_n)$. This can be done using Kummer theory (for a review of Kummer theory, see Lecture 8, Section 3.1); simply set

$$A_n^{\mathrm{tr}} = W(k_n)[x]/(x^{w_n} - p).$$

As before, Kummer theory shows that the Galois group of A_n^{tr} over $W(k_n)$ is canonically isomorphic to k_n^*. (See Lecture 1, Section 3.) This further implies that A_n^{tr} really is the *maximal* tamely ramified extension of A_n, since we have shown that the Galois group of any tamely ramified extension of A_n will inject into k_n^*. (See Lecture 3, Proposition 1.1. One must also use the fact that the residue field does not change under totally ramified extensions.) Choose a uniformizer π_n of A_n^{tr}. Letting T_n be the Galois group of A_n^{tr} over $W(\mathbb{F}_p) = \mathbb{Z}_p$, we have a diagram

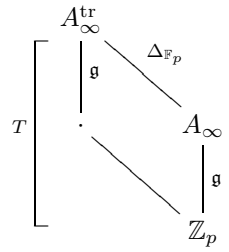


where the unlabeled extension isn't even Galois, since $\mathbb{Z}_p$ doesn't contain the w_n^{th}-roots of unity for $n \geq 2$. Nevertheless, we do get a semi-direct product decomposition

$$T_n = k_n^* \rtimes \mathfrak{g}_n$$

where the action of $\mathfrak{g}_n$ on k_n^* is simply its natural action. (This is immediate, using the fact that the isomorphism of Kummer theory is Galois equivariant.)

Next, we take the limit as n goes to infinity of the above construction. This yields a diagram



where $A_\infty = W(\overline{\mathbb{F}}_p)$, $\mathfrak{g} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}$, A_∞^{tr} is the tamely ramified extension of A_∞ generated by all non p-power roots of p, T is the Galois group of the fraction field of A_∞^{tr} over $\mathbb{Q}_p$, and the unnamed entry is some non-canonical non-Galois extension of $\mathbb{Z}_p$. In particular, as above $T = \Delta_{\mathbb{F}_p} \rtimes \mathfrak{g}$, where the action of $\mathfrak{g}$ on $\Delta_{\mathbb{F}_p}$ is its natural action. We can also write this as an exact sequence

$$1 \to \Delta_{\mathbb{F}_p} \to T \to \mathfrak{g} \to 1$$

or, via our earlier canonical isomorphisms,

$$1 \to \prod_{l \neq p} \mathbb{Z}_l(1) \to T \to \widehat{\mathbb{Z}} \to 1.$$

Both of the flanking terms in this exact sequence are topologically cyclic in the sense of Lecture 3, Section 3. Let φ be any lifting of the canonical Frobenius generator of $\mathfrak{g}$; we will refer to it as a Frobenius element of T. Let τ be any topological generator of $\Delta_{\mathbb{F}_p}$. No matter the choice of φ and τ, they are related by

$$\varphi\tau\varphi^{-1} = \tau^p$$

since φ acts as Frobenius on $\Delta_{\mathbb{F}_p}$, and the action in this setting is given by conjugation. In fact, this is a presentation of T, in a sense that we make precise in the following proposition.

PROPOSITION 1.1. *The group T is the profinite completion of the group on two generators τ and φ satisfying the single relation $\varphi\tau\varphi^{-1} = \tau^p$.*

PROOF. We sketch the proof. Let F be the group generated by τ and φ with the above relation. Every element can be written uniquely in the form $\tau^a\varphi^b$, and we have the commutation relation $\varphi^a\tau^b = \tau^{bp^a}\varphi^a$. One first shows that the profinite completion of the subgroup generated by φ is $\widehat{\mathbb{Z}}$; this is because combining the above relation with $\varphi^n = 1$ and $\tau^n = 1$ doesn't introduce any additional conditions solely on φ. On the other hand, the same construction with the subgroup generated by τ does result in the condition

$$\tau^{p^n - 1} = 1.$$

It follows from Lecture 3, Section 3 that the profinite completion of the subgroup generated by τ is isomorphic to

$$\prod_{l \neq p} \mathbb{Z}_l.$$

Also, the relation shows that this subgroup is normal. Thus we get an exact sequence

$$1 \to \prod_{l \neq p} \mathbb{Z}_l \to \hat{F} \to \widehat{\mathbb{Z}} \to 1,$$

where $\hat{F}$ is the profinite completion of F. Furthermore, we have a lifting of a generator of $\widehat{\mathbb{Z}}$ to $\hat{F}$: namely, φ. We also know how φ acts on the other factor, by the defining relation. Thus

$$\hat{F} \cong \prod_{l \neq p} \mathbb{Z}_l \rtimes \widehat{\mathbb{Z}},$$

with the same action of $\widehat{\mathbb{Z}}$ on $\prod_{l \neq p} \mathbb{Z}_l$ as T. Thus $T \cong \hat{F}$. □

It follows easily from this characterization that we also have a homeomorphism (although definitely *not* a homomorphism)

$$\prod_{l \neq p} \mathbb{Z}_l \times \widehat{\mathbb{Z}} \to T$$

given by sending $\alpha \times \beta$ to $\tau^\alpha \varphi^\beta$.

Let us now consider a subgroup T' of T of finite index. T' must contain some power of φ, since otherwise all of the powers of φ would lie in different cosets. Similarly, it must contain some power of τ, and we can take this power to be prime to p since p is "invertible" when acting on τ. In other words, there is some integer e prime to p, some integer f and some lifting φ of $1 \in \widehat{\mathbb{Z}}$ such that

$$\tau^e, \varphi^f \subseteq T'.$$

We will denote by $T_{e,f}$ the closed subgroup of T generated by τ^e and φ^f for e and f as above; the above argument shows that these are all of the subgroups of T of finite index. (In particular they are open.) They are not all normal, however; one can check easily (by conjugating τ^e by φ and φ^f by τ) that this occurs if and only if e divides $p^f - 1$.

1.3. Absolute Galois Groups. Since T is the maximal tamely ramified quotient of the absolute Galois group $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, we have an exact sequence

$$1 \to \mathcal{P} \to G_{\mathbb{Q}_p} \to T \to 1$$

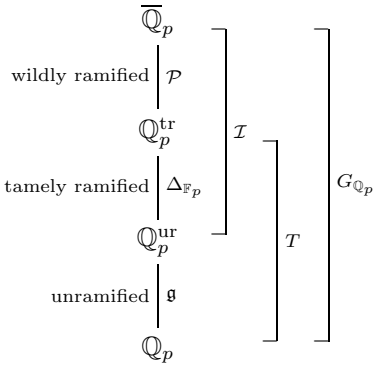
where $\mathcal{P}$ is the wild ramification subgroup of $G_{\mathbb{Q}_p}$; it is pro-p. Letting $\mathcal{I}$ be the inertia subgroup of $G_{\mathbb{Q}_p}$, we have an exact sequence

$$1 \to \mathcal{I} \to G_{\mathbb{Q}_p} \to \mathfrak{g} \to 1.$$

Restricting our attention to $\mathcal{I}$ alone, we have an exact sequence

$$1 \to \mathcal{P} \to \mathcal{I} \to \Delta_{\mathbb{F}_p} \to 1.$$

This is all sumarized in the diagram



Now let K be any finite extension of $\mathbb{Q}_p$. Let G_K be its absolute Galois group, so that $G_K \subseteq G_{\mathbb{Q}_p}$. We set $\mathcal{I}_K = \mathcal{I} \cap G_K$ and $\mathcal{P}_K = \mathcal{P} \cap G_K$; $\mathcal{I}_K$ is simply the inertia group of $\bar{K}/K$. We also let T_K be the image of G_K under the map $G_{\mathbb{Q}_p} \to T$; this is *not* the same as the tame inertia group of K in the usual sense if K has wild ramification over $\mathbb{Q}_p$. One easily checks that $T_K = T_{e,f}$ where e is the prime to p part of the inertial degree of K and f is the residue degree of K. We now have an exact sequence

$$1 \to \mathcal{P}_K \to G_K \to T_K \to 1.$$

2. Galois Representations

2.1. Definitions and Reductions. Let K be a local field of residue characteristic p. Let F be a field of scalars; for our purposes we will take F to also be a local field, of residue characteristic l. We will usually, but not always, want $l \neq p$. Let V be a vector space over F of finite dimension d. We consider G_K-representations on V; of course, we assume them to be continuous and F-linear. So, by a *Galois representation* we mean a continuous homomorphism

$$\rho : G_K \to \mathrm{Aut}_F(V) \cong \mathrm{GL}_d(F),$$

the isomorphism being given by any choice of an F-basis of V.

We begin by showing that one may actually assume that the image of G_K lands in $\mathrm{GL}_d(\mathcal{O}_F)$, where $\mathcal{O}_F$ is the ring of integers in F. More generally, let Γ be any profinite group which acts continuously and F-linearly on V:

$$\Gamma \to \mathrm{Aut}_F(V).$$

Recall that a lattice $\Omega \subseteq V$ is a free $\mathcal{O}_F$-submodule of V of rank d, such that

$$\Omega \otimes_{\mathcal{O}_F} F \xrightarrow{\cong} V.$$

We claim that there is some lattice Ω which is stabilized by Γ. Let Ω_0 be any lattice of V. Then if we choose the basis for V to also be an $\mathcal{O}_F$-basis of Ω_0, we can realize $\mathrm{GL}_d(\mathcal{O}_F)$ as the compact open subgroup of $\mathrm{GL}_d(V)$ preserving Ω_0. The cosets $\mathrm{GL}_d(F)/\mathrm{GL}_d(\mathcal{O}_F)$ correspond to the set of all lattices of V, the correspondence given by sending $g \in \mathrm{GL}_d(F)$ to $g\Omega_0$. Now, for our purposes we may replace Γ by its image in $\mathrm{GL}_d(F)$, so that Γ is now a compact subgroup of $\mathrm{GL}_d(F)$. Consider the set

$$\Gamma_0 = \Gamma \cap \mathrm{GL}_d(\mathcal{O}_F).$$

This is open in Γ, and thus has finite index since Γ is profinite and thus compact. Let $\gamma_1, \ldots, \gamma_\nu$ be a set of coset representatives for Γ/Γ_0. Take

$$\Omega = (\gamma_1 + \cdots + \gamma_\nu)\Omega_0.$$

One can check that Ω is a lattice, and it is clearly stabilized by Γ since Ω_0 is stabilized by Γ_0. (Use the easily checked fact that given a lattice of rank n in a vector space of dimension n over a local field, adding any vector to the lattice results again in a lattice of rank n.)

The fact that Γ stabilizes the lattice Ω implies that, by choosing the basis of F to be an $\mathcal{O}_F$-basis of Ω, the action of Γ on $\mathrm{GL}_d(F)$ factors through $\mathrm{GL}_d(\mathcal{O}_F)$. We state the Galois case as a proposition.

PROPOSITION 2.1. *Let V be an F-vector space of dimension d, and let*

$$\rho : G_K \to \mathrm{Aut}_F(V)$$

be a Galois representation. Then there is a basis of V such that with respect to this basis the image of ρ is in $\mathrm{GL}_d(\mathcal{O}_F)$.

2.2. Potentially Semistable Representations. By our presentation of the Galois group T in Section 1.2, we know that a representation of T on V is simply given by specifying two invertible F-linear operators τ and φ satisfying the single relation

$$\varphi\tau\varphi^{-1} = \tau^p.$$

By our above reductions we can further assume that τ and φ preserve $\mathcal{O}_F$.

Let $v \in V$ be an eigenvector of τ with eigenvalue λ. Set $v_n = \varphi^{-n}v$ for all $n \geq 0$. Then using the above relation one easily checks that v_n is an eigenvector of τ with eigenvalue λ^{p^n}. (Each time you "commute" a φ^{-1} with τ the τ is replaced by a τ^p.) But V is finite dimensional, so τ has only finitely many eigenvalues. Thus for some $m < n$,

$$\lambda^{p^m} = \lambda^{p^n}.$$

In particular, λ is a $(p^{n-m} - 1)p^m$-root of unity. In fact, we can take the above m to be zero, for we are free to replace λ by λ^{p^m} (by replacing v with v_m), in which case the above equality becomes

$$\lambda = \lambda^{p^{n-m}}.$$

Thus λ is a $(p^\nu - 1)^{\text{th}}$ root of unity for some ν. Since all of the eigenvalues of $\tau^{p^\nu - 1}$ are thus 1, we see that $\tau^{p^\nu - 1}$ becomes *unipotent* (that is, the sum of the identity matrix and a nilpotent matrix) over some finite extension of F which contains all of its eigenvalues. *unipotent*; that is, it is the sum of the identity matrix and a nilpotent matrix.

We are now in a position to prove a fundamental result of Grothendieck. We first need a definition.

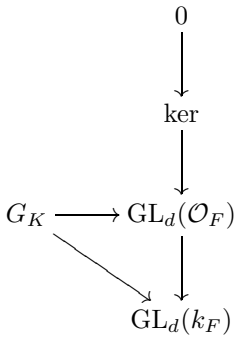
DEFINITION 1. Assume $l \neq p$. A Galois representation

$$\rho : G_K \to \mathrm{GL}_d(F)$$

is said to be *semistable* if the image of $\mathcal{I}_K$ is unipotent. ρ is said to be *potentially semistable* if there is some finite extension L/K such that $\rho|_{G_L}$ is semistable.

PROPOSITION 2.2 (Grothendieck). *Let $\rho : G_K \to \mathrm{GL}_d(F)$ be a Galois representation. Suppose that F and K have different residue characteristics l and p respectively. Then ρ is potentially semistable.*

PROOF. As before, we can conjugate ρ so as to assume that its image is in $\mathrm{GL}_d(\mathcal{O}_F)$; this is permitted because conjugation does not affect the property of being unipotent. Consider the diagram



where k_F is the residue field of $\mathcal{O}_F$ and ker is the kernel of the above map. Since $\mathrm{GL}_d(k_F)$ is finite, ker has finite index in $\mathrm{GL}_d(\mathcal{O}_F)$. Thus, since we are allowing finite extensions, we can replace K by the fixed field of ker and thus assume that

$$G_K \to \mathrm{GL}_d(k_F)$$

is the trivial representation.

It follows that ρ actually maps G_K into the above kernel. But we know that this kernel is pro-l (see Lecture 3, Section 2). In particular, since $\mathcal{P}_K \subseteq G_K$ is pro-p, it must vanish under ρ. Thus we have shown that ρ factors through $G_K/\mathcal{P}_K = T_K$.

We can also extend K so that all of the eigenvalues of τ (acting on V) lie in K. The image of $\mathcal{I}_K$ in T_K is just Δ_k, where k is the residue field of $\mathcal{O}_K$. Δ_k is (topologically) generated by τ^e, where τ is a topological generator of $\Delta_{\mathbb{F}_p}$ and e is the tame inertial degree of $K/\mathbb{Q}_p$. We saw above that τ^n is unipotent for its action on V for some n prime to p; let L be a the unique totally tamely ramified extension of K of degree n. L is the fixed field of τ^{ne} and φ, and it follows that the image of $\mathcal{I}_L$ acting on V is unipotent. Thus $\rho|_{G_L}$ is semistable, which completes the proof. □

The above proof rested very heavily on the fact that l was distinct from p; the case where $l = p$ is very far from settled. Indeed, the above definition of semistable isn't even appropriate in this case.

2.3. Further Reductions. Suppose for now that $l \neq p$. We will now use the methods of the proof of Proposition 2.2 to get additional reductions on our representations.

Let $K/\mathbb{Q}_p$ be a finite extension and let k be the residue field of K. We have a commutative diagram with exact rows relating the groups T and T_K.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_k & \longrightarrow & T_K & \longrightarrow & \mathfrak{g}_k & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \Delta_{\mathbb{F}_p} & \longrightarrow & T & \longrightarrow & \mathfrak{g} & \longrightarrow & 1 \end{array}$$

Here $\mathfrak{g}_k$ is the absolute Galois group of k. The index of Δ_k in $\Delta_{\mathbb{F}_p}$ is the tame inertial degree and the index of $\mathfrak{g}_k$ in $\mathfrak{g}$ is the residue degree $[k : \mathbb{F}_p]$.

We want to consider only the pro-l part of Δ_k. More precisely, let $T_{l,K}$ be the quotient of T_K by the maximal non-pro-l subgroup of Δ_k. This reduces the exact sequence

$$1 \to \prod_{r \neq p} \mathbb{Z}_r(1) \to T_K \to \widehat{\mathbb{Z}} \to 1$$

to an exact sequence

$$1 \to \mathbb{Z}_l(1) \to T_{l,K} \to \widehat{\mathbb{Z}} \to 1.$$

The methods of Proposition 2.2 now give the following result.

PROPOSITION 2.3. *Let $\rho : G_K \to \mathrm{GL}_d(F)$ be a Galois representation with $p \neq l$. Then there exists a finite extension L/K such that $\rho|_{G_L}$ factors through $T_{l,L}$ and the image of the inertia group of L acts unipotently.*

PROOF. The proof is virtually the same as that of Proposition 1.1. □

We make one final comment on reducing the domain of Galois representations. Let $\rho : G_K \to \mathrm{GL}_d(\mathcal{O}_F)$ be a Galois representation, and consider the residual representation $\overline{\rho} : G_K \to \mathrm{GL}_d(k_F)$. Let G_K^0 be the kernel of $\overline{\rho}$; G_K^0 is the set of elements of G_K such that $\rho(g)$ is in the kernel of the natural map

$$\mathrm{GL}_d(\mathcal{O}_F) \to \mathrm{GL}_d(k_F).$$

G_K^0 is an open, normal subgroup of G_K of finite index since $\mathrm{GL}_d(k_F)$ is finite. We let $G_K^{0,l}$ be its pro-l completion; that is, $G_K^{0,l}$ is the projective limit of all finite quotients of G_K^0 of order a power of l. Since G_K^0 is already profinite, there is a natural surjection $G_K^0 \twoheadrightarrow G_K^{0,l}$; let H be the kernel:

$$1 \to H \to G_K^0 \to G_K^{0,l} \to 1.$$

ρ must vanish on H, since H is completely non-pro-l and ρ maps it into the pro-l kernel of $\mathrm{GL}_d(\mathcal{O}_F) \to \mathrm{GL}_d(k_F)$. Thus ρ factors as a map

$$G_K/H \to \mathrm{GL}_d(\mathcal{O}_F).$$

But G_K/H is simply an extension of the pro-l group $\mathrm{GL}^{0,l}$ by the finite group G_K/G_K^0. In this way one can often gain more control over the Galois representation ρ.

CHAPTER 5

Lecture 5

1. Group Cohomology

1.1. Basic Facts. Let G be a profinite group and let M be a discrete submodule of G in the usual sense that

$$M = \bigcup_{H \text{ open subgroup of } G} M^H.$$

Equivalently we could take the union over all open normal subgroups. This condition merely means that G acts on each element of M through a finite quotient. We recall that the cohomology groups of G with coefficients in M are abelian groups defined by

$$H^j(G, M) = \varinjlim_{H \lhd G} H^j(G/H, M^H)$$

where the limit is over all open normal subgroups H of G and the maps of the directed system are the inflation maps. (Note that open subgroups of G automatically have finite index, so that all of the groups G/H are finite. See [**Se-LF**, Chapter 7] for the definitions of the standard maps of cohomology groups.) There are various other equivalent definitions of these cohomology groups; for example,

$$H^j(G, M) = \mathrm{Ext}^j_{\mathbb{Z}[G]}(\mathbb{Z}, M) = \varinjlim_{H \lhd G} \mathrm{Ext}^j_{\mathbb{Z}[G/H]}(\mathbb{Z}, M^H)$$

where here one can simply consider Ext as it is usually defined for rings. The equivalence of these definitions stems from the fact that (for *profinite* G and *discrete* M; things are more complicated in general) these $H^j(G, M)$ are the right derived functors of the left exact functor

$$M \mapsto M^G,$$

where M^G is the submodule of G-invariants of M. That is,

$$M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}.$$

In particular, this shows that

$$H^0(G, M) = M^G,$$

which we note is independent of all topological considerations.

[0]Last modified September 4, 2003

1.2. The First Cohomology Group. We now turn to the first cohomology group, which is the one which we will primarily be concerned with. In this case, inflation is injective (see below), so we can actually realize $H^1(G, M)$ as a union

$$H^1(G, M) = \bigcup_{H \lhd G} H^1(G/H, M^H),$$

the union as usual over open, normal subgroups of G.

There are other somewhat more concrete descriptions of $H^1(G, M)$ as well. The most standard is to realize it as equivalence classes of crossed homomorphisms. We define a *crossed homomorphism* to be a continuous map

$$h : G \to M$$

such that

$$h(g_1 g_2) = h(g_1) + g_1 h(g_2).$$

We define $\mathrm{CrossHom}(G, M)$ to be the set of all (continuous) crossed homomorphisms from G to M. $\mathrm{CrossHom}(G, M)$ is made into an abelian group through the abelian group structure of M. We say that a crossed homomorphism $h : G \to M$ is *principal* if it has the form

$$h(g) = gm - m$$

for some fixed $m \in M$ and all $g \in G$. (Such a map is indeed continuous, thanks to our assumption that M is discrete.) It is easy to check that every such map is a crossed homomorphism. We let $\mathrm{PrincCrossHom}(G, M)$ denote the subgroup of $\mathrm{CrossHom}(G, M)$ of principal crossed homomorphisms. With these definitions, it can be shown that

$$H^1(G, M) \cong \mathrm{CrossHom}(G, M)/\,\mathrm{PrincCrossHom}(G, M);$$

see [**Se-LF**, Chapter 7, Section 3]. (In fact, if one is working with general G and M (not necessarily profinite and discrete, respectively), one usually takes this as the definition of $H^1(G, M)$; it is a theorem that in our case this agrees with the derived functor and direct limit definitions.) An element of $\mathrm{CrossHom}(G, M)$ is sometimes also called a 1-*cocycle*; an element of $\mathrm{PrincCrossHom}(G, M)$ is a 1-*coboundary*.

As an important special case of this, note that if G acts trivially on M, then

$$\mathrm{CrossHom}(G, M) = \mathrm{Hom}_{\mathbb{Z}}(G, M)$$

and

$$\mathrm{PrincCrossHom}(G, M) = 0,$$

so that

$$H^1(G, M) \cong \mathrm{Hom}_{\mathbb{Z}}(G, M).$$

Using this description, we can see directly that inflation is injective. In this setting, for N closed and normal in G, inflation is induced by the natural map

$$\mathrm{CrossHom}(G/N, M^N) \to \mathrm{CrossHom}(G, M)$$

defined by composing crossed homomorphisms with the map $G \twoheadrightarrow G/N$. (It is clear that $\mathrm{PrincCrossHom}(G/N, M^N)$ maps to $\mathrm{PrincCrossHom}(G, M)$, so that we get a well-defined map on H^1's.) To show injectivity we must check that if $h : G/N \to M^N$ is a crossed homomorphism, and if it becomes principal as a map $G \to M$, say by $h(g) = gm - m$ for some $m \in M$, then we can actually write $h(g) = gm_0 - m_0$ for some $m_0 \in M^N$. But this is easy; since h vanishes on N, we must have $nm = m$ for all $n \in N$. Thus we can take $m = m_0$, so inflation is indeed injective on H^1's.

1.3. The Basic Exact Sequence. We can actually extend our injection

$$H^1(G/N, M^N) \xhookrightarrow{\text{inf}} H^1(G, M)$$

to a longer exact sequence. We first recall how G/N acts on the cohomology group $H^1(N, M)$. Most concretely, if $h : N \to M$ is a crossed homomorphism, we define $\gamma h : N \to M$ for $\gamma \in G/N$ as follows : first choose a lifting $\tilde{\gamma} \in G$ of γ. Now define

$$\gamma h(x) = \tilde{\gamma} h(\tilde{\gamma}^{-1} x \tilde{\gamma})$$

for $x \in N$. This makes sense since N is normal, and one can check easily that it is still a crossed homomorphism. Furthermore, it is not hard to show that a different choice of $\tilde{\gamma}$ gives a crossed homomorphism which differs from γh by a principal crossed homomorphism, so that we really do get a well-defined action of G/N on $H^1(N, M)$.

There is another way to define this action which is more abstract but somewhat cleaner. Recall that $H^j(G, M)$ is contravariant in G and covariant in M. For any $\gamma \in G$, we can define maps

$$N \leftarrow N, \ M \to M$$

by sending $n \in N$ to $\gamma^{-1} n \gamma \in N$ and $m \in M$ to $\gamma m \in M$. These maps are compatible in the sense of [**Se-LF**, Chapter 7, Section 5] (this just means that the map $M \to M$ is a map of N-modules with the normal G-action on the second factor and the twisted action on the first factor) so that we get induced homomorphisms

$$H^j(N, M) \xrightarrow{\gamma} H^j(N, M)$$

for all j. This defines our G-action. However, one can check easily that the action of any $\gamma \in N$ is in fact trivial; this is done by looking at the 0^{th} level and then either using the universal property of derived functors or else a dimension shifting argument. (See [**Se-LF**, Chapter 7, Section 5, Proposition 3].) Thus we get an action of G/N on all of the $H^j(N, M)$.

We are now in a position to state the extension of our above injection. In it's simplest form it is an exact sequence

$$0 \longrightarrow H^1(G/N, M^N) \xrightarrow{\text{inf}} H^1(G, M) \xrightarrow{\text{res}} H^1(N, M)^{G/N}.$$

This can be proved directly, working with crossed homomorphisms; see [**Se-LF**, Chapter 7, Section 6]. We can get a more general result by using the full *Hochschild-Serre spectral sequence*: for N a closed normal subgroup of G and M a discrete G-module this is a second stage, first quadrant, cohomological spectral sequence

$$E_2^{pq} = H^p(G/N, H^q(N, M)) \Rightarrow H^{p+q}(G, M).$$

The exact sequence of low degree terms takes the form

$$\begin{aligned} 0 &\longrightarrow H^1(G/N; M^N) \xrightarrow{\text{inf}} H^1(G; M) \xrightarrow{\text{res}} H^1(N; M)^{G/N} \\ &\longrightarrow H^2(G/N; M^N) \xrightarrow{\text{inf}} H^2(G; M). \end{aligned}$$

For the construction of the Hochschild-Serre spectral sequence, see [**Wei**, Chapter 5]; for a proof of the above exact sequence and some generalizations, see [**Wes-IR**].

1.4. Cup Products. We briefly recall the notion of cup products; for a statement of the main properties, see [**Se-LF**, Chapter 8, Section 3]. For proofs of these properties, see [**AW**, Section 7].

Let M_1 and M_2 be A-modules, where A is some commutative ring, which are also discrete G-modules for some profinite group G. We further suppose that the action of G is A-linear; this is all equivalent to saying that M_1 and M_2 are $A[G]$-modules rather than just $\mathbb{Z}[G]$-modules. We endow the tensor product $M_1 \otimes_A M_2$ with a structure of G-module by setting $g(m_1 \otimes m_2) = gm_1 \otimes gm_2$. It is also, of course, still an A-module. The *cup product* is then a pairing

$$H^i(G, M_1) \otimes_A H^j(G, M_2) \to H^{i+j}(G, M_1 \otimes_A M_2).$$

We will usually write $m_1 \cup m_2$ for the cup product of $m_1 \in H^i(G, M_1)$ and $m_2 \in H^j(G, M_2)$.

Often one takes cup products in a situation where there is also a natural map

$$M_1 \otimes_A M_2 \to M_3$$

for some $A[G]$-module M_3, in which case we can consider the natural map

$$H^i(G, M_1) \otimes_A H^j(G, M_2) \to H^{i+j}(G, M_3)$$

induced by cup product and the above map.

2. Galois Cohomology

2.1. Torsors for Finite G_K-modules. For this section we fix a field K and let $G_K = \mathrm{Gal}(K_s/K)$ be its absolute Galois group. We further assume that M is a *finite* G_K-module. (M is also assumed to be discrete and the action continuous, of course.) We will refer to finite sets on which G_K acts as G_K*-sets*. What we say below is actually true for general groups, but we will confine ourself to the case of G_K.

Definition 2. An M*-torsor* is a G_K-set T together with a G_K-equivariant principal homogeneous action of M,

$$\alpha : M \times T \to T.$$

We will write $\alpha(m, t)$ as $m + t$, and by G_K-equivariance we mean that $g(m + t) = gm + gt$. Recall that a principal homogeneous action is one which is simply transitive; that is, for any fixed $t_0 \in T$, the map

$$M \to T$$

given by sending m to $m + t_0$ is a bijection.

Thus an M-torsor is a G_K-set which looks exactly like M, except that it isn't itself an abelian group; by choosing a t_0 to act as the identity it can be made into one. So an M-torsor is a "copy" of M without a distinguished identity element.

There are other ways to describe M-torsors which can be somewhat more illuminating. For each $t_0 \in T$ we get a commutative diagram

$$\begin{array}{ccc} M \times T & \xrightarrow{\alpha} & T \\ \cong\uparrow & & \uparrow\cong \\ M \times M & \longrightarrow & M \end{array}$$

where the bottom map is just the group law on M, the first vertical isomorphism sends (m_1, m_2) to $(m_1, m_2 + t_0)$ and the second vertical isomorphism sends m to $m + t_0$. This diagram expresses both the fact that α is a group action and that it is principal homogeneous.

Combining all of these diagrams over T, we get a diagram

$$\begin{array}{ccc} (M \times T) \times T & \xrightarrow{\alpha \times 1} & (T) \times T \\ \cong \uparrow & & \uparrow \cong \\ (M \times M) \times T & \longrightarrow & (M) \times T \end{array}$$

where all of the maps on the last T-factor are the identity, and the vertical maps now send (m_1, m_2, t) to $(m_1, m_2 + t, t)$ and (m, t) to $(m + t, t)$.

Considering the last T factor as a sort of parameter space for the other commutative diagrams, it might make somewhat more sense to write the previous diagram as

$$\begin{array}{ccc} (M \times T)_T & \xrightarrow{\alpha} & T_T \\ \cong \uparrow & & \uparrow \cong \\ (M \times M)_T & \longrightarrow & M_T \end{array}$$

2.2. Connetions between Torsors and $H^1(G, M)$. We first recall that it is possible to put a group structure on the set of M-torsors. Let T_1 and T_2 be two M-torsors. Consider the finite set $T_1 \times T_2$ with its natural product G_K-action. $M \times M$ acts naturally on $T_1 \times T_2$, and we define an equivalence relation on $T_1 \times T_2$ by decreeing that

$$(t_1, t_2) \sim (t_1 + m, t_2 - m)$$

for all $m \in M$. We define the *Baer sum* $T_1 \odot T_2$ of T_1 and T_2 to be the quotient of $T_1 \otimes T_2$ by this equivalence relation. One can easily check that $T_1 \odot T_2$ is actually an M-torsor, with its M-action defined by having M act on the first factor but not the second.

We are now in a position to state our main theorem on torsors. We say that two M-torsors T_1 and T_2 are isomorphic as M-torsors if there is na isomorphism of G_K-sets between them commuting with the action of M.

THEOREM 2.1. *$H^1(G_K, M)$ is naturally isomorphic to the set of M-torsors up to isomorphism of M-torsors. It is in fact an isomorphism of groups where the M-torsors are made into a group by the Baer sum.*

PROOF. This is actually fairly easy. One uses the identification

$$H^1(G_K, M) = \varinjlim_{H \lhd G} \operatorname{Ext}^1_{\mathbb{Z}[G_K/H]}(\mathbb{Z}, M^H),$$

together with the description of this group as isomorphism classes of extensions

$$0 \to M \to \varepsilon \to \mathbb{Z} \to 0.$$

Given such an extension, the corresponding torsor is simply the inverse image of $1 \in \mathbb{Z}$ in ε. We leave the details to the reader. □

Recall that the category of G_K-sets is equivalent to the category of étale algebras over K. (An *étale algebra* is one which is flat and unramified; see [**Mi-EC**, Chapter 1, Section 3, p. 21] for the definition of an unramified algebra.) In the case that G_K acts trivially on M, we have that

$$H^1(G_K, M) \cong \mathrm{Hom}_{\mathrm{cts}}(G_K, M)$$

classifies étale algebras over K with M-action. If the homomorphism $G_K \to M$ is actually surjective, then it corresponds to a field extension L/K with Galois group M.

2.3. Torsors for Algebraic Groups. There is a similar theory of torsors for algebraic groups. We replace M by an algebraic group Γ defined over K (recall that an *algebraic group* is an algebraic variety with a group structure such that the multiplication and inversion maps are actually morphisms of algebraic varieties and the identity is K-rational), and for simplicity we assume that Γ is smooth as an algebraic variety over K. With appropriate definitions everything we say can be generalized to the case where Γ is non-commutative, but we will concentrate on the commutative case. (Note that if Γ is non-commutative we haven't even defined the cohomology set (it isn't a group in this generality) $H^1(G_K, \Gamma(K_s))$.)

In this setting, a Γ-torsor T is an algebraic variety over K together with a morphism

$$\Gamma \times T \xrightarrow{\alpha} T$$

satisfying the same conditions as our map α above. Specifically, we have a diagram

$$\begin{array}{ccc} (\Gamma \times T) \times T & \xrightarrow{\alpha \times 1} & (T) \times T \\ {\scriptstyle u}\uparrow{\scriptstyle \cong} & & {\scriptstyle \cong}\uparrow{\scriptstyle v} \\ (\Gamma \times \Gamma) \times T & \longrightarrow & (\Gamma) \times T \end{array}$$

where the bottom map is the multiplication morphism on Γ and the identity on T,

$$u = \mathrm{id} \times \alpha \times \mathrm{id}$$

(where α operates on the last two factors $\Gamma \times T$) and

$$v = \alpha \times \mathrm{id}\,.$$

On points,

$$u(\gamma_1, \gamma_2, t) = (\gamma_1, \gamma_2 + t, t)$$

and

$$v(\gamma, t) = (\gamma + t, t).$$

It follows from this definition that T is isomorphic to K over $\bar{K}$ (it might not be isomorphic over K since it might not even have any points defined over K), so T is necessarily smooth. Also, we can define a Baer sum in an analagous way to that used previously.

We have in this setting the following analogue of Theorem 2.1.

THEOREM 2.2 (Grothendieck). *If Γ is a smooth algebraic group over K, then $H^1(G_K, \Gamma(K_s))$ is naturally isomorphic to the group of Γ-torsors (defined over K) up to isomorphism.*

PROOF. The proof of this theorem is quite difficult, in contrast to the fairly immediate proof of Theorem 2.1. The fact that Γ is smooth is absolutely essential; if Γ isn't smooth, then we must allow flat coverings rather than merely étale coverings. For a proof in the much easier case that Γ is an elliptic curve, see [**Si-AEC**, Chapter 10, Theorem 3.6]. □

2.4. The Local Invariant. We now consider the algebraic group $\mathbb{G}_{\mathrm{m}}$ over a local field K (in our usual sense). More accurately, we will fix an algebraic closure $\bar{K}$ of K and consider the attached G_K-module $\bar{K}^*$. We will denote its torsion subgroup by $\mu(\bar{K})$; it is just the group of roots of unity of $\bar{K}^*$.

In this setting we have the following fundamental theorem of local class field theory.

THEOREM 2.3. *Let K be a local field. Then there is a canonical isomorphism* inv*, called the invariant map,*

$$H^2(G_K, \mu(\bar{K}^*)) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}.$$

PROOF. See [**Se-LF**, Chapter 13, Section 3]. This theorem is often stated as

$$H^2(G_K, \bar{K}^*) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z},$$

but either form can easily be obtained from the other. □

In this section we will use our knowledge of the structure of G_K to compute the l-adic component of $H^2(G_K, \mu(\bar{K}^*))$; that is, we will show that $H^2(G_K, \mu_{l^\infty}(\bar{K}^*))$ is canonically isomorphic to $\mathbb{Q}_l/\mathbb{Z}_l$, at least in the case $l \neq p$, where p is the characteristic of the residue field of K. Here $\mu_{l^\infty}(\bar{K}^*)$ is the group of l-power roots of unity in $\bar{K}^*$.

Our main tools will be the Hochschild-Serre spectral sequence and the following lemma.

LEMMA 2.4. *Let G be a pro-p group and let M be a discrete G-module in which each element is killed by a power of l. If $p \neq l$, then for all $j \geq 1$,*

$$H^j(G, M) = 0.$$

PROOF. Recall that

$$H^j(G, M) = \varinjlim_{H \lhd G} H^j(G/H, M^H),$$

the direct limit being over the open, normal subgroups of G. Choose an element $x \in H^j(G/H, M^H)$ and let $c : (G/H)^j \to M^H$ be a j-cocyle representing x. (See [**Se-LF**, Chapter 7, Section 3].) Since G/H is finite, c takes on only finitely many values in M^H. Thus there must be some $n \geq 0$ such that $l^n c = 0$, and therefore $l^n x = 0$. But G/H has order p^m for some m, so $p^m x = 0$ by [**Se-LF**, Chapter 8, Section 2, Corollary 1]. Since $l \neq p$, we thus must have $x = 0$. So every group in the direct limit is 0, and $H^j(G, M) = 0$ as well. □

We will use various exact sequences from Lecture 4, Sections 1.3 and 2.3. First, we have an exact sequence

$$1 \to \mathcal{P}_K \to G_K \to T_K \to 1$$

where $\mathcal{P}_K$ is a p-group. The Hochschild-Serre spectral sequence for this exact sequence collapses to the bottom row by Lemma 2.4, since $\mathcal{P}_K$ is pro-p. Thus we get an isomorphism

$$H^2(G_K, \mu_{l^\infty}(\bar{K}^*)) \cong H^2(T_K, \mu_{l^\infty}(\bar{K}^*)).$$

Next we recall that we have an exact sequence

$$1 \to \prod_{r \neq p,l} \mathbb{Z}_r(1) \to T_K \to T_{l,K} \to 1.$$

Since $\prod_{r\neq p,l} \mathbb{Z}_r(1)$ has no pro-l component, the same argument as above shows that

$$H^2(T_K, \mu_{l^\infty}(\bar{K}^*)) \cong H^2(T_{l,K}, \mu_{l^\infty}(\bar{K}^*)),$$

and thus that

$$H^2(G_K, \mu_{l^\infty}(\bar{K}^*)) \cong H^2(T_{l,K}, \mu_{l^\infty}(\bar{K}^*)).$$

Next we use the exact sequence

$$1 \to \mathbb{Z}_l(1) \to T_{l,K} \to \widehat{\mathbb{Z}} \to 1.$$

This time the Hochschild-Serre spectral sequence is entirely zero outside of the bottom left 2×2 square, since $\widehat{\mathbb{Z}}$ and $\mathbb{Z}_l(1)$ cohomology vanish on torsion modules in all dimensions greater than or equal to 2. (See [**Se-LF**, Chapter 13, Section 1, Proposition 2].) From this we get an isomorphism

$$H^2(G_K, \mu_{l^\infty}(\bar{K}^*)) \cong H^1\big(\widehat{\mathbb{Z}}, H^1(\mathbb{Z}_l(1), \mu_{l^\infty}(\bar{K}^*))\big).$$

Since $l \neq p$, $\mu_{l^\infty}(\bar{K}) \subseteq K^{\mathrm{ur}}$, so $\mathbb{Z}_l(1)$ (which at the moment lies in the inertia group) acts trivially on it. Thus,

$$H^1(\mathbb{Z}_l(1), \mu_{l^\infty}(\bar{K}^*)) = \mathrm{Hom}(\mathbb{Z}_l(1), \mu_{l^\infty}(\bar{K}^*)) = \mathrm{Hom}(\mathbb{Z}_l, \mathbb{Q}_l/\mathbb{Z}_l) \cong \mathbb{Q}_l/\mathbb{Z}_l,$$

since as abelian groups $\mathbb{Z}_l(1)$ is just $\mathbb{Z}_l$ and $\mu_{l^\infty}(\bar{K}^*)$ is just $\mathbb{Q}_l/\mathbb{Z}_l$. (All Hom-groups are continuous homomorphisms, of course.) In fact, $H^1(\mathbb{Z}_l(1), \mu_{l^\infty}(\bar{K}^*))$ even has trivial $\widehat{\mathbb{Z}} = \mathrm{Gal}(K^{\mathrm{ur}}/K)$-action, since $\widehat{\mathbb{Z}}$ acts via the l-cyclotomic character on each and the actions cancel. Thus,

$$H^1\big(\widehat{\mathbb{Z}}, H^1(\mathbb{Z}_l(1), \mu_{l^\infty}(\bar{K}^*))\big) = \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}_l/\mathbb{Z}_l) \cong \mathbb{Q}_l/\mathbb{Z}_l.$$

Thus, as promised, we have shown that

$$H^2(G_K, \mu_{l^\infty}(\bar{K}^*)) \cong \mathbb{Q}_l/\mathbb{Z}_l.$$

Of course, this is not yet the full determination of the invariant map. Most importantly, we have not computed the p-part; our methods above would be completely ineffective in that case.

3. Tate Local Duality

Let K be a local field and let M be a finite discrete G_K-module. We define the *Pontrjagin dual* $M^\vee$ of M by

$$M^\vee = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z}),$$

with the usual adjoint G_K-action. We further define the *Cartier dual* M^* by

$$M^* = \mathrm{Hom}(M, \mu(\bar{K}^*)),$$

again with the adjoint G_K-action. $M^\vee$ and M^* are isomorphic as abelian groups, but not as G_K-modules, and in both cases the double dual is simply M.

Pontrjagin duality is simply the obvious assertion that there is a natural, G_K-equivariant, perfect pairing

$$M \otimes M^\vee \to \mathbb{Q}/\mathbb{Z}.$$

Similarly, Cartier duality is the assertion that there is a natural G_K-equivariant perfect pairing

$$M \otimes M^* \to \mu(\bar{K}^*).$$

Tate local duality is essentially the extension of Cartier duality to cohomology groups.

THEOREM 3.1 (Tate Local Duality). *Let K and M be as above. Then, for all i, $H^i(G_K, M)$ is finite, and there are perfect pairings*

$$H^i(G_K, M) \otimes H^{2-i}(G_K, M^*) \to \mathbb{Q}/\mathbb{Z}$$

induced by cup product, Cartier duality and the invariant map.

PROOF. See [**Mi-ADT**, Chapter 1, Section 2]. □

CHAPTER 6

Lecture 6

1. Duality Preliminaries

1.1. Pontrjagin Duality. As always, let K be a local field with residue field k of characteristic p. Let G_K and $\mathfrak{g}_k$ be the absolute Galois groups $\mathrm{Gal}(\bar{K}/K)$ and $\mathrm{Gal}(\overline{k}/k)$ respectively. We let M be a finite G_K-module (where the G_K-action is continuous with respect to the discrete topology on M, of course).

We define two duals of M. The first is the *Pontrjagin dual*

$$M^\vee = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}),$$

the Hom being as abelian groups. $M^\vee$ receives the usual adjoint G_K-action; in this case, since G_K acts trivially on $\mathbb{Q}/\mathbb{Z}$, this means that for any $f : M \to \mathbb{Q}/\mathbb{Z}$ and $\sigma \in G_K$, $\sigma f : M \to \mathbb{Q}/\mathbb{Z}$ is given by

$$(\sigma f)(m) = f(\sigma^{-1} m)$$

for all $m \in M$. There is a natural perfect pairing of abelian groups

$$M \otimes_{\mathbb{Z}} M^\vee \to \mathbb{Q}/\mathbb{Z},$$

given by

$$m \otimes f \mapsto f(m)$$

for $m \in M$ and $f \in M^\vee$. (Recall that for a pairing $M \otimes_A N \to P$ to be *a perfect pairing of A-modules* means that the induced maps

$$M \to \mathrm{Hom}_A(N, P)$$

and

$$N \to \mathrm{Hom}_A(M, P)$$

are isomorphisms.) The pairing is perfect in this case because M is a finite abelian group, and thus (loosely speaking) every element of M can find something in $\mathbb{Q}/\mathbb{Z}$ to map to. In fact, if $M \otimes M^\vee$ is given the usual induced G_K-action, one easily checks that this pairing, and thus the induced maps as well, are G_K-equivariant. Note also that $(M^\vee)^\vee$ is canonically isomorphic to M as G_K-modules.

Now, let H be an arbitrary subgroup of G_K. Then M is an H-module in the obvious way, and one easily checks directly from the definitions that $(M^H)^\vee = (M^\vee)_H$ and $(M_H)^\vee = (M^\vee)^H$, where M^H and M_H are the H-invariants and coinvariants respectively. (These two equalities are actually formally equivalent; simply replace M by $M^\vee$ in either to get the other one.) Put differently, our above perfect pairing "restricts" to perfect pairings

$$M^H \otimes (M^\vee)_H \to \mathbb{Q}/\mathbb{Z}$$

[0]Last modified September 4, 2003

and

$$M_H \otimes (M^\vee)^H \to \mathbb{Q}/\mathbb{Z}.$$

1.2. Cartier Duality. The *Cartier dual* of M is a G_K-module M^* which is isomorphic to $M^\vee$ as abelian groups, but with a different G_K-action. Precisely, we define

$$M^* = \mathrm{Hom}_{\mathbb{Z}}(M, \mu(\bar{K})),$$

where $\mu(\bar{K})$ is the group of roots of unity in $\bar{K}$. The fact that $M^\vee \cong M^*$ (non-canonically) as abelian groups follows from the fact that there are non-canonical isomorphims $\mathbb{Q}/\mathbb{Z} \cong \mu(\bar{K})$. The difference is that $\mu(\bar{K})$ is a non-trivial G_K-module, so the induced adjoint G_K-action on M^* is different from that on $M^\vee$: for any $f : M \to \mu(\bar{K})$ and $\sigma \in G_K$, we have

$$(\sigma f)(m) = \sigma f(\sigma^{-1} m)$$

for all $m \in M$, the outside action being that of G_K on $\mu(\bar{K})$. We still have $(M^*)^* = M$ as G_K-modules.

Just as in the Pontrjagin case, we have a canonical perfect pairing

$$M \otimes_{\mathbb{Z}} M^* \to \mu(\bar{K})$$

given by evaluation. It is again easily checked to be G_K-equivariant. In this case, however, the pairing does not always restrict to subgroups. Specifically, let H be any subgroup of G_K. Then the direct argument from the definitions shows only that $(M^H)^* = (M^*)_H$ and $(M_H)^* = (M^*)^H$ if H acts trivially on $\mu(\bar{K})$. However, with a little more work we can recover these results in the following special case.

LEMMA 1.1. *Suppose that M is a finite G_K-module of prime to p order, where p is the residue characteristic of k. Then*

$$(M^{\mathcal{I}_K})^* = (M^*)_{\mathcal{I}_K}$$

and

$$(M_{\mathcal{I}_K})^* = (M^*)^{\mathcal{I}_K},$$

where $\mathcal{I}_K$ is the inertia subgroup of G_K.

PROOF. Let $\mu'(\bar{K})$ be the subgroup of $\mu(\bar{K})$ of roots of unity of prime to p order. Using the decomposition

$$\mu(\bar{K}) = \mu'(\bar{K}) \times \mu_{p^\infty}(\bar{K})$$

we get a decomposition

$$M^* = \mathrm{Hom}(M, \mu(\bar{K})) = \mathrm{Hom}(M, \mu'(\bar{K})) \times \mathrm{Hom}(M, \mu_{p^\infty}(\bar{K})),$$

and the last of these groups is zero, since M has prime to p order. Thus

$$M^* = \mathrm{Hom}(M, \mu'(\bar{K})).$$

Now, since $K(\mu'(\bar{K}))$ is unramified over K, $\mathcal{I}_K$ acts trivially on $\mu'(\bar{K})$. The usual argument now extends to this case to finish the proof. □

1.3. Tate Modules. In order to clarify the relationship between $M^\vee$ and M^* we will now present formally a subject which we have touched on before. Let l be a prime number (possibly equal to p), and let W be a l-divisible, l-torsion abelian group. Thus

$$W = \bigcup_n W[l^n],$$

where $W[l^n]$ is the l^n-torsion in W. We define a functor Ta_l from the category of such groups to the category of $\mathbb{Z}_l$-modules by defining

$$\mathrm{Ta}_l(W) = \varprojlim_n W[l^n],$$

the inverse limit being with respect to the maps

$$W[l^{n+1}] \xrightarrow{l} W[l^n]$$

given by multiplication by l. These are surjective since W is l-divisible. $\mathrm{Ta}_l(W)$ is a $\mathbb{Z}_l$-module since each $W[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module. In fact, if $W[l]$ is finite, then it follows easily that $\mathrm{Ta}_l(W)$ is a free $\mathbb{Z}_l$-module of finite rank equal to $|W[l]|/l$. (The relevant structure of W is actually determined by $W[l]$, as can be seen just by staring at it for a moment.) It is also easy to see that if W is a G_K-module, then $\mathrm{Ta}_l(W)$ is also a G_K-module. However, it is not true that $\mathrm{Ta}_l(W)$ need be discrete, even if W was.

The canonical example is, of course,

$$\mathrm{Ta}_l(\mathbb{Q}_l/\mathbb{Z}_l) = \mathbb{Z}_l;$$

it follows immediately that

$$\mathrm{Ta}_l\big((\mathbb{Q}_l/\mathbb{Z}_l)^r\big) = \mathbb{Z}_l^r,$$

the free $\mathbb{Z}_l$-module of rank r. Since $\mu_{l^\infty}(\bar{K})$ is isomorphic to $\mathbb{Q}_l/\mathbb{Z}_l$ as abelian groups, $\mathrm{Ta}_l(\mu_{l^\infty}(\bar{K}))$ must be a free $\mathbb{Z}_l$-module of rank 1. In fact, one checks easily (since all of the G_K-actions involved essentially come from $\mu_{l^\infty}(\bar{K})$) that

$$\mathrm{Ta}_l(\mu_{l^\infty}(\bar{K})) \cong \mathbb{Z}_l(1).$$

(See Lecture 3, Section 3.2.) In the case $l = p$ we use this to define the module $\mathbb{Z}_p(1)$, which we had not previously defined.

If M is any pro-l G_K-module, we define its (first) *Tate twist* by

$$M(1) = M \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(1).$$

More generally, we define inductively

$$M(n) = M(n-1) \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(1)$$

for any positive integer n. We also define

$$\mathbb{Z}_l(-1) = \mathrm{Hom}_{\mathbb{Z}_l}(\mathbb{Z}_l(1), \mathbb{Z}_l),$$

where the $\mathbb{Z}_l$ in the range has trivial G_K-action and correspondingly

$$M(-1) = M \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(-1) = \mathrm{Hom}_{\mathbb{Z}_l}(\mathbb{Z}_l(1), M)$$

and

$$M(n) = M(n+1) \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(-1)$$

for any negative integer n. One checks immediately that

$$\mathbb{Z}_l(n_1) \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(n_2) = \mathbb{Z}_l(n_1 + n_2)$$

for any integers n_1 and n_2.

This entire theory generalizes to the case where one considers all primes l at once. Specifically, we define a functor Ta from torsion, divisible groups to $\widehat{\mathbb{Z}}$-modules (which are just profinite abelian groups) by

$$\mathrm{Ta}(W) = \varprojlim_N W[N],$$

where the maps of the inverse system are the multiplication by m maps

$$W[mN] \xrightarrow{m} W[N];$$

these are surjective since W is divisible. As above, $\mathrm{Ta}(W)$ inherits a G_K-action from W if W is a G_K-module.

As an example, we find

$$\mathrm{Ta}(\mathbb{Q}/\mathbb{Z}) = \widehat{\mathbb{Z}}$$

canonically, and

$$\mathrm{Ta}(\mu(\bar{K})) = \prod_{l \text{ prime}} \mathbb{Z}_l(1)$$

which we will denote simply $\widehat{\mathbb{Z}}(1)$. Suppressing the p-part, we find that we have essentially recovered the Galois group Δ_k.

If M is any profinite G_K-module, we define its (first) *Tate twist* to be

$$M(1) = M \otimes_{\widehat{\mathbb{Z}}} \widehat{\mathbb{Z}}(1).$$

Also defining

$$M(-1) = \mathrm{Hom}_{\widehat{\mathbb{Z}}}(\widehat{\mathbb{Z}}(1), M),$$

we proceed as above to get G_K-modules $M(n)$ for all integers n. In the case that M is pro-l it is easy to check that these definitions agree with our earlier ones.

It is immediate from these definitions that if M is any finite G_K-module, the Pontrjagin and Cartier duals are related by

$$M^* = M^\vee(1).$$

1.4. Cohomology of Topologically Cyclic Profinite Groups. Let C be a profinite group which is (not necessarily canonically) isomorphic to

$$\prod_{l \in \mathcal{L}} \mathbb{Z}_l$$

for some set of prime numbers $\mathcal{L}$. Let M be a finite discrete C-module, with continuous C-action. If C were actually canonically isomorphic to the product of $\mathbb{Z}_l$'s, meaning that it has a chosen generator γ, then there is a canonical isomorphism

$$H^1(C, M) = M_C = M/(\gamma - 1)M,$$

given by sending a cocycle $\varphi : C \to M$ to $\varphi(\gamma)$. (This adapts easily from [**Se-LF**, Chapter 13, Section 1].) In the case where C has no chosen generator, we can still obtain a canonical isomorphism via the map

$$C \otimes_{\widehat{\mathbb{Z}}} H^1(C, M) \to M_C$$

given by sending a pair $c \otimes \varphi$ of an element of C and a cocycle to the class of $\varphi(c)$ in M_C. That this is an isomorphism follows easily either from the fact that the non-canonical version is, or else it can also be seen easily from the finite cyclic case.

One can actually "solve" for $H^1(C, M)$ in the above equation in the case where M has order divisible only by primes in $\mathcal{L}$. Simply take the tensor product of both sides with $\mathrm{Hom}_{\widehat{\mathbb{Z}}}(C, \prod_{l\in\mathcal{L}} \mathbb{Z}_l)$. This yields an isomorphism

$$H^1(C, M) = \mathrm{Hom}_{\widehat{\mathbb{Z}}}(C, M_C),$$

since $\mathrm{Hom}_{\widehat{\mathbb{Z}}}(C, \prod_{l\in\mathcal{L}} \mathbb{Z}_l) \otimes_{\widehat{\mathbb{Z}}} C = \prod_{l\in\mathcal{L}} \mathbb{Z}_l$.

2. Tate Local Duality

2.1. An Example : Local Class Field Theory. We keep the notation of the last section. Recall that Tate local duality states that the cohomology groups $H^1(G_K, M)$ and $H^1(G_K, M^*)$ are finite, and that there is a perfect pairing

$$H^1(G_K, M) \otimes H^1(G_K, M^*) \to \mathbb{Q}/\mathbb{Z}$$

given by cup product, Cartier duality and the local invariant map. (See Lecture 5, Section 3.)

We begin by working through the implications in an example. Let N be a positive integer and set $M = \mathbb{Z}/N\mathbb{Z}$, with trivial G_K-action. Then

$$M^* = \mathrm{Hom}(\mathbb{Z}/N\mathbb{Z}, \mu(\bar{K})) = \mathrm{Hom}(\mathbb{Z}/N\mathbb{Z}, \mu_N(\bar{K})) = \mu_N(\bar{K}),$$

where $\mu_N(\bar{K})$ is the group of N^{th} roots of unity in $\bar{K}$. Thus in this case Tate local duality gives a perfect pairing

$$H^1(G_K, \mathbb{Z}/N\mathbb{Z}) \otimes H^1(G_K, \mu_N(\bar{K})) \to \mathbb{Q}/\mathbb{Z};$$

in fact, the image must land in $\frac{1}{N}\mathbb{Z}/\mathbb{Z}$, since both groups are N-torsion. Since $\mathbb{Z}/N\mathbb{Z}$ has trivial G_K-action, the first of these cohomology groups is given by

$$H^1(G_K, \mathbb{Z}/N\mathbb{Z}) = \mathrm{Hom}(G_K, \mathbb{Z}/N\mathbb{Z}) = \mathrm{Hom}(G_K^{\mathrm{ab}}, \mathbb{Z}/N\mathbb{Z}).$$

We can compute $H^1(G_K, \mu_N(\bar{K}))$ using Kummer theory. We begin with the exact sequence of G_K-modules

$$0 \to \mu_N(\bar{K}) \to \bar{K}^* \xrightarrow{N} \bar{K}^* \to 0.$$

The long exact sequence of cohomology gives us an exact sequence

$$0 \to K^*/(K^*)^N \to H^1(G_K, \mu_N(\bar{K})) \to H^1(G_K, \bar{K}^*)[N] \to 0.$$

But $H^1(G_K, \bar{K}^*) = 0$ by Hilbert's Theorem 90. (See [**Se-LF**, Chapter 10, Section 1, Proposition 2]. Alternatively, if one thinks of $H^1(G_K, \bar{K}^*)$ as classifying isomorphism classes of one-dimensional K-vector spaces which become isomorphic over $\bar{K}$, the result is clear, since isomorphism classes of vector spaces are completely determined by dimension.) Thus

$$K^*/(K^*)^N \xrightarrow{\sim} H^1(G_K, \mu_N(\bar{K}^*)).$$

Combining these results, we have a perfect pairing

$$\mathrm{Hom}(G_K^{\mathrm{ab}}, \mathbb{Z}/N\mathbb{Z}) \otimes K^*/(K^*)^N \to \mathbb{Q}/\mathbb{Z}.$$

Equivalently, we have an isomorphism

$$\mathrm{Hom}(G_K^{\mathrm{ab}}, \mathbb{Z}/N\mathbb{Z}) \cong \mathrm{Hom}(K^*/(K^*)^N, \mathbb{Q}/\mathbb{Z}).$$

Taking the direct limit over N yields

$$\mathrm{Hom}(G_K^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(\widehat{K^*}, \mathbb{Q}/\mathbb{Z}),$$

where $\widehat{K^*}$ is the profinite completion of K^*. (K^* is not already complete; it is isomorphic to $\mathcal{U} \times \mathbb{Z}$, where $\mathcal{U}$ is the group of units. $\mathcal{U}$ is complete, but $\mathbb{Z}$ is not.) Taking Pontrjagin duals finally yields the isomorphism

$$G_K^{\mathrm{ab}} \cong \widehat{K^*}.$$

Thus we have obtained the main isomorphism of local class field theory from Tate local duality. However, there are two flaws with this approach. First, local class field theory is an essential ingredient in most proofs of Tate local duality, so the argument is circular. (In fact, in spirit a good deal of the content of the proof of Tate local duality consists in compiling the known reciprocity isomorphisms of local class field theory.) Second, it would require a lot of effort to relate the above computation to the usual reciprocity isomorphism, which is a key ingredient of the theory.

2.2. Restrictions of Tate Local Duality : First Attempt. We now make two assumptions on the finite G_K-module M. First, we assume that it is of prime to p order. Second, we assume that the G_K-action on M is at worst tamely ramified; that is, we assume that the wild ramification group $\mathcal{P}_K$ acts trivially on M. Thus G_K acts on M through $G_K/\mathcal{P}_K = T_K$, in our usual notation.

We will refer to the inflation-restriction exact sequence

$$0 \to H^1(\mathfrak{g}_k, M^{\mathcal{I}_K}) \to H^1(G_K, M) \to H^1(\mathcal{I}_K, M)^{\mathfrak{g}_k} \to 0$$

as the *basic exact sequence*. (It is exact on the right since $H^2(\mathfrak{g}_k, M^{\mathcal{I}_K}) = 0$, as M is torsion.) We are interested in relating this exact sequence with Tate local duality.

Recall that we have an exact sequence

$$1 \to \Delta_k \to T_K \to \mathfrak{g}_k \to 1,$$

where Δ_k is the image of $\mathcal{I}_K$ in T_K. We claim that we have an isomorphism

$$H^1(\Delta_k, M) \cong H^1(\mathcal{I}_K, M).$$

To see this, we simply write down a portion of the inflation-restriction sequence associated to the exact sequence

$$1 \to \mathcal{P}_K \to \mathcal{I}_K \to \Delta_k \to 1;$$

specifically, consider

$$0 \to H^1(\Delta_k, M^{\mathcal{P}_K}) \to H^1(\mathcal{I}_K, M) \to H^1(\mathcal{P}_K, M).$$

By Lecture 5, Lemma 2.4, $H^1(\mathcal{P}_K, M) = 0$ since $\mathcal{P}_K$ is pro-p and M has prime to p order. Since by hypothesis $\mathcal{P}_K$ acts trivially on M, we obtain the desired isomorphism.

Thus we can rewrite our basic exact sequence as

$$0 \to H^1(\mathfrak{g}_k, M^{\Delta_k}) \to H^1(G_K, M) \to H^1(\Delta_k, M)^{\mathfrak{g}_k} \to 0.$$

We now use the results of Section 1.4 to compute the outside terms. Since $\mathfrak{g}_k \cong \widehat{\mathbb{Z}}$ canonically, we have a canonical isomorphism

$$H^1(\mathfrak{g}_k, M^{\Delta_k}) \cong (M^{\Delta_k})_{\mathfrak{g}_k}.$$

Since $\Delta_k \cong \prod_{l\neq p} \mathbb{Z}_l(1)$ and M has prime to p order, we have a canonical isomorphism

$$H^1(\Delta_k, M)^{\mathfrak{g}_k} \cong \mathrm{Hom}(\Delta_k, M_{\Delta_k})^{\mathfrak{g}_k} \cong \mathrm{Hom}\left(\prod_{l\neq p} \mathbb{Z}_l(1), M_{\Delta_k}\right)^{\mathfrak{g}_k} \cong \left(M_{\Delta_k}(-1)\right)^{\mathfrak{g}_k}.$$

Our basic exact sequence now takes the form

$$0 \to (M^{\Delta_k})_{\mathfrak{g}_k} \to H^1(G_K, M) \to \left(M_{\Delta_k}(-1)\right)^{\mathfrak{g}_k} \to 0.$$

We now rewrite the Pontrjagin dual of our basic exact sequence together with the basic exact sequence for M^*.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \left(\left(M_{\Delta_k}(-1)\right)^{\mathfrak{g}_k}\right)^\vee & \longrightarrow & H^1(G_K, M)^\vee & \longrightarrow & \left((M^{\Delta_k})_{\mathfrak{g}_k}\right)^\vee & \longrightarrow & 0 \\ & & & & \cong\uparrow & & & & \\ 0 & \longrightarrow & \left((M^*)^{\Delta_k}\right)_{\mathfrak{g}_k} & \longrightarrow & H^1(G_K, M^*) & \longrightarrow & \left((M^*)_{\Delta_k}(-1)\right)^{\mathfrak{g}_k} & \longrightarrow & 0 \end{array}$$

The vertical isomorphism is induced by Tate duality. Now, we claim that the other two vertical pairs of groups are isomorphic. For example,

$$\begin{aligned} \left((M^*)^{\Delta_k}\right)_{\mathfrak{g}_k} &= \left(\left(M^\vee(1)\right)^{\Delta_k}\right)_{\mathfrak{g}_k} \\ &= \left(\left((M(-1))^\vee\right)^{\Delta_k}\right)_{\mathfrak{g}_k} \\ &= \left(\left(M(-1)_{\Delta_k}\right)^\vee\right)_{\mathfrak{g}_k} \\ &= \left(\left(M(-1)_{\Delta_k}\right)^{\mathfrak{g}_k}\right)^\vee \\ &= \left(\left(M_{\Delta_k}(-1)\right)^{\mathfrak{g}_k}\right)^\vee. \end{aligned}$$

Here we have used some easy isomorphisms together with some already mentioned in Section 1.1. This shows that the first two terms are isomorphic, and the last two are done in a similar way.

One should note, however, that there is absolutely no apparent reason why these isomorphisms should make the above diagram commutative. We will state what will be useful to us as a proposition.

PROPOSITION 2.1. *With K, k and M as above, the groups $H^1(\mathfrak{g}_k, M^{\mathcal{I}_K})$ and $H^1(\mathcal{I}_K, M^*)^{\mathfrak{g}_k}$ have the same order. Similarly, $H^1(\mathcal{I}_K, M)^{\mathfrak{g}_k}$ and $H^1(\mathfrak{g}_k, (M^*)^{\mathcal{I}_K})$ have the same order.*

PROOF. This follows immediately from the isomorphisms constructed above, after translating back into the language of cohomology. Note that the fact that these groups are all finite follows from the statement of Tate duality. □

2.3. Restrictions of Tate Duality : Second Attempt. We keep the same assumptions on M. We can now use the results we obtained above to relate Tate local duality to our basic exact sequences

$$0 \to H^1(\mathfrak{g}_k, M^{\mathcal{I}_K}) \to H^1(G_K, M) \to H^1(\mathcal{I}_K, M)^{\mathfrak{g}_k} \to 0$$

and

$$0 \to H^1(\mathfrak{g}_k, (M^*)^{\mathcal{I}_K}) \to H^1(G_K, M^*) \to H^1(\mathcal{I}_K, M^*)^{\mathfrak{g}_k} \to 0.$$

We claim that under the Tate pairing

$$H^1(G_K, M) \otimes H^1(G_K, M^*) \to \mathbb{Q}/\mathbb{Z},$$

$H^1(\mathfrak{g}_k, M^{\mathcal{I}_K})$ and $H^1(\mathfrak{g}_k, (M^*)^{\mathcal{I}_K})$ are orthogonal. To see this consider the commutative diagram

$$\begin{array}{ccc}
H^1(\mathfrak{g}_k, M^{\mathcal{I}_K}) \otimes H^1(\mathfrak{g}_k, (M^*)^{\mathcal{I}_K}) & \xrightarrow{\inf \otimes \inf} & H^1(G_K, M) \otimes H^1(G_K, M^*) \\
\downarrow & & \downarrow \\
H^2(\mathfrak{g}_k, M^{\mathcal{I}_K} \otimes (M^*)^{\mathcal{I}_K}) & & H^2(G_K, M \otimes M^*) \\
\downarrow & & \downarrow \\
H^2(\mathfrak{g}_k, \mu(\overline{k})) & \xrightarrow{\inf} & H^2(G_K, \mu(\bar{K})) \\
 & & \downarrow \\
 & & \mathbb{Q}/\mathbb{Z}
\end{array}$$

where the first vertical map in the second column is induced by the inclusions $M^{\mathcal{I}_K} \hookrightarrow M$ and $(M^*)^{\mathcal{I}_K} \hookrightarrow M^*$ and the rest of that column gives the Tate pairing. Note that since M has prime to p order we really do only need to consider $\mu(\overline{k})$. But $H^2(\mathfrak{g}_k, \mu(\overline{k})) = 0$, so for $H^1(\mathfrak{g}_k, M^{\mathcal{I}_K})$ and $H^1(\mathfrak{g}_k, (M^*)^{\mathcal{I}_K})$ the pairing factors through 0; thus they are orthogonal under the Tate pairing, as claimed.

This orthogonality together with Proposition 2.1 implies the following fundamental theorem.

THEOREM 2.2. *Let K be a local field with residue field k. Let M be a finite tamely ramified G_K-module of prime to p order. Then under Tate local duality, $H^1(\mathfrak{g}_k, M)$ and $H^1(\mathcal{I}_K, M^*)^{\mathfrak{g}_k}$ are orthogonal complements. Similarly, $H^1(\mathcal{I}_K, M)^{\mathfrak{g}_k}$ and $H^1(\mathfrak{g}_k, M^*)$ are orthogonal complements. Thus Tate local duality induces perfect pairings*

$$H^1(\mathfrak{g}_k, M) \otimes H^1(\mathcal{I}_K, M^*)^{\mathfrak{g}_k} \to \mathbb{Q}/\mathbb{Z}$$

and

$$H^1(\mathcal{I}_K, M)^{\mathfrak{g}_k} \otimes H^1(\mathfrak{g}_k, M^*) \to \mathbb{Q}/\mathbb{Z}.$$

In particular, we have an exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \left(H^1(\mathcal{I}_K, M)^{\mathfrak{g}_k}\right)^\vee & \longrightarrow & \left(H^1(G_K, M)\right)^\vee & \longrightarrow & \left(H^1(\mathfrak{g}_k, M)\right)^\vee & \longrightarrow & 0 \\
 & & \cong \uparrow & & \cong \uparrow & & \cong \uparrow & & \\
0 & \longrightarrow & H^1(\mathfrak{g}_k, M^*) & \longrightarrow & H^1(G_K, M^*) & \longrightarrow & H^1(\mathcal{I}_K, M^*)^{\mathfrak{g}_k} & \longrightarrow & 0
\end{array}$$

PROOF. The injectivity of the first vertical maps and the surjectivity of the second vertical map follow from the the orthogonality constructions above. The fact that they are isomorphisms then follows from Proposition 2.1. The rest of the theorem is just a restatement of the diagram. □

CHAPTER 7

Lecture 7

1. Finite/Singular Structures

1.1. Local Structures. Let K be a local field with residue field k of characteristic p, and let M be a finite G_K-module of prime to p order. In any case we have exact sequences

$$0 \to H^1(\mathfrak{g}_k, M^{\mathcal{I}_K}) \to H^1(G_K, M) \to H^1(\mathcal{I}_K, M)^{\mathfrak{g}_k} \to 0$$

and

$$0 \to H^1(\mathfrak{g}_k, (M^*)^{\mathcal{I}_K}) \to H^1(G_K, M^*) \to H^1(\mathcal{I}_K, M^*)^{\mathfrak{g}_k} \to 0.$$

If in addition M is only tamely ramified, then Theorem 2.2 of Lecture 6 applies. In this case we define the *finite* and *singular* parts of $H^1(G_K, M)$ by

$$H^1_f(G_K, M) = H^1(\mathfrak{g}_k, M^{\mathcal{I}_K})$$

and

$$H^1_s(G_K, M) = H^1(\mathcal{I}_K, M)^{\mathfrak{g}_k}.$$

The definition also applies to M^*. We will refer to these choices as the *standard finite/singular structure* on M. (We could of course make these definitions without any conditions on M, but they would not in general have the properties that we want.) Thus there is an exact commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1_s(G_K, M)^\vee & \longrightarrow & H^1(G_K, M)^\vee & \longrightarrow & H^1_f(G_K, M)^\vee & \longrightarrow & 0 \\ & & \cong\uparrow & & \cong\uparrow & & \cong\uparrow & & \\ 0 & \longrightarrow & H^1_f(G_K, M^*) & \longrightarrow & H^1(G_K, M^*) & \longrightarrow & H^1_s(G_K, M^*) & \longrightarrow & 0 \end{array}$$

with the vertical isomorphisms coming from Tate local duality. Put differently, Tate duality identifies $H^1_f(G_K, M)$ and $H^1_s(G_K, M^*)$ as duals; it also identifies $H^1_s(G_K, M)$ and $H^1_f(G_K, M^*)$ as duals.

Note that in the case that M is unramified as a G_K-module (meaning that $\mathcal{I}_K$ acts trivially on M), we have the slightly simpler definitions

$$H^1_f(G_K, M) = H^1(\mathfrak{g}_k, M)$$

and

$$H^1_s(G_K, M) = \mathrm{Hom}(\mathcal{I}_K, M)^{\mathfrak{g}_k}.$$

We will now briefly describe an interpretation of $H^1_f(G_K, M)$ that helps to explain the terminology "finite". We do this using the interpretation of $H^1(G_K, M)$ in terms of torsors. (See Lecture 5, Section 2.) So let T be an M-torsor. In particular, T is a finite G_K-set. There is an equivalence of categories between the

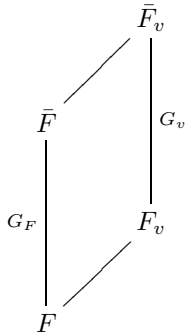
[0]Last modified September 4, 2003

FIGURE 1. Extending finite étale schemes over $\operatorname{Spec} K$

category of finite G_K-sets and the category of finite, étale schemes over $\operatorname{Spec} K$. (See [**Mi-EC**, Chapter 1, Section 5, Theorem 5.3].) Let $\mathcal{T}$ be the finite, étale scheme over $\operatorname{Spec} K$ associated with T.

Let $\mathcal{O}_K$ be the ring of integers of K. $\operatorname{Spec} \mathcal{O}_K$ consists of the generic point $\operatorname{Spec} K$ and the closed point $\operatorname{Spec} k$. A natural question is when the $\operatorname{Spec} K$ scheme $\mathcal{T}$ can be extended to a finite, étale scheme $\mathcal{T}'$ over $\operatorname{Spec} \mathcal{O}_K$. It is not difficult to see that any finite, étale $\mathcal{T}$ over $\operatorname{Spec} K$ can be extended to a quasi-finite, étale scheme over $\operatorname{Spec} \mathcal{O}_K$; the difficult part is getting it to be finite and étale . It turns out that, at least in the case where M is unramified, $\mathcal{T}'$ can be taken to be finite if and only if the cohomology class associated to T lies in $H^1_f(G_K, M)$. Thus the "finite" terminology is appropriate, at least in this case.

1.2. Global Structures. We now consider a global field F. For us we will simply take global field to mean number field; that is, a finite extension of $\mathbb{Q}$. We will always consider F to come along with a choice of algebraic closure $\bar{F}$, and we set $G_F = \operatorname{Gal}(\bar{F}/F)$ as usual. For each place v of F (archimedean or non-archimedean) we let F_v be the completion of F at v; we fix an algebraic closure $\bar{F}_v$ of F_v. We also choose an embedding of $\bar{F}$ into $\bar{F}_v$; this is equivalent to choosing a place of $\bar{F}$ above v, which in turn is equivalent to choosing a decomposition group of v in G_F. We will write G_{F_v} or just G_v for the Galois group $\operatorname{Gal}(\bar{F}_v/F_v)$; this is (because of our choices) identified with the decomposition group of v in G_F. In the case where v is non-archimedean, we will write $\mathfrak{g}_v$ for the absolute Galois group of the residue field of F_v.



Let M be a finite G_F-module, with the G_F-action continuous for the discrete topology on M. Note that for every place v, M is also a G_v-module by restriction. Thus our choice of embedding

$$G_v \hookrightarrow G_F$$

induces maps on cohomology

$$H^i(G_F, M) \xrightarrow{\operatorname{res}_v} H^i(G_v, M)$$

for all $i \geq 0$. Here a remarkable thing happens: the maps res_v are independent of our choice of embedding $G_v \hookrightarrow G_F$. This follows from the fact that G_v is determined as a subgroup of G_F up to conjugation by elements of G_F; since conjugation induces the identity automorphism on cohomology ([**Se-LF**, Chapter 7, Section 5, Proposition 3]), res_v is thus independent of the choice of G_v in G_F.

We want to impose local structures on the first global cohomology group of M, $H^1(G_F, M)$; we essentially want to use our finite/singular structures defined previously. However, we have only defined these local structures in the case that v is non-archimedean, M is at worst tamely ramified as a G_v-module, and the residue characteristic of F_v does not divide the order of M. (From now on we will say that the non-archimedean place v divides the order of M if its residue characteristic does.) We do not yet want to impose any particular structure at the other places of F, so we make the following definition.

DEFINITION 3. A *structured* G_F-module is a finite, discrete G_F-module M together with a choice of finite/singular structure at each place v of F; by this we simply mean a choice of an exact sequence

$$0 \to H^1_f(G_v, M) \to H^1(G_v, M) \to H^1_s(G_v, M) \to 0$$

for each v. (That is, simply pick either a subgroup or a quotient group of $H^1(G_v, M)$ and define the other group via the exact sequence.) We further require that there is a finite set S of places of F such that for all $v \notin S$,

$$H^1_f(G_v, M) = H^1(\mathfrak{g}_v, M^{\mathcal{I}_v})$$

and

$$H^1_s(G_v, M) = H^1(\mathcal{I}_v, M)^{\mathfrak{g}_v}.$$

That is, we require that our choice of finite/singular structure agree with that defined previously, at least for $v \notin S$.

We will always take S to contain all archimedean places, all places where M has wild ramification, and all places dividing the order of M, since we have not even defined finite/singular structures in these cases. It is easy to check that since M is finite and discrete there are only finitely many such places, so the definition makes sense. We can in fact improve this statement slightly; M is actually *unramified* as a G_v-module for all but finitely many v.

In order to exploit Tate local duality we want to be somewhat careful as to how the structure on M relates to that on its Cartier dual M^*. In order to do this we must carefully consider the archimedean places for the first time. In fact, they behave much like the non-archimedean places. Since the case where v is complex is trivial (everything vanishes), the next proposition is all that we will need.

PROPOSITION 1.1. *Let M be a finite $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$-module. Then the pairing*

$$H^1(G, M) \otimes H^1(G, M^*) \to H^2(G, M \otimes M^*) \to H^2(G, \mu(\mathbb{C}^*)) \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

given by cup product, Cartier duality and an easy computation, is perfect.

PROOF. Write $G = \{1, c\}$, where c is complex conjugation. c acts on $\mu(\mathbb{C}^*)$ by inversion, so we can choose an identification of $\mu(\mathbb{C}^*)$ with $\mathbb{Q}/\mathbb{Z}$ on which c acts by negation. Cartier duality between M and M^* now becomes a sort of Pontrjagin duality

$$M \otimes M^* \to \mathbb{Q}/\mathbb{Z},$$

where $\varphi \in M^*$ is considered as a map $\varphi : M \to \mathbb{Q}/\mathbb{Z}$ such that

$$(c\varphi)(m) = c\varphi(c^{-1}m)$$

for all $m \in M$. Given our action of c on $\mathbb{Q}/\mathbb{Z}$ and the fact that $c = c^{-1}$, this becomes

$$(c\varphi)(m) = -\varphi(cm).$$

Recall that we have an identification

$$H^1(G, M) = \text{CrossHom}(G, M)/\,\text{PrincCrossHom}(G, M).$$

A crossed homomorphism h must send $1 \in G$ to $0 \in M$, so it is determined completely by where it sends c. The cocycle condition is just

$$c(h(c)) + h(c) = 0,$$

so we can identify $\text{CrossHom}(G, M)$ with the subgroup of M on which c acts by negation; we write this as M^-. Under this identification the principal crossed homomorphisms are just $(1 - c)M$, so we have an identification

$$H^1(G, M) = M^-/(1 - c)M.$$

We have a similar expression for M^*.

Now, we return to our "Pontrjagin" duality

$$M \otimes M^* \to \mathbb{Q}/\mathbb{Z}.$$

The annihilator of M^{*-} in M is easily seen to be $(1 - c)M$, since $\varphi \in M^{*-}$ if and only if

$$\varphi(cm) = \varphi(m)$$

for all $m \in M$. Similarly, the annihilator of M^- is just $(1 - c)M^*$. Thus the above pairing restricts to a perfect pairing

$$M^-/(1 - c)M \otimes M^{*-}/(1 - c)M^* \to \mathbb{Q}/\mathbb{Z}.$$

Now our above observations and an easy computation using the definition of cup products (see [**AW**, Section 7]) identify this pairing with the cup product followed by Cartier duality, so the proof is complete. □

We will refer to the above pairing simply as a local pairing.

Definition 4. Let M be a structured G_F-module. We define the *Cartier dual* of M as a structured G_F-module to be the G_F-module

$$M^* = \text{Hom}_{\mathbb{Z}}(M, \mu(\bar{F}))$$

together with choices of local finite/singular structures

$$0 \to H^1_f(G_v, M^*) \to H^1(G_v, M^*) \to H^1_s(G_v, M^*) \to 0$$

such that $H^1_f(G_v, M^*)$ is the exact dual of $H^1_s(G_v, M)$ under the local pairing for *all* v. Since the local pairings are perfect, it follows that $H^1_s(G_v, M^*)$ is the exact dual of $H^1_f(G_v, M)$.

Note that Theorem 2.2 of Lecture 6 insures that the above definition really does give a finite/singular structure on M^*.

2. Generalized Selmer Groups

2.1. Definitions. We continue to let F be a number field and we let M be a finite, structured G_F-module. We now define finite and singular parts of $H^1(G_F, M)$ using local conditions. First note that under the maps

$$H^1(G_F, M) \xrightarrow{\text{res}_v} H^1(G_v, M),$$

each element $h \in H^1(G_F, M)$ maps to $H^1_f(G_v, M)$ for all but finitely many v. To see this, recall that $H^1(G_F, M)$ is defined as a direct limit, so we can consider h as an element of $H^1(\text{Gal}(L/F), M^{G_L})$ for some finite, Galois extension L of F. Let v be a place of F and let w be the place of L above v determined by our choice $G_v \hookrightarrow G_F$. Further suppose that v is non-archimedean and that L/F is unramified at v; this is true for almost all v. But in this situation, letting ℓ_w and f_v be the residue fields of L_w and F_v respectively, the inflation-restriction sequence gives an isomorphism

$$H^1(\text{Gal}(\ell_w/f_v), M^{G_L}) \xrightarrow{\cong} H^1(\text{Gal}(L_w/F_v), M^{G_L}),$$

since the inertia group is trivial. If also M has the standard structure at v, the commutative diagram

$$\begin{array}{ccc} H^1(\text{Gal}(L/F), M^{G_L}) & \xrightarrow{\text{res}_v} & H^1(\text{Gal}(\ell_w/f_v), M^{G_L}) \\ \Big\downarrow{\scriptstyle \text{inf}} & & \Big\downarrow{\scriptstyle \text{inf}} \\ & & H^1_f(G_v, M) \\ & & \Big\downarrow{\scriptstyle \text{inf}} \\ H^1(G_F, M) & \xrightarrow{\text{res}_v} & H^1(G_v, M) \end{array}$$

shows that $\text{res}_v(h) \in H^1_f(G_v, M)$; thus this is true almost always, as claimed.

We want to define $H^1_f(G_F, M)$ to be the set of global cohomology classes which are always locally finite. Precisely we define

$$H^1_f(G_F, M) = \ker\big(H^1(G_F, M) \to \oplus_v H^1_s(G_v, M)\big),$$

where the direct sum is over all places v of F. (Our argument above shows that this map really does land in the direct sum.) That is,

$$H^1_f(G_F, M) = \{h \in H^1(G_F, M) \mid \text{res}_v(h) \in H^1_f(G_v, M) \text{ for all } v\}.$$

We will call $H^1_f(G_F, M)$ the *Selmer group* of the structured G_F-module M.

We define

$$H^1_s(G_F, M) = H^1(G_F, M)/H^1_f(G_F, M),$$

so that there is an exact sequence

$$0 \to H^1_f(G_F, M) \to H^1(G_F, M) \to H^1_s(G_F, M) \to 0.$$

We will call $H^1_s(G_F, M)$ the *Kolyvagin group* of the structured G_F-module M.

We should note that our choice of notation is not intended to imply that there is any sort of duality between the Selmer groups and Kolyvagin groups of M and M^*. The statement of Poitou-Tate global duality is significantly more complicated than that of Tate local duality.

2.2. A First Example. In order to illuminate the meaning of a Selmer group slightly, we now consider a simple example. Let M be a finite abelian group considered as a G_F-module with trivial G_F-action. We define a structure on M as follows: Let S be a set of places of F containing all of the bad places. That is, S contains the archimedean places and the set of places dividing the order of M. For $v \in S$, we simply take

$$H^1_f(G_v, M) = H^1(G_v, M)$$

so that

$$H^1_s(G_v, M) = 0.$$

For $v \notin S$, we take the standard finite/singular structure. Since M is unramified everywhere, this takes the simple form

$$0 \to H^1(\mathfrak{g}_v, M) \to H^1(G_v, M) \to \mathrm{Hom}(\mathcal{I}_v, M)^{\mathfrak{g}_v} \to 0.$$

Now, consider $H^1(G_F, M)$. Since G_F acts trivially on M, we have

$$H^1(G_F, M) = \mathrm{Hom}(G_F, M) = \mathrm{Hom}(G_F^{\mathrm{ab}}, M).$$

(The homomorphisms are continuous, of course.) A cocycle $h \in H^1(G_F, M)$ lies in the Selmer group $H^1_f(G_F, M)$ if it maps to 0 in $H^1_s(G_v, M)$ for all places v. If $v \in S$, this is automatic. If $v \notin S$, this simply asks that h vanishes on the inertia group $\mathcal{I}_v$. (We get these simple interpretations since h is just a homomorphism.) Thus $H^1_f(G_F, M)$ is simply the subgroup of $\mathrm{Hom}(G_F^{\mathrm{ab}}, M)$ of homomorphisms vanishing on all inertia groups of $v \in S$. In other words, letting $F^{\mathrm{ab},S}$ be the maximal abelian extension of F unramified outside of S, we have

$$H^1_f(G_F, M) = \mathrm{Hom}(\mathrm{Gal}(F^{\mathrm{ab},S}/F), M).$$

($\mathrm{Hom}(\mathrm{Gal}(F^{\mathrm{ab},S}/F), M)$ is considered as a subgroup of $\mathrm{Hom}(G_F^{\mathrm{ab}}, M)$ via the natural surjection $G_F^{\mathrm{ab}} \twoheadrightarrow \mathrm{Gal}(F^{\mathrm{ab},S}/F)$.) Thus knowledge of $H^1_f(G_F, M)$ should yield information about $F^{\mathrm{ab},S}$.

If instead we had imposed the finite/singular structure with

$$H^1_f(G_v, M) = 0$$

and

$$H^1_s(G_v, M) = H^1(G_v, M)$$

for $v \in S$, one can easily check in the same way as above that we would have obtained

$$H^1_f(G_F, M) = \mathrm{Hom}(\mathrm{Gal}(F'/F), M),$$

where F' is the maximal abelian extension of F which is unramified everywhere and in which all places in S split completely. (The key fact here is that all of the local Galois groups for a place v vanish if and only if v splits completely.)

2.3. Interpretation in terms of Étale Cohomology. We now give an interpretation of (some) Selmer groups in terms of étale cohomology. We let M be any finite G_F-module, and we again take S to be a set of places containing all of the bad places. (This time it also contains those places where M is wildly ramified.) We take the standard finite/singular structure at $v \notin S$, and we set

$$H^1_f(G_v, M) = H^1(G_v, M)$$

for $v \in S$. We let S' be the subset of S of non-archimedean places.

Recall (see Lecture 1, Section 1) that to M we can associate an étale sheaf $\mathcal{M}$ over $\operatorname{Spec} F$. Let $\mathcal{O}_F$ be the ring of integers of F, and consider the natural maps

$$\operatorname{Spec} F \overset{j}{\hookrightarrow} \operatorname{Spec} \mathcal{O}_F - S' \overset{i}{\hookrightarrow} \operatorname{Spec} \mathcal{O}_F.$$

Here $\operatorname{Spec} F$ maps to the generic point. Note that $\operatorname{Spec} \mathcal{O}_F - S'$ is an open subscheme of $\operatorname{Spec} \mathcal{O}_F$ and can be realized as $\operatorname{Spec} \mathcal{O}_F[1/N]$ where N is any element of $\mathcal{O}_F$ divisible by every place of S' and no other places. In this situation it can be shown that

$$H^1_f(G_F, M) = H^1_{\text{et}}(\operatorname{Spec} \mathcal{O}_F - S', j_*\mathcal{M}).$$

We sketch a proof. Set $X = \operatorname{Spec} \mathcal{O}_F - S'$. The Leray spectral sequence ([**Mi-EC**, Chapter 3, Theorem 1.18]) for $j : \operatorname{Spec} F \to X$ takes the form

$$H^p_{\text{et}}(X, R^q j_*\mathcal{M}) \Rightarrow H^{p+q}_{\text{et}}(\operatorname{Spec} F, \mathcal{M}).$$

The exact sequence of low degree terms begins

$$0 \to H^1_{\text{et}}(X, j_*\mathcal{M}) \to H^1_{\text{et}}(\operatorname{Spec} F, \mathcal{M}) \to R^1 j_*\mathcal{M}(X).$$

But $H^1_{\text{et}}(\operatorname{Spec} F, \mathcal{M})$ is just $H^1(G_F, M)$ (see [**Mi-EC**, Chapter 3, Example 1.7]), so we have identified $H^1_{\text{et}}(X, j_*\mathcal{M})$ with the subgroup of elements of $H^1(G_F, M)$ which vanish in $R^1 j_*\mathcal{M}(X)$.

To check that an element of this last group vanishes it is enough to check on the stalks. So let $\overline{v} \hookrightarrow X$ be a geometric point sitting over some prime v of F, $v \notin S'$. The stalk of $\mathcal{O}_X$ at $\overline{v}$ is just the strict Henselization of the local ring of $\mathcal{O}_X$ at v (recall that the *strict Henselization* of a local ring A is the smallest local ring containing A which has algebraically closed residue field and satisfies Hensel's lemma); in this case, this is just the ring of integers of the maximal unramified extension of F_v. The base change of $\operatorname{Spec} \mathcal{O}_{X,\overline{x}}$ up to $\operatorname{Spec} F$ is then $\operatorname{Spec} F_v^{\text{ur}}$, so by [**Mi-EC**, Chapter 3, Theorem 1.15] we have

$$R^1 j_*(\mathcal{M})_{\overline{v}} = H^1(\operatorname{Spec} F_v^{\text{ur}}, \mathcal{M}) = H^1(\mathcal{I}_v, M),$$

where $\mathcal{I}_v$ is the inertia group at v. A similar calculation shows that the stalk at the generic point is 0.

Combining this with our above exact sequence, we see that an element $h \in H^1(F, M)$ lies in $H^1_{\text{et}}(X, j_*\mathcal{M})$ if and only if h maps to 0 in each $H^1(\mathcal{I}_v, M)$ for $v \notin S$. But this is exactly the definition of $H^1_f(G_F, M)$, so

$$H^1_f(G_F, M) = H^1_{\text{et}}(\operatorname{Spec} \mathcal{O}_F - S', j_*\mathcal{M}),$$

as claimed.

2.4. Other Notation. Our notation differs somewhat from that in [**Ru-ES**]. The translation is easy; for convenience, and so the reader can go through [**Ru-ES**, Chapter 1, Section 6], we record it here.

First, Rubin uses the standard notations

$$H^i(K, M) = H^i(\operatorname{Gal}(K_s/K), M)$$

for any field K, and

$$H^i(L/K, M) = H^i(\operatorname{Gal}(L/K), M)$$

for any Galois extension L/K. He defines standard finite/singular structures for archimedean v and for all v not dividing the order of M; they agree with ours when both are defined.

Our Selmer group $H^1_f(G_F, M)$, assuming our finite/singular structures agree with his for v not dividing the order of M and given our choices for those v which do divide the order of M, would be written as $\mathcal{S}(F, M)$. Rubin also defines "partial" Selmer groups where not all local conditions are enforced, and "strict" Selmer groups where some $H^1_f(G_F, M)$ are set to be 0 (in our terminology). For details, see [**Ru-ES**, Chapter 1, Section 5].

In [**Ru-ES**, Chapter 1, Section 6] he gives several interesting interpretations of Selmer groups, relating them to ideal class groups, units and abelian varieties. The reader is strongly encouraged to look at that section.

We should also note that Rubin's Galois modules are rarely finite; they tend to be p-adic. This distinction can probably be safely ignored.

3. Brauer Groups

3.1. Definitions. We begin by recalling the various interpretations of the Brauer group. For proofs of the claims in this section, see [**FD**, Chapter 4]. For any field L, we take as our definition

$$\mathrm{Br}_L = H^2(G_L, L_s).$$

As a first alternate definition, Br_L can be considered as the set of finite dimensional central simple algebras over L modulo the equivalence relation where two central simple algebras are considered to be equivalent if they become isomorphic as L-algebras after tensoring each with (possibly different) total matrix algebras $\mathcal{M}_n(L)$. Br_L is made into a group by tensor product. It can be shown that every central simple algebra over L is a matrix algebra over a central divison algebra over L, and that central simple algebras are equivalent in our sense if and only if they come from the same division algebra. Thus Br_L also classifies central division algebras over L. Lastly, it is also true that an L-algebra is central simple over L if and only if it becomes isomorphic to $\mathcal{M}_n(\bar{L})$, for some n, after tensoring with $\bar{L}$. In particular, the dimension of any central simple algebra over L is a perfect square.

To recall a few examples, if k is a finite field we have Wedderburn's theorem (see [**FD**, Chapter 3, Theorem 3.18])

$$\mathrm{Br}_k = 0,$$

and for the real numbers we have

$$\mathrm{Br}_{\mathbb{R}} = \mathbb{Z}/2\mathbb{Z}$$

with the non-trivial division algebra being the quaternions $\mathbb{H}$. (See [**FD**, Chapter 3, Theorem 3.20]) We also note that

$$\mathrm{Br}_{\bar{L}} = 0$$

for any algebraically closed field $\bar{L}$; the proof of this is easy.

3.2. Brauer Group of a Local Field. Recall that if K is a local field, then local class field theory gives an isomorphism

$$\mathrm{Br}_K = H^2(G_K, \bar{K}^*) \xrightarrow{\mathrm{inv}_K} \mathbb{Q}/\mathbb{Z}.$$

(See [**Se-LF**, Chapter 13, Section 3].) For completeness, we include here the proof that this implies that

$$H^2(G_K, \mu(\bar{K}^*)) \cong \mathbb{Q}/\mathbb{Z}.$$

We use the Kummer exact sequence

$$1 \to \mu_N(\bar{K}^*) \to \bar{K}^* \xrightarrow{N} \bar{K}^* \to 1$$

for every N. The long exact sequence in cohomology yields

$$H^1(G_K, \bar{K}^*) \to H^2(G_K, \mu_N(\bar{K}^*)) \to H^2(G_K, \bar{K}^*)[N] \to 0,$$

where by $H^2(G_K, \bar{K}^*)[N]$ we mean the N-torsion. But by Hilbert's Theorem 90 the first term is zero, and by the invariant map the last term is $\frac{1}{N}\mathbb{Z}/\mathbb{Z}$. Taking the direct limit over N now completes the proof.

We recall the explicit description of division algebras over K. Let $m/n \in \mathbb{Q}/\mathbb{Z}$ be in lowest terms, with $0 < m < n$. ($0 \in \mathbb{Q}/\mathbb{Z}$ corresponds to K, of course.) We will construct the central division algebra A mapping to m/n under the invariant map. Let L be the unique unramified extension of K of degree n. A has dimension n^2 over K, and contains L as a maximal commutative subalgebra. In fact, it requires only one more generator: $A = L[\gamma]$, where γ normalizes L (that is, $\gamma L \gamma^{-1} = L$), and for any $x \in L$, $\gamma x \gamma^{-1} = \mathrm{Fr}^m\, x$, where Fr is the Frobenius automorphism for K. See [**Pi**, Chapter 17, Section 10] for details.

3.3. Global Brauer Groups. We now consider the Brauer group of a number field F. Recall that we have canonical maps

$$H^2(G_F, \bar{F}^*) \xrightarrow{\mathrm{res}_v} H^2(G_v, \bar{F}_v^*)$$

for every place v of F. We claim that for any $h \in H^2(G_F, \bar{F}^*)$, the image of h in $H^2(G_v, \bar{F}_v^*)$ is zero for almost all v.

PROPOSITION 3.1. *For any $h \in H^2(G_F, \bar{F}^*)$, $\mathrm{res}_v(h) = 0$ for all but finitely many places v of F.*

PROOF. Note that as usual, since $H^2(G_F, \bar{F}^*)$ is a direct limit, we can assume that h lies in $H^2(\mathrm{Gal}(L/F), L^*)$ for some finite Galois extension L/F. Now, let c be a cocycle representing h. Since $\mathrm{Gal}(L/F)$ is finite, c takes on only finitely many values; in particular, its image is divisible by only finitely many primes. So let T be the set of all such places, together with the archimedean places and the places where L/K is ramified; T is finite.

Now consider $\mathrm{res}_v(h) \in H^2(\mathrm{Gal}(L_w/F_v), L_w^*)$ for any $v \notin T$, where w is the place of L above v induced by our choice of embedding $\bar{F} \hookrightarrow \bar{F}_v$. By the definition of the restriction map, $\mathrm{res}_v(h)$ is represented by the restriction of c. In particular, c takes values in $\mathcal{O}_w^*$, the units of the ring of integers of L_w. This means that $\mathrm{res}_v(h)$ lies in the image of the natural map

$$H^2(\mathrm{Gal}(L_w/F_v), \mathcal{O}_w^*) \to H^2(\mathrm{Gal}(L_w/F_v), L_w^*).$$

Consider the exact sequence

$$0 \to \mathcal{U}_1 \to \mathcal{O}_w^* \to \ell^* \to 0,$$

where $\mathcal{U}_1$ are the units congruent to 1 modulo $\mathfrak{m}_w$, and ℓ^* is the residue field of L_w. This is an exact sequence of $\mathrm{Gal}(L_w/F_v)$-modules, and using the fact (see [**Se-LF**, Chapter 12, Section 3, Lemma 2]) that $H^i(\mathrm{Gal}(L_w/F_v), \mathcal{U}_1) = 0$ for all $i \geq 1$, we get an isomorphism

$$H^2(\mathrm{Gal}(L_w/F_v), \mathcal{O}_w^*) \cong H^2(\mathrm{Gal}(L_w/F_v), \ell^*).$$

Finally, since L_w/F_v is unramified, the cohomology of a finite cyclic group ([**Se-LF**, Chapter 8, Section 4]) and the surjectivity of the norm on a finite field show that

$$H^2(\mathrm{Gal}(L_w/F_v), \ell^*) = 0,$$

which implies that the image of $H^2(\mathrm{Gal}(L_w/F_v), \mathcal{O}_w^*)$ in $H^2(\mathrm{Gal}(L_w/F_v), L_w^*)$ is zero, and thus that $\mathrm{res}_v(h) = 0$ for all places not in T. This proves the claim. □

For a proof of this fact using the cohomology of the ideles, see [**Ta**, Section 7, Proposition 7.3 and Section 9.6]. (Note that he doesn't actually prove that the maps he is considering are the restriction map, but it is not too difficult to see this.) For a proof in terms of divison algebras, see [**Pi**, Chapter 18, Section 5].

It follows that the restriction maps combine to give a map

$$H^2(G_F, \bar{F}^*) \xrightarrow{\mathrm{res}} \oplus_v H^2(G_v, \bar{F}_v^*),$$

the direct sum being over all places v of F. One of the fundamental theorems of global class field theory is the determination of the kernel and cokernel of this map. Before we state it, we consider

$$\oplus_v H^2(G_v, \bar{F}_v^*).$$

This can be evaluated as

$$\oplus_{v \text{ non-arch}} \mathbb{Q}/\mathbb{Z} \oplus \oplus_{v \text{ real}} \frac{1}{2}\mathbb{Z}/\mathbb{Z},$$

given the results of the previous two sections.

THEOREM 3.2. *There is an exact sequence*

$$0 \to \mathrm{Br}_F \xrightarrow{\mathrm{res}} \oplus_v \mathrm{Br}_{F_v} \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where the last map is summation of elements of $\mathbb{Q}/\mathbb{Z}$ in the identification above.

PROOF. This is proved along with the fundamental results of global class field theory; see [**Ta**, Section 9.6] for the statement. □

CHAPTER 8

Lecture 8

1. Notation for Generalized Selmer Groups

1.1. Structures. For convenience we will set some notation for our generalized Selmer groups. We continue to let F be a number field with the conventions of Lecture 7, Section 1.2. Let M be a finite G_F-module. We recall that a structure σ on M is a choice of exact sequences

$$\sigma_v : 0 \to H^1_f(G_v, M) \to H^1(G_v, M) \to H^1_s(G_v, M) \to 0$$

for all places v of M, such that the exact sequence σ_v is the standard local finite/singular exact sequence for almost all v. We will write M_σ for the G_F-module M with the structure σ; if there is no chance of confusion we will just write M.

Given two structures σ_1 and σ_2 on M, we will say that σ_1 is *more stringent* than σ_2, written

$$\sigma_1 < \sigma_2,$$

if

$$H^1_f(G_v, M_{\sigma_1}) \subseteq H^1_f(G_v, M_{\sigma_2})$$

for all places v. In particular, this implies that

$$H^1_f(G_F, M_{\sigma_1}) \subseteq H^1_f(G_F, M_{\sigma_2}),$$

since the conditions to lie in $H^1_f(G_F, M_{\sigma_1})$ are more restrictive than those to lie in $H^1_f(G_F, M_{\sigma_2})$. This relation gives a partial ordering on the set of all structures.

Given a structured module M_σ we will write σ^* for the structure defined on M^* in Definition 4 of Lecture 7. It follows easily from the definition of this structure on M^* that if $\sigma_1 < \sigma_2$, then $\sigma_2^* < \sigma_1^*$.

Let S be a finite set of places of F containing all the archimedean places, all the places dividing the order of M and all places where M is ramified. We define the *S-structure* on M, written as M_S, to be the structure with the standard finite/singular structures for all $v \notin S$ and with the choices

$$H^1_f(G_v, M_S) = H^1(G_v, M)$$

for all $v \in S$. (We considered this structure in Lecture 7, Sections 2.2 and 2.3.) So an S-structure is the least stringent structure on M with the standard choices outside of S. In particular, if σ is any structure, then there is some S-structure which is less stringent than σ; simply take S to contain all places where σ is not standard.

[0]Last modified September 4, 2003

1.2. The Singular Restriction Map. Recall that for every place v we have a canonical restriction map

$$H^1(G_F, M) \xrightarrow{\text{res}_v} H^1(G_v, M).$$

We define the *local singular restriction map at* v

$$\text{res}_{s,v} : H^1(G_F, M) \to H^1_s(G_v, M)$$

to be the composition of res_v with the quotient map

$$H^1(G_v, M) \twoheadrightarrow H^1_s(G_v, M).$$

We saw in Lecture 7, Section 2.1 that for any $h \in H^1(G_F, M)$ we have $\text{res}_v(h) \in H^1_f(G_v, M)$ for almost all v; in our new notation this says that $\text{res}_{s,v}(h) = 0$ for almost all v. Thus we obtain a map, which we call the *singular restriction map*,

$$\text{res}_s : H^1(G_F, M) \to \oplus_v H^1_s(G_v, M),$$

the direct sum being over all places of F. With this notation we have

$$H^1_f(G_F, M) = \ker \text{res}_s,$$

so there is an exact sequence

$$0 \to H^1_f(G_F, M) \to H^1(G_F, M) \to \oplus_v H^1_s(G_v, M).$$

Recall that by definition of the Kolyvagin group $H^1_s(G_F, M)$ we have an exact sequence

$$0 \to H^1_f(G_F, M) \to H^1(G_F, M) \to H^1_s(G_F, M) \to 0.$$

Comparing this to the exact sequence above we see that there is a natural injection

$$H^1_s(G_F, M) \hookrightarrow \oplus_v H^1_s(G_v, M).$$

Given any $c \in H^1_s(G_F, M)$, this map is simply the map

$$c \mapsto (\text{res}_{s,v}(\tilde{c}))_v,$$

where $\tilde{c}$ is any lifting of c to $H^1(G_F, M)$. We will write c_v for $\text{res}_{s,v}(\tilde{c}) \in H^1_s(G_v, M)$, so that the above map is simply

$$c \mapsto (c_v)_v.$$

We conclude with a few more definitions. Given any

$$c = (c_v)_v \in \oplus_v H^1_s(G_v, M),$$

define the *support* of c, $\text{Supp}(c)$, to be the set of places v for which $c_v \neq 0$; our previous discussion shows that $\text{Supp}(c)$ is finite. If c is actually in $H^1_s(G_F, M)$, we again write $\text{Supp}(c)$ for the set of places for which $c_v \neq 0$. Also, for any $h \in H^1(G_F, M)$ we will write h_v for $\text{res}_v(h) \in H^1(G_v, M)$. In particular, if $h \in H^1_f(G_F, M)$, then $h_v \in H^1_f(G_v, M)$ for all v

2. A Global Pairing

We continue with the notation of the previous section. In particular, M is a finite structured G_F-module with (structured) Cartier dual M^*. For *any* place v we will write $\langle \cdot, \cdot \rangle_v$ for the pairing

$$H^1(G_v, M) \otimes H^1(G_v, M^*) \to H^2(G_v, M \otimes M^*) \to H^2(G_v, \mu(F_v^*)) \to \mathbb{Q}/\mathbb{Z}$$

given by cup product, Cartier duality and the invariant map. Thus for non-archimedean v, $\langle \cdot, \cdot \rangle_v$ is just the Tate pairing; for real v it is the pairing

$$H^1(G_v, M) \otimes H^1(G_v, M^*) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

of Lecture 7, Proposition 1.1; and for complex v all of the groups are 0, since $G_v = 0$. For any $c_v \in H^1(G_v, M^*)$, we will also think of the pairing as giving a map

$$c_v : H^1(G_v, M) \to \mathbb{Q}/\mathbb{Z},$$

given by $c_v(h_v) = \langle h_v, c_v \rangle$.

We now define a global pairing

$$H^1_f(G, M) \otimes \oplus_v H^1_s(G_v, M^*) \to \mathbb{Q}/\mathbb{Z}$$

by

$$h \otimes (c_v)_v \mapsto \sum_v \langle h_v, c_v \rangle_v .$$

(Recall the definition of h_v in the previous section.) This is actually well-defined since $h_v \in H^1_f(G_v, M)$ for all v and by our definition of the structure on M^* the perfect pairings

$$H^1(G_v, M) \otimes H^1(G_v, M^*) \to \mathbb{Q}/\mathbb{Z}$$

yield perfect pairings

$$H^1_f(G_v, M) \otimes H^1_s(G_v, M^*) \to \mathbb{Q}/\mathbb{Z}$$

for all v. Also, the sum is simply a finite sum

$$\sum_v \langle h_v, c_v \rangle_v = \sum_{v \in \mathrm{Supp}(c)} \langle h_v, c_v \rangle_v$$

since $(c_v)_v$ is an element of the direct sum.

We will write the pairing as $\langle h, c \rangle$; alternately, for any $c \in \oplus_v H^1_s(G_v, M^*)$, we will also write c for the map

$$c : H^1_f(G_F, M) \to \mathbb{Q}/\mathbb{Z}$$

given by $c(h) = \langle h, c \rangle$.

This pairing, together with the next proposition, will be our principal tool for bounding the order of Selmer groups.

PROPOSITION 2.1. *The subgroup $H^1_s(G_F, M^*)$ of $\oplus_v H^1_s(G_v, M^*)$ is orthogonal to all of $H^1_f(G_F, M)$ under the above pairing; that is, the composition*

$$H^1_f(G_F, M) \otimes H^1_s(G_F, M^*) \to H^1_f(G_F, M) \otimes \oplus_v H^1_s(G_v, M^*) \to \mathbb{Q}/\mathbb{Z}$$

is zero.

PROOF. Take any $h \in H^1_f(G_F, M)$ and $c \in H^1_s(G_F, M^*)$, and let $\tilde{c}$ be a lifting of c to $H^1(G_F, M^*)$. Consider the commutative diagram

$$\begin{array}{ccc}
H^1(G_F, M) \otimes H^1(G_F, M^*) & \longrightarrow & \prod_v H^1(G_v, M) \otimes H^1(G_v, M^*) \\
\downarrow & & \downarrow \\
H^2(G_F, M \otimes M^*) & \longrightarrow & \prod_v H^2(G_v, M \otimes M^*) \\
\downarrow & & \downarrow \\
H^2(G_F, \mu(\bar{F}^*)) & \longrightarrow & \prod_v H^2(G_v, \mu(\bar{F}_v^*)) \\
\| & & \| \\
\mathrm{Br}_F & \longrightarrow & \prod_v \mathrm{Br}_{F_v}
\end{array}$$

where all horizontal maps are restriction and the second column is the product of all of the local pairings $\langle \cdot, \cdot \rangle_v$. Note also that by Lecture 7, Proposition 3.1, the image of Br_F actually lands in $\oplus_v \mathrm{Br}_{F_v}$. Further, by Lecture 7, Theorem 3.2, Br_F is the kernel of the summation map

$$\oplus_v \mathrm{Br}_{F_v} \to \mathbb{Q}/\mathbb{Z}.$$

Now, following $h \otimes \tilde{c}$ clockwise around the diagram and then mapping by summation to $\mathbb{Q}/\mathbb{Z}$ gives the global pairing $\langle h, c \rangle$, by definition. But going counterclockwise shows that the image of $h \otimes \tilde{c}$ in $\oplus_v \mathrm{Br}_{F_v}$ lies in the image of Br_F, and thus maps to 0 under summation. This completes the proof. □

The above result is extremely useful in bounding the order of Selmer groups. We quote Mazur:

> Any Kolyvagin element $c \in H^1_s(G, M^*)$ imposes some *local condition* (at places v in its support) that must be satisfied by all Selmer elements $h \in H^1_f(G, M)$.
>
> **For example:** If the support of $c \neq 0$ is concentrated at exactly one place v_o, then any Selmer element h must have the property that $h_{v_0} \in \ker(c_{v_0}) \subset H^1_f(G_{v_0}, M)$. Here is a way of thinking about the local condition detected by this Kolyvagin element c: It tells us that we may *strengthen* the f/s structure on the Galois module M, without changing the finite part of its (1-dimensional) cohomology. That is, let us define M' to be the structured module whose underlying Galois module is M again, whose f/s structure for all places $v \neq v_0$ is equal to the f/s structure on M, but on v_0 we place a more stringent f/s structure on the G_{v_0}-module M by setting:
>
> $$H^1_f(G_{v_0}, M') := \ker\{c_{v_0} : H^1_f(G_{v_0}, M) \to \mathbb{Q}/\mathbb{Z}\} \subset H^1_f(G_{v_0}, M).$$
>
> The above discussion gives us that the finite part of the 1-dimensional cohomology of the more stringent structure M' is *equal* to the finite part of the 1-dimensional cohomology of M. Now this is already a curiously favorable state of affairs, because if we are

trying to to show that $H^1_f(G, M)$ is small, we have (by constructing the Kolyvagin element c) that

$$H^1_f(G, M') = H^1_f(G, M),$$

where M' is more stringent than M, and there is nothing to stop us from trying to do this again inductively, to force the finite cohomology to satisfy more and more stringent local conditions by finding further Kolyvagin elements for these increasingly stringent structures. In the most extreme cases one then shows that $H^1_f(G, M)$ satisfies such stringent conditions that it is forced to vanish, or else it is generated by specifically constructed cohomology classes. The efficacy of this method is determined by our ability to manufacture Kolyvagin elements with good control over their local components. This approach, combined with the following two further ideas is the underlying philosophy behind Kolyvagin's method:

(1) It is possible, at times, to judiciously enlarge the base field F without losing too much of the Selmer group, but this larger base field gives us an even better chance of constructing Kolyvagin elements.
(2) In various different contexts, one can find well-behaved collections of objects (these are the **Euler systems** of algebraic cycles, Heegner points, circular units, elements in algebraic K-groups, etc.) which produce the desired Kolyvagin elements in cohomology.

3. The Finiteness of the Selmer Group

3.1. Kummer Theory : Perfect Fields. Later in this section we will show that the Selmer group $H^1_f(G_F, M)$ is finite; we review first some Kummer theory which we will need. For the time being, let L be any field; for simplicity we assume that L is perfect. Fix an integer n and consider the exact Kummer sequence

$$1 \to \mu_n(\bar{L}^*) \to \bar{L}^* \xrightarrow{n} \bar{L}^* \to 1.$$

The long exact sequence of G_L-cohomology begins

$$1 \to \mu_n(L) \to L^* \xrightarrow{n} L^* \to H^1(G_L, \mu_n(\bar{L})) \to H^1(G_L, \bar{L}^*).$$

By Hilbert's Theorem 90, $H^1(G_L, \bar{L}^*) = 0$, so we obtain an isomorphism

$$L^*/L^{*n} \xrightarrow{\sim} H^1(G_L, \mu_n(\bar{L})).$$

Recalling the definition of the boundary map in cohomology, this map simply sends any $\alpha \in L^*$ to the cocycle

$$c : G_L \to \mu_n(\bar{L}^*)$$

given by

$$c(\sigma) = \frac{\sigma(\alpha^{1/n})}{\alpha^{1/n}};$$

it is independent of the choice of n^{th} root of α and is constant on the equivalence class of α in L^*/L^{*n} (up to coboundaries, of course).

Let us now assume that $\mu_n = \mu_n(\bar{L}^*) \subseteq L$; this is the usual situation of Kummer theory. Our above isomorphism becomes

$$L^*/L^{*n} \xrightarrow{\sim} \mathrm{Hom}(G_L, \mu_n).$$

Since μ_n is abelian of exponent n, we can rewrite our isomorphism as

$$L^*/L^{*n} \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(L'/L), \mu_n),$$

where L' is the maximal abelian extension of L of exponent n. Taking duals gives a canonical isomorphism

$$\mathrm{Gal}(L'/L) \cong \mathrm{Hom}(L^*/L^{*n}, \mu_n).$$

Let V be a subgroup of L^*/L^{*n}. Then $\mathrm{Hom}(V, \mu_n)$ is a quotient of $\mathrm{Hom}(L^*/L^{*n}, \mu_n)$, so it corresponds under our above isomorphism to a quotient of $\mathrm{Gal}(L'/L)$; this in turn corresponds to an intermediate field $L \subseteq E \subseteq L'$. This correspondance sets up a bijection between subgroups of L^*/L^{*n} and abelian extensions of L of exponent n; if V corresponds to E, then there is an isomorphism

$$\mathrm{Gal}(E/L) \cong \mathrm{Hom}(V, \mu_n).$$

Let us attempt to make this correspondance more explicit. To do this, note that $\mathrm{Gal}(L'/E)$ is precisely the subgroup of $\mathrm{Gal}(L'/L)$ mapping to 0 in $\mathrm{Hom}(V, \mu_n)$; that is, $\sigma \in \mathrm{Gal}(L'/E)$ if and only if

$$\frac{\sigma(\alpha^{1/n})}{\alpha^{1/n}} = 1$$

for all $\alpha \in L^*$ lifting elements of V. It now follows immediately from Galois theory that

$$E = L(V^{1/n}),$$

the notation meaning that E is obtained by adjoining n^{th} roots of lifts of everything in V to L. We state our results of this section as a theorem.

THEOREM 3.1. *Let L be a perfect field containing $\mu_n(L^*)$, and let L' be the maximal abelian extension of L of exponent n. Then*

$$\mathrm{Gal}(L'/L) \cong \mathrm{Hom}(L^*/L^{*n}, \mu_n).$$

Furthermore, there is a bijective correspondance between subgroups of L^*/L^{*n} and intermediate fields between L and L'; if V corresponds to E, then

$$\mathrm{Gal}(E/L) \cong \mathrm{Hom}(V, \mu_n)$$

and

$$E = L(V^{1/n}).$$

3.2. Kummer Theory : Local and Global Fields. We now take K to be a local field with uniformizer π. We continue to assume that K contains the n^{th} roots of unity. Let $V \subseteq K^*/K^{*n}$ and E/K correspond under the correspondance of Theorem 3.1. We wish to relate the ramification in E/K to V.

This is fairly easy given that $E = K(V^{1/n})$. Let α be a lift of some element of V and let β be an n^{th} root of α. E is the compositum of $K(\beta)$ for all such β, so it will be ramified over K if and only if $K(\beta)/K$ is ramified for some α.

Write $\alpha = u\pi^m$ for some unit u. Suppose first that n divides m. Then $K(\beta) = K(\beta')$, where β' is an n^{th} root of u. β' satisfies the polynomial

$$x^n - u,$$

although it may not be minimal. In any event, a standard theorem of algebraic number theory (see [**Se-LF**, Chapter 3, Section 5, Corollary 1 and Section 6, Corollary 2]) says that $K(\beta')/K$ is ramified only if nu^{n-1} is not a unit in $K(\beta')$; this occurs only if π divides n. (However, even if π divides n we can not be sure that the extension is ramified.)

On the other hand, if n does not divide m, then $K(\beta)$ must contain some non-trivial root of a uniformizer of K; this immediately implies that $K(\beta)/K$ is ramified. We rephrase our results so far as a proposition.

PROPOSITION 3.2. *Let K be a local field with uniformizer π. Suppose that K contains the n^{th} roots of unity. Let E/K be an abelian extension of exponent n corresponding to a subgroup $V \subseteq K^*/K^{*n}$. If there is an $\alpha \in V$ such that*

$$v(\alpha) \neq 0 \pmod{n},$$

where v is the normalized valuation on K, then E/K is ramified. If instead

$$v(\alpha) \equiv 0 \pmod{n}$$

for all $\alpha \in V$ and $v(n) = 0$, then E/K is unramified.

Now let F be a global field. Considering ramification locally immediately yields the following theorem.

THEOREM 3.3. *Let F be a number field containing the n^{th} roots of unity. Let E/F be an abelian extension of exponent n corresponding to a subgroup $V \subseteq F^*/F^{*n}$. Then E/F is ramified at a non-archimedean place v if there is an $\alpha \in V$ with*

$$v(\alpha) \neq 0 \pmod{n};$$

E/F is unramified at all other v except possibly those dividing n.

COROLLARY 3.4. *Let F be a number field and let S be a finite set of places of F. Let L be the maximal abelian extension of F of exponent n, unramified outside of S. Then L/F is finite.*

PROOF. Let $F' = F(\mu_n(\bar{F}^*))$. Then the corresponding extension of F' contains that of F, so we can assume that F contains the n^{th} roots of unity. In the same way we can assume that F is totally imaginary, so that the archimedean places are irrelevant.

There is a natural map

$$F^* \to \oplus_{v \text{ non-arch}} \mathbb{Z},$$

given by the valuation maps at all non-archimedean places, with kernel $\mathcal{U}$, the units of the ring of integers of F. This map descends to an exact sequence

$$0 \to \mathcal{U}/\mathcal{U}^n \to F^*/F^{*n} \to \oplus_v \mathbb{Z}/n\mathbb{Z}.$$

(The kernel is a priori $\mathcal{U}/(F^{*n} \cap \mathcal{U})$, but any element of F^* which has a power which is a unit is itself a unit.) If V is the subgroup of F^*/F^{*n} corresponding to L, then by Theorem 3.3 the image of V in each $\mathbb{Z}/n\mathbb{Z}$ factor for $v \notin S$ is zero; thus we have an exact sequence

$$0 \to V \cap \mathcal{U}/\mathcal{U}^n \to V \to \oplus_{v \in S} \mathbb{Z}/n\mathbb{Z}.$$

By Dirichlet's Theorem, $\mathcal{U}$ is finitely generated, so $\mathcal{U}/\mathcal{U}^n$ is finite. Since S is also finite, V must be finite. This implies that L/F is finite. □

3.3. The Finiteness of Selmer Groups.

THEOREM 3.5. *Let F be a number field and let M be a finite structured G_F-module. Then $H^1_f(G_F, M)$ is finite.*

PROOF. Let S be a finite set of places of F containing all places where M does not have the standard finite/singular structure; in particular, S contains all archimedean places, all places dividing the order of M, and all places where M is wildly ramified. Let us also take S to contain all places where M is at all ramified. Let M_S be the same G_F-module as M with the S-structure (see Section 1.1). Then we have

$$H^1_f(G_F, M) \subseteq H^1_f(G_F, M_S),$$

so it will be enough to prove finiteness for M_S.

Next, let L be a finite Galois extension of F which splits M; that is, such that G_L acts trivially on M. (It is easy to see that such an L exists; see Lecture 1, Section 1.1.) If L/F is ramified outside of S, then enlarge S to contain all places where L/F is ramified. Let T be the set of places of L lying above places of F in S, and let M_T be M considered as a G_L-module with the T-structure. Consider, for all places v of F and all places w of L lying over v, the maps

$$H^1(G_{F_v}, M_S) \xrightarrow{\text{res}} H^1(G_{L_w}, M_T).$$

We claim that under these maps the image of $H^1_f(G_{F_v}, M_S)$ lies in $H^1_f(G_{L_w}, M_T)$. If $v \in S$ (so $w \in T$) this is immediate; if $v \notin S$, then this follows from the commutative diagram

$$\begin{array}{ccc} H^1(\mathfrak{g}_v, M_S) & \xrightarrow{\text{res}} & H^1(\mathfrak{g}_w, M_T) \\ \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} \\ H^1(G_{F_v}, M_S) & \xrightarrow{\text{res}} & H^1(G_{L_w}, M_T) \end{array}$$

This implies that we have a natural map

$$\oplus_v H^1_s(G_{F_v}, M_S) \to \oplus_w H^1_s(G_{L_w}, M_T)$$

sitting in a commutative diagram

$$\begin{array}{ccc} H^1(G_F, M_S) & \longrightarrow & \oplus_v H^1_s(G_{F_v}, M_S) \\ \downarrow & & \downarrow \\ H^1(G_L, M_T) & \longrightarrow & \oplus_w H^1_s(G_{L_w}, M_T) \end{array}$$

We now get induced maps on the kernels of the horizontal maps, which are just the Selmer groups:

$$H^1_f(G_F, M_S) \to H^1_f(G_L, M_T).$$

Let ker be the kernel of this map; it sits in an exact commutative diagram

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \ker & \longrightarrow & H^1(\mathrm{Gal}(L/F), M) & & \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1_f(G_F, M_S) & \longrightarrow & H^1(G_F, M_S) & \longrightarrow & \oplus_v H^1_s(G_{F_v}, M_S) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^1_f(G_L, M_T) & \longrightarrow & H^1(G_L, M_T) & \longrightarrow & \oplus_w H^1_s(G_{L_w}, M_T)
\end{array}$$

It is clear from the cocycle interpretation that $H^1(\mathrm{Gal}(L/F), M)$ is finite; thus ker is also finite. It follows that it will be enough to prove that $H^1_f(G_L, M_T)$ is finite.

We are now in the situation of Lecture 7, Section 2.2: we have

$$H^1_f(G_L, M_T) = \mathrm{Hom}(G^{\mathrm{ab}}_{L,T}, M)$$

where $G^{\mathrm{ab}}_{L,T}$ is the Galois group of the maximal abelian extension of L unramified outside of T. Decomposing M as a product of cyclic groups, we see that to show this it will be enough to show that

$$\mathrm{Hom}(G^{\mathrm{ab}}_{L,T}, \mathbb{Z}/n\mathbb{Z})$$

is finite for any n.

We have

$$\mathrm{Hom}(G^{\mathrm{ab}}_{L,T}, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(L'/L), \mathbb{Z}/n\mathbb{Z}),$$

where L' is the maximal abelian extension of L of exponent n, unramified outside of T. By Corollary 3.4 we know that L' is a finite extension of L, and thus that

$$\mathrm{Hom}(\mathrm{Gal}(L'/L), \mathbb{Z}/n\mathbb{Z})$$

is finite. This completes the proof. □

CHAPTER 9

Lecture 9

1. Abelian Varieties

We will refer to the two articles [**Ro**] and [**Mi-AV**] in [**CS**] for most of the results in this section. Both articles refer to [**Mu**] for most proofs, but since we feel that attempting to read [**Mu**] is a much more demanding activity than reading the summaries in [**CS**] we will simply refer to those and let them refer the reader to the appropriate part of [**Mu**].

1.1. Complex Tori. A *complex torus* T is a compact, connected commutative Lie group over $\mathbb{C}$. Let g be its dimension, and let $\mathfrak{t}$ be the tangent space to T at the origin; we have $\mathfrak{t} \cong \mathbb{C}^g$. The exponential map

$$\exp : \mathfrak{t} \to T$$

in this situation is surjective, and since T is compact and connected the kernel Λ must be a a discrete subgroup of $\mathfrak{t} \cong \mathbb{C}^g$ of maximal rank; that is, Λ is a lattice. In this way we get a complex analytic group isomorphism

$$T \cong \mathfrak{t}/\Lambda \cong \mathbb{C}^g/\Lambda.$$

(See [**Ro**, Section 1] for details.)

Let

$$m : T \to T$$

be the multiplication by m map; it is a homomorphism since T is commutative. In fact, the identification $T \cong \mathbb{C}^g/\Lambda$ makes it clear that it is surjective, so we have an exact sequence

$$0 \to T[m] \to T \xrightarrow{m} T \to 0,$$

where $T[m]$ is the m-torsion in T. Considering T once again as $\mathbb{C}^g/\Lambda$, we find that

$$T[m] \cong \frac{1}{m}\Lambda/\Lambda \cong (\mathbb{Z}/m\mathbb{Z})^{2g},$$

the last isomorphism being non-canonical.

1.2. Abelian Varieties. An *abelian variety over a field* L is a proper, geometrically connected variety A defined over L together with a point $O \in A(L)$, a *multiplication morphism*

$$\mu : A \times A \to A$$

and an *inversion morphism*

$$\iota : A \to A,$$

both defined over L, making A into a group object in the category of proper varieties over L, with O as the identity element. (All this means is that the appropriate

[0]Last modified September 4, 2003

diagrams expressing associativity, inverses and the identity all commute. See [**Sh**, Section 2] for the diagrams.)

There are some rather remarkable consequences of this definition. First, A is nonsingular, since any variety is nonsingular on a non-empty open set and μ can be used to translate this set over all of A. Second, A is actually projective; see [**Mi-AV**, Section 7]. Lastly, the group law must be commutative; see [**Mi-AV**, Section 2]. Thus for any field $L' \supseteq L$ the L'-valued points $A(L')$ form an abelian group.

Now, suppose that L is a subfield of $\mathbb{C}$. Then $A(\mathbb{C})$ is a compact, connected (since we assumed that A was geometrically connected), commutative Lie group over $\mathbb{C}$; that is, $A(\mathbb{C})$ is a complex torus. (Not every complex torus can be given the structure of an algebraic variety; see [**Ro**, Section 3].) In particular, we have an exact sequence

$$0 \to A(\mathbb{C})[m] \to A(\mathbb{C}) \xrightarrow{m} A(\mathbb{C}) \to 0$$

as above. Recall that $A(\mathbb{C})[m] \cong (\mathbb{Z}/m\mathbb{Z})^{2g}$, where g is the dimension of A.

LEMMA 1.1. *Every point of $A(\mathbb{C})[m]$ actually lies in $A(L')$ for some finite extension L' of L.*

PROOF. Let P be an m-torsion point over $\mathbb{C}$. Since μ and thus $m : A \to A$ is defined over L,

$$m(P^\sigma) = m(P)^\sigma = 0$$

for any $\sigma \in \mathrm{Aut}(\mathbb{C}/L)$. In particular, all of the conjugate points to P are also in $A(\mathbb{C})[m]$. Thus P has only finitely many conjugates over L, which implies that it is defined over a finite extension of L. □

In particular, $A(\mathbb{C})[m] = A(\bar{L})[m]$. This is not exactly what one would like; the optimal situation would be to define a projective algebraic group $A[m]$ over L by

$$A[m] = A \times_A 0,$$

where the map $A \to A$ is multiplication by m and 0 is the trivial abelian variety over L. (Intuitively this is the correct notion, since a point in $A \times_A 0$ is an ordered pair $(a, 0)$ where a maps to 0 under multiplication by m.) One then would want to show that the morphism $A \xrightarrow{m} A$ is surjective with finite kernel (such a map is called an *isogeny*), so that $A[m]$ is a *finite* projective algebraic group over L. (Recall that a map $f : A \to B$ of abelian varieties over L is surjective if it satisfies any of the following equivalent conditions:

(1) f is surjective as a map of topological spaces;
(2) $f : A(\bar{L}) \to B(\bar{L})$ is surjective as a map of abelian groups;
(3) the induced map between the étale sheaves defined by A and B is surjective.)

This program can actually be carried out over an arbitrary field L; one finds that multiplication by m is an isogeny of degree m^{2g} and that it is étale if and only if the characteristic of L does not divide m. In particular, $A[m]$ has all points in $\bar{L}$, and

$$A[m](\bar{L}) \cong (\mathbb{Z}/m\mathbb{Z})^{2g},$$

assuming that the characteristic of L does not divide m. See [**Mi-AV**, Section 8] for more details. (There may be fewer points in $A[m](\bar{L})$ when the characteristic of L divides m.)

The usefulness of our above results is that we have obtained a well-behaved $\mathrm{Gal}(\bar{L}/L)$-module $A[m](\bar{L})$; in fact, by an easy variant of Lemma 1.1 it is actually discrete.

2. Selmer Groups of Abelian Varieties

2.1. Definitions. Let F be a global field, let A be an abelian variety defined over F and let m be an integer. Since multiplication by m is surjective, we have an exact sequence

$$0 \to A[m](\bar{F}) \to A(\bar{F}) \xrightarrow{m} A(\bar{F}) \to 0.$$

We saw in the previous section that $A[m](\bar{F})$ is a finite, discrete G_F-module, so we can apply all of the theory we have developed to it. We will write it (only slightly ambiguously) just as $A[m]$.

Consider the portion of the long exact cohomology sequence

$$A(F) \xrightarrow{m} A(F) \to H^1(G_F, A[m]) \to H^1(G_F, A) \xrightarrow{m} H^1(G_F, A)$$

We can reduce this to a short exact sequence

$$0 \to A(F)/mA(F) \to H^1(G_F, A[m]) \to H^1(G_F, A)[m] \to 0.$$

If we are interested in the arithmetic of $A(F)$, this exact sequence is a good start; we have expressed a quotient of $A(F)$ as a subgroup of a cohomology group. Unfortunately, both of the cohomology groups in the exact sequence are quite large. We will use local considerations to replace them by much smaller subgroups.

To do this, we consider the composition

$$H^1(G_F, A[m]) \to H^1(G_F, A(\bar{F})) \to \prod_v H^1(G_v, A(\bar{F}_v)),$$

where the last map is the product of the restriction maps over all places v of F. The groups we are looking for are the kernel of the second map and the kernel of the composition.

Definition 5. The m^{th} *Selmer group* $\mathcal{S}_m(A/F)$ is defined by

$$\mathcal{S}_m(A/F) = \ker\left(H^1(G_F, A[m]) \to \prod_v H^1(G_v, A(\bar{F}_v))\right),$$

the map being the composition above. The *Shafarevich-Tate group* $Ш(A/F)$ is defined by

$$Ш(A/F) = \ker\left(H^1(G_F, A(\bar{F})) \to \prod_v H^1(G_v, A(\bar{F}_v))\right).$$

By their definitions, $\mathcal{S}_m(A/F)$ and $Ш(A/F)$ fit into an exact commutative diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & 0 \\
 & & & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & A(F)/mA(F) & \longrightarrow & \mathcal{S}_m(A/F) & \longrightarrow & Ш(A/F) & \xrightarrow{m} & Ш(A/F) \\
 & & \| & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & A(F)/mA(F) & \longrightarrow & H^1(G_F, A[m]) & \longrightarrow & H^1(G_F, A(\bar{F})) & \xrightarrow{m} & H^1(G_F, A(\bar{F})) \\
 & & & & & & \downarrow & & \downarrow \\
 & & & & & & \prod_v H^1(G_v, A(\bar{F}_v)) & \xrightarrow{m} & \prod_v H^1(G_v, A(\bar{F}))
\end{array}$$

Exactness of the top row follows from a simple diagram chase. Extracting that row, we obtain the fundamental exact sequence

$$0 \to A(F)/mA(F) \to \mathcal{S}_m(A/F) \to Ш(A/F)[m] \to 0.$$

2.2. The Abelian Variety Structure on $A[m]$. The next step is to endow $A[m]$ with a suitable finite/singular structure (in the sense of Lecture 7, Section 1.2) so that we can apply our general theory. In fact, by choosing all of the local structures correctly we will identify $H^1_f(G_F, A[m])$ with the m^{th} Selmer group $\mathcal{S}_m(A/F)$; Theorem 3.3 of Lecture 8 will then have immediate important arithmetic consequences.

To define this structure, we want to extend the bottom row of our above commutative diagram by using the local versions

$$0 \to A(F_v)/mA(F_v) \to H^1(G_v, A[m]) \to H^1(G_v, A)[m] \to 0$$

of our original exact sequence

$$0 \to A(F)/mA(F) \to H^1(G_F, A[m]) \to H^1(G_F, A)[m] \to 0.$$

(Note that the $A[m]$ notation is not really ambiguous here, since we have chosen an embedding $\bar{F} \subseteq \bar{F}_v$.) We obtain a commutative diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & 0 \\
 & & & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & A(F)/mA(F) & \longrightarrow & \mathcal{S}_m(A/F) & \longrightarrow & Ш(A/F) & \xrightarrow{m} & Ш(A/F) \\
 & & \| & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & A(F)/mA(F) & \longrightarrow & H^1(G_F, A[m]) & \longrightarrow & H^1(G_F, A(\bar{F})) & \xrightarrow{m} & H^1(G_F, A(\bar{F})) \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \prod_v A(F_v)/mA(F_v) & \longrightarrow & \prod_v H^1(G_v, A[m]) & \longrightarrow & \prod_v H^1(G_v, A(\bar{F}_v)) & \xrightarrow{m} & \prod_v H^1(G_v, A(\bar{F}_v))
\end{array}$$

with exact rows, although at the moment we only know that the last two columns are exact. After a little bit of comtemplation of the above diagram and the definition of $\mathcal{S}_m(A/F)$ it becomes clear what the appropriate finite/singular structure should be.

DEFINITION 6. We define the *abelian variety structure* on $A[m]$ to be the finite/singular structure σ defined by the local exact sequences

$$\sigma_v : 0 \to A(F_v)/mA(F_v) \to H^1(G_v, A[m]) \to H^1(G_v, A)[m] \to 0;$$

that is, we define

$$H^1_f(G_v, A[m]) = \mathrm{im}\big(A(F_v)/mA(F_v) \hookrightarrow H^1(G_v, A[m])\big)$$

and

$$H^1_s(G_v, A[m]) = \mathrm{im}\big(H^1(G_v, A[m]) \to H^1(G_v, A)\big).$$

The exact sequence

$$0 \to A(F_v)/mA(F_v) \to H^1(G_v, A[m]) \to H^1(G_v, A)$$

shows that these definitions are compatible. It is not immediately clear, however, that σ is really a finite/singular structure. We will prove this in the next lecture; for the time being we derive some consequences.

PROPOSITION 2.1. *If F is a number field, A/F is an abelian variety and $A[m]$ is endowed with the abelian variety structure σ, then*

$$H^1_f(G_F, M_\sigma) = \mathcal{S}_m(A/F).$$

PROOF. This is just an easy diagram/definition chase in the above diagram. □

COROLLARY 2.2. *The m^{th} Selmer group $\mathcal{S}_m(A/F)$ is finite.*

PROOF. This follows immediately from Proposition 2.1 and Theorem 3.3 of Lecture 8. □

COROLLARY 2.3 (The Weak Mordell-Weil Theorem). *If A is abelian variety and F is a number field, then $A(F)/mA(F)$ is finite for any integer m.*

The full Mordell-Weil theorem states that $A(F)$ is a finitely generated abelian group; to derive this from Corollary 2.3 one must use the theory of height functions. (See [**Si-AEC**, Chapter 8, Sections 5 and 6] or [**Si-H**].)

COROLLARY 2.4. *The m-torsion in $Ш(A/F)$ is finite for any m.*

$\mathcal{S}_m(A/F)$ itself is effectively computable in many cases; see [**Si-AEC**, Chapter 10, Section 1] for the case of elliptic curves with 2-torsion. More recent work of Schaffer and Grant has given good algorithms for computing it for abelian varieties of dimension 1 or 2, independent of any other hypotheses.

To relate $\mathcal{S}_m(A/F)$ to $A(F)/mA(F)$ requires knowledge of $Ш(A/F)$, however, and this group has proved much more resistant to computation. Note that Corollary 2.4 does not imply that $Ш(A/F)$ itself is finite. That $Ш(A/F)$ is finite is a standard conjecture; it was not known for a single abelian variety over a number field until the work of Karl Rubin in 1986. He showed that it was finite for elliptic curves over $\mathbb{Q}$ with complex multiplication and analytic rank 0 or 1. (See [**Ru-TS**].) It is now known, using the work of Kolyvagin, Gross-Zagier, Murty-Murty and Bump-Friedberg-Hoffstein, for all modular elliptic curves over $\mathbb{Q}$ of analytic rank 0 or 1. (See [**Ko**], [**GZ**], [**MM**], [**BFH**].)

Note that knowledge of $A(F)_{\mathrm{tors}}$ and $A(F)/mA(F)$ for a single $m > 1$ determines the abelian group structure of $A(F)$. Alternately, knowledge of $A(F)/mA(F)$ for a few values of m would suffice. Nevertheless, we know very little about the

rank of $A(F)$ in general. For example, although it is relatively easy to construct infinite families of abelian varieties over $\mathbb{Q}$ of rank r and dimension g such that

$$\frac{r}{g} \geq 1$$

for all sufficiently large g, it is not known how to extend these constructions to give

$$\frac{r}{g} \geq 1 + \varepsilon$$

for any ε.

CHAPTER 10

Lecture 10

1. Kummer Theory

1.1. The Ring of S-Integers. We present in this section an alternative (and more precise) approach to Kummer theory over global fields. Let F be a number field and let S be a finite set of primes of F. (Later, when we assume that S contains all of the archimedean places, there will be times when only the non-archimedean places are relevant and our notation may not reflect this. We leave these issues to the reader to sort out. Also, we will use both $\mathfrak{p}$ and v to denote primes, depending on the context.) Let $\mathcal{O}_F$ be the ring of integers of F. We define the *ring of S-integers*, $\mathcal{O}_{F,S}$, by

$$\mathcal{O}_{F,S} = \{x \in F \mid \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

That is, $\mathcal{O}_{F,S}$ consists of those elements of F which are integral away from S and arbitrary in S.

Intuitively, then, $\mathcal{O}_{F,S}$ is just the localization of $\mathcal{O}_F$ at an element of F divisible exactly by the primes in S. However, since $\mathcal{O}_F$ need not be a principal ideal domain, it is not immediately clear that such an element exists. That they do in fact exist follows from the finiteness of the ideal class group. (See [**La-ANT**, Chapter 5, Section, pp. 100-101].) Specifically, let $\mathfrak{p}$ be a prime in S. Then, since the ideal class group of $\mathcal{O}_F$ is finite, $\mathfrak{p}^n$ is principal for some n, say $\mathfrak{p}^n = \alpha_{\mathfrak{p}}\mathcal{O}_F$. Setting

$$\alpha = \prod_{\mathfrak{p} \in S} \alpha_{\mathfrak{p}},$$

we see that

$$\mathcal{O}_{F,S} = \mathcal{O}_F[\alpha].$$

This description gives an immediate determination of the primes of $\mathcal{O}_{F,S}$: they are simply the primes of $\mathcal{O}_F$ which are not in S. It also now follows immediately that the localizations and completions of $\mathcal{O}_F$ and $\mathcal{O}_{F,S}$ at primes $\mathfrak{p} \notin S$ agree. Essentially, then, $\mathcal{O}_{F,S}$ has none of the information of $\mathcal{O}_F$ about $\mathfrak{p} \in S$, but has all of it for $\mathfrak{p} \notin S$.

The following theorem is one of two fundamental finiteness results for $\mathcal{O}_{F,S}$.

THEOREM 1.1 (Dirichlet Unit Theorem). *$\mathcal{O}_{F,S}^*$ is a finitely generated abelian group. More precisely, $\mathcal{O}_{F,S}^*/\mu(F^*)$ is free abelian of rank $r_1 + r_2 + |S| - 1$, where r_1 is the number of real embeddings of F and r_2 is the number of pairs of complex conjugate embeddings.*

PROOF. See [**La-ANT**, Chapter 5, Section 1, Corollary of p. 105]. □

[0]Last modified September 4, 2003

In order to state the other finiteness result, which is just a slight generalization of the finiteness of the ideal class group, we first must define locally free modules over $\mathcal{O}_{F,S}$. We will say that an $\mathcal{O}_{F,S}$-module V is *locally free* if

$$V_v = V \otimes_{\mathcal{O}_{F,S}} (\mathcal{O}_{F,S})_v = V \otimes_{\mathcal{O}_{F,S}} \mathcal{O}_{F_v}$$

is free as an $\mathcal{O}_{F_v}$-module for all $v \notin S$. (This is equivalent to V being free over all of the localizations of $\mathcal{O}_{F,S}$, rather than going all the way to the completions.) We define the *Picard group* $\mathrm{Pic}(\mathcal{O}_{F,S})$ of $\mathcal{O}_{F,S}$ to be the set of isomorphism classes of finitely generated $\mathcal{O}_{F,S}$-modules which are locally free of rank 1. $\mathrm{Pic}(\mathcal{O}_{F,S})$ is made into a group by tensor product; it is easy to see that the tensor product of two finitely generated locally free of rank 1 $\mathcal{O}_{F,S}$-modules is of the same form. Inverses are given simply by duals,

$$V^{-1} = \mathrm{Hom}_{\mathcal{O}_{F,S}}(V, \mathcal{O}_{F,S}),$$

as is easy to check. (For a more geometric treatment of the Picard group, see [**Ha**, Chapter 2, Section 6, esp. Remark 6.3.2 and pp. 143-146].)

$\mathrm{Pic}(\mathcal{O}_{F,S})$ also has an interpretation in terms of ideals. Recall that a *fractional ideal* of $\mathcal{O}_{F,S}$ is a non-zero finitely-generated sub-$\mathcal{O}_{F,S}$-module of F. The fractional ideals are made into a group by multiplication. This group is simply free abelian on the primes of F not in S. A fractional ideal is said to be *principal* if it is of the form $x\mathcal{O}_{F,S}$ for some $x \in F^*$.

Proposition 1.2. *There is a canonical isomorphism between* $\mathrm{Pic}(\mathcal{O}_{F,S})$ *and the group of fractional ideals of* $\mathcal{O}_{F,S}$ *modulo principal fractional ideals.*

Proof. For a proof in the context of divisors and invertible sheaves, see [**Ha**, Chapter 2, Section 6, Proposition 6.15]. We give a purely algebraic proof.

There is a natural map from the group of fractional ideals to $\mathrm{Pic}(\mathcal{O}_{F,S})$, simply considering a fractional ideal as a locally free $\mathcal{O}_{F,S}$-module. The kernel of the map is easily seen to be the principal fractional ideals, so we are left to show that the map is surjective.

Let V be a locally-free $\mathcal{O}_{F,S}$-module of rank 1. We claim that

$$V \otimes_{\mathcal{O}_{F,S}} F \cong F.$$

To see this, choose any prime $\mathfrak{p}$ not in S and let R be the localization of $\mathcal{O}_{F,S}$ at $\mathfrak{p}$. Then

$$V \otimes_{\mathcal{O}_{F,S}} F \cong (V \otimes_{\mathcal{O}_{F,S}} R) \otimes_R F \cong R \otimes_R F \cong F,$$

since V is locally free. (Note that here we only used the fact that V is locally free at one prime.)

Given this isomorphism, we tensor the injection

$$\mathcal{O}_{F,S} \hookrightarrow F$$

with the flat (since it is locally free) $\mathcal{O}_{F,S}$-module V to get an injection

$$V \hookrightarrow V \otimes_{\mathcal{O}_{F,S}} F \cong F,$$

which realizes V as a submodule of F, and thus, since it is finitely generated, as a fractional ideal. □

Corollary 1.3. $\mathrm{Pic}(\mathcal{O}_{F,S})$ *is finite.*

PROOF. It is a standard fact that the ideal class group of $\mathcal{O}_F$ is finite; thus, $\mathrm{Pic}(\mathcal{O}_F)$ is finite. The finiteness for $\mathrm{Pic}(\mathcal{O}_{F,S})$ follows immediately, since under the isomorphism of Proposition 1.2 $\mathrm{Pic}(\mathcal{O}_{F,S})$ can be identified with a subquotient of $\mathrm{Pic}(\mathcal{O}_F)$. □

In fact, one sees easily from the proof of the corollary that by taking S large enough to kill everything in $\mathrm{Pic}(\mathcal{O}_F)$ we get $\mathrm{Pic}(\mathcal{O}_{F,S}) = 0$. More precisely, one only has to choose representative ideals of $\mathrm{Pic}(\mathcal{O}_F)$ and let S contain every prime divisor of each representative.

1.2. The Kummer map. Let $N \geq 1$ be an integer and let F be a number field such that $\mu_N(\bar{F}) \subseteq F^*$; we will just write μ_N for $\mu_N(\bar{F})$. Let S be a set of places of F containing all of the archimedean places and all places of F dividing N. We wish to define a natural map

$$\mathcal{O}_{F,S}^*/\mathcal{O}_{F,S}^{*N} \to \mathrm{Hom}(G_{F,S}^{\mathrm{ab}}, \mu_N).$$

Here $G_{F,S}^{\mathrm{ab}}$ is the Galois group of the maximal abelian extension of F unramified outside of S.

Let u be in $\mathcal{O}_{F,S}^*$. Fix a $\xi \in \bar{F}$ such that $\xi^N = u$. (Normally making such a choice is a very bad idea, but we will see that since $\mu_N \subseteq F^*$ the choice will not matter.) Note that ξ is actually in the maximal abelian extension of F unramified outside of S, since $F(\xi)/F$ is cyclic of order dividing N with discriminant dividing $N\xi^{N-1}$. Since ξ is a unit away from S, $F(\xi)/F$ can only be ramified at places in S.

Define $\varphi_u \in \mathrm{Hom}(G_{F,S}^{\mathrm{ab}}, \mu_N)$ by

$$\varphi_u(g) = \frac{g(\xi)}{\xi}.$$

Note first that since the conjugates of ξ are just $\zeta\xi$ for various $\zeta \in \mu_N$, φ_u really does have image in μ_N. In fact, the map φ_u is independent of the choice of N^{th} root of u: the fact that $\mu_N \subseteq F^*$ implies that any $g \in G_{F,S}^{\mathrm{ab}}$ acts trivially on μ_N, so

$$\frac{g(\zeta\xi)}{\zeta\xi} = \frac{\zeta g(\xi)}{\zeta\xi} = \frac{g(\xi)}{\xi}.$$

Thus we have a canonical map

$$\mathcal{O}_{F,S}^* \to \mathrm{Hom}(G_{F,S}^{\mathrm{ab}}, \mu_N),$$

and it is easily seen to be a homomorphism (using the fact that we can use any N^{th} root of u to define φ_u). Furthermore, $u \in \mathcal{O}_{F,S}^*$ defines the trivial homomorphism on $G_{F,S}^{\mathrm{ab}}$ if any only if

$$g(\xi) = \xi$$

for all $g \in G_{F,S}^{\mathrm{ab}}$, where $\xi^N = u$. By Galois theory this happens if and only if $\xi \in F$; thus we have defined a natural injection

$$\mathcal{O}_{F,S}^*/\mathcal{O}_{F,S}^{*N} \to \mathrm{Hom}(G_{F,S}^{\mathrm{ab}}, \mu_N).$$

The determination of the cokernel, however, is somewhat more difficult.

1.3. Preparation for Descent. In order to determine the cokernel of the map of the previous section we must introduce the notion of twisting locally free modules. We begin with some easier examples.

Let K be any field and let L be a finite Galois extension, with Galois group G of order d. Then L is a K-vector space of dimension d on which G acts K-linearly. Thus L is a K-representation space for G; in other words L is a $K[G]$-module. In fact, L is just the regular representation; that is, L is a free $K[G]$-module of rank 1. This follows immediately from the normal basis theorem ([**La-Al**]).

In particular, suppose G is abelian and let $\varphi : G \to K^*$ be a character. Define the *φ-representation space* of L by

$$L^\varphi = \{x \in L \mid g(x) = \varphi(g)x \text{ for all } g \in G\}.$$

Identifying L with $K[G]$, we find that

$$\begin{aligned} L^\varphi \cong & K[G]^\varphi \\ &= \left\{ \sum_{g\in G} a_g g \in K[G] \mid \sum a_g hg = \sum \varphi(h) a_g g \text{ for all } h \in G \right\} \\ &= \left\{ \sum a_g g \in K[G] \mid a_g = \varphi(g^{-1})a_1 \text{ for all } g \in G \right\} \\ &= \left\{ a \sum \varphi(g^{-1}) g \right\}, \end{aligned}$$

so L^φ is one dimensional over K.

Restrict now to the case where K is a local field. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the rings of integers of K and L respectively. Then $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank d as well as a $\mathcal{O}_K[G]$-module. However, it is not always free of rank 1 over $\mathcal{O}_K[G]$, since the normal basis theorem does not apply to rings of integers. In fact, it can be shown that if L/K is unramified, then there is a form of the normal basis theorem for the ring of integers and $\mathcal{O}_L \cong \mathcal{O}_K[G]$ as $\mathcal{O}_K[G]$-modules.

Suppose that L/K is an arbitrary finite abelian extension of local fields and that V is an $\mathcal{O}_K$-module which is free of rank 1. Let $\varphi : G \to \mathcal{O}_K^*$ be a character of G. (Any character of G to K^* must land in $\mathcal{O}_K^*$ since its image is just roots of unity, which are integral.) We define the *φ-representation space* of V by

$$\begin{aligned} V^\varphi &= (V \otimes_{\mathcal{O}_K} \mathcal{O}_L)^\varphi \\ &= \{v \otimes x \in V \otimes_{\mathcal{O}_K} \mathcal{O}_L \mid v \otimes g(x) = \varphi(g)(v \otimes x) \text{ for all } g \in G\}. \end{aligned}$$

We know that V^φ is torsion-free, since it is a submodule of $V \otimes_{\mathcal{O}_K} \mathcal{O}_L$, which is free of rank n over $\mathcal{O}_K$. Thus, since $\mathcal{O}_K$ is a principal ideal domain, V^φ is free. In fact, it is easy to show that $V^\varphi \otimes_{\mathcal{O}_K} K \cong K^\varphi$, so that the rank must be 1.

1.4. Descent for Global Fields. We now return to the case where F is a global field containing μ_N and S is a finite set of places containing the archimedean places and the places dividing N. We will define a map

$$\mathrm{Hom}(G_{F,S}^{\mathrm{ab}}, \mu_N) \to \mathrm{Pic}(\mathcal{O}_{F,S}).$$

We first work in slightly more generality. Let V be a locally free $\mathcal{O}_{F,S}$-module and let φ be in $\mathrm{Hom}(G_{F,S}^{\mathrm{ab}}, \mu_N)$. Since μ_N is finite, φ factors through some finite

extension L/F, which we can take to be abelian and unramified outside of S:

$$\begin{array}{ccc} G_{F,S}^{\mathrm{ab}} & \twoheadrightarrow & \mathrm{Gal}(L/F) \\ \downarrow{\scriptstyle \varphi} & \swarrow{\scriptstyle \varphi} & \\ \mu_N & & \end{array}$$

Let T be the set of places of L lying above places of S. Then $\mathcal{O}_{L,T}$ is an $\mathcal{O}_{F,S}$-module. We define the *φ-representation space* of V by

$$\begin{aligned} V^{\varphi} &= (V \otimes_{\mathcal{O}_{F,S}} \mathcal{O}_{L,T})^{\varphi} \\ &= \{v \otimes x \in V \otimes_{\mathcal{O}_{F,S}} \mathcal{O}_{L,T} \mid v \otimes g(x) = \varphi(g)(v \otimes x) \text{ for all } g \in G\}. \end{aligned}$$

For example,

$$\mathcal{O}_{F,S}^{\varphi} = \{x \in \mathcal{O}_{L,T} \mid g(x) = \varphi(g)x \text{ for all } g \in G\}.$$

For general V, V^{φ} is just

$$V^{\varphi} = V \otimes_{\mathcal{O}_{F,S}} \mathcal{O}_{F,S}^{\varphi}.$$

Note first that the $\mathcal{O}_{F,S}$-modules V^{φ} defined by different choices of splitting fields are canonically isomorphic, so that the above definition makes sense. Note also that if V is locally free of rank 1, then so is V^{φ}; this follows from the local computations of the previous section.

Thus, we can define the desired map

$$\mathrm{Hom}(G_{F,S}^{\mathrm{ab}}, \mu_N) \to \mathrm{Pic}(\mathcal{O}_{F,S})$$

by sending φ to $\mathcal{O}_{F,S}^{\varphi}$. It is easy to check from the definitions that this is a homomorphism, using the fact that the definition is independent of the choice of splitting field.

THEOREM 1.4. *There is a natural exact sequence*

$$1 \to \mathcal{O}_{F,S}^{*}/\mathcal{O}_{F,S}^{*N} \to \mathrm{Hom}(G_{F,S}^{\mathrm{ab}}, \mu_N) \to \mathrm{Pic}(\mathcal{O}_{F,S})[N] \to 1$$

where the maps are as defined above.

PROOF. We already know that the first map is injective. Next we show that the composition of the maps is zero. So let u be in $\mathcal{O}_{F,S}^{*}$ and let ξ be an N^{th} root. We wish to show that $\mathcal{O}_{F,S}^{\varphi_u}$ is isomorphic to $\mathcal{O}_{F,S}$. Set $L = F(\xi)$ (which is indeed abelian and unramified outside of S since $\mu_n \subseteq F^*$ and S contains the places dividing N) and note that

$$\begin{aligned} \mathcal{O}_{F,S}^{\varphi_u} &= \{x \in \mathcal{O}_{L,T} \mid g(x) = \varphi_u(g)x \text{ for all } g \in G\} \\ &= \{x \in \mathcal{O}_{L,T} \mid g(x) = \frac{g(\xi)}{\xi}x \text{ for all } g \in G\} \\ &= \{x \in \mathcal{O}_{L,T} \mid g\left(\frac{x}{\xi}\right) = \frac{x}{\xi} \text{ for all } g \in G\}. \end{aligned}$$

From this one sees easily that the map

$$\mathcal{O}_{F,S}^{\varphi} \to \mathcal{O}_{F,S}$$

given by multiplication by ξ^{-1} is an isomorphism.

To show that the last map is surjective we use the interpretation of $\mathrm{Pic}(\mathcal{O}_{F,S})$ in terms of fractional ideals. So let I be a fractional ideal such that I^N is trivial. Thus $I^N = \alpha\mathcal{O}_{F,S}$ for some $\alpha \in F^*$. Choose an N^{th} root ξ of α and set $L = F(\xi)$.

Then L/F is unramified outside of S since α is the N^{th} power of a fractional ideal of $\mathcal{O}_{F,S}$. (This criterion for ramification becomes quite transparent when viewed locally.) Define

$$\varphi : G_{F,S}^{\text{ab}} \to \mu_N$$

by

$$\varphi(g) = \frac{g(\xi)}{\xi}.$$

Then φ factors through $\text{Gal}(L/K)$. We claim that $\mathcal{O}_{F,S}^{\varphi} \cong I$. To see this, first do a computation as above to show that

$$\mathcal{O}_{F,S}^{\varphi} = \xi \mathcal{O}_{F,S}.$$

To check that $\xi\mathcal{O}_{F,S}$ and I are isomorphic it is enough to check that they agree as fractional ideals of L, since L/K is unramified outside of S. But this is clear, which establishes surjectivity.

Finally, let $\varphi : G_{F,S}^{\text{ab}} \to \mu_N$ be such that $\mathcal{O}_{F,S}^{\varphi}$ is trivial in $\text{Pic}(\mathcal{O}_{F,S})[N]$. Thus there is an isomorphism

$$\mathcal{O}_{F,S}^{\varphi} \cong \mathcal{O}_{F,S}.$$

Let ξ be the element of $\mathcal{O}_{F,S}^{\varphi}$ corresponding to $1 \in \mathcal{O}_{F,S}$ under this isomorphism. One easily checks that φ is given simply by

$$\varphi(g) = \frac{g(\xi)}{\xi},$$

and that $\mathcal{O}_{F,S}^{\varphi} = \xi\mathcal{O}_{F,S}$. ξ may not be a unit, but we note that the fractional ideal of $\mathcal{O}_{F,S}$ it defines is trivial by hypothesis. Thus we can modify ξ by an element of $\mathcal{O}_{F,S}$ to get a unit ξ' of $\mathcal{O}_{L,T}$. Now $(\xi')^N \in \mathcal{O}_{F,S}^*$ and ξ' yields the same homomorphism φ, which completes the proof of exactness. □

2. Cohomology of Abelian Varieties

2.1. Lang's Theorem. Recall that if A is an abelian variety over a field K, we have an exact sequence of G_K-modules

$$0 \to A[N] \to A(\bar{K}) \xrightarrow{N} A(\bar{K}) \to 0,$$

where N is any positive integer prime to the characteristic of K and $A[N]$ is the N-torsion in $A(\bar{K})$. The long exact sequence in G_K-cohomology yields an exact sequence

$$0 \to A(K)/NA(K) \to H^1(G_K, A[N]) \to H^1(G_K, A(\bar{K}))[N] \to 0.$$

In order to understand this exact sequence it is important to gain more control over $H^1(G_K, A(\bar{K}))$. An important result in this direction is Lang's theorem.

THEOREM 2.1 (Lang). *Let A be a smooth, connected, commutative algebraic group over a finite field k. Then*

$$H^1(\mathfrak{g}_k, A(\overline{k})) = 0.$$

PROOF. We sketch the proof, the underlying idea being to "think geometrically". For details see [**Car**, p. 32] or [**PR**, Chapter 6, Section 2].

Recall that we have evaluated the cohomology group $H^1(\mathfrak{g}_k, A(\overline{k}))$ as

$$H^1(\mathfrak{g}_k, A(\overline{k})) \cong A(\overline{k})/(\text{Fr} - 1)A(\overline{k}),$$

where Fr is the Frobenius automorphism $x \mapsto x^q$, $q = |k|$. So we want to show that

$$\mathrm{Fr} - 1 : A(\overline{k}) \to A(\overline{k})$$

is surjective. To do this we want to interpret Fr geometrically and then see that $\mathrm{Fr} - 1$ is surjective.

We begin by considering the category of commutative k-algebras. If R is such an algebra, then there is a natural k-linear automorphism of R

$$\mathrm{Fr} : R \to R$$

given by $x \mapsto x^q$. Under the natural equivalence of categories between k-algebras and affine schemes over $\operatorname{Spec} k$ this yields a $\operatorname{Spec} k$-automorphism Fr for $\operatorname{Spec} R$.

Let X now be an arbitrary scheme over $\operatorname{Spec} k$. Let $U = \operatorname{Spec} R$ and $V = \operatorname{Spec} S$ be two affine open subsets of X. In order to show that the automorphisms Fr glue to an automorphism of X it will be enough to show that they agree for any $W = \operatorname{Spec} R_r = \operatorname{Spec} S_s$, $r \in R$, $s \in S$. But this is clear, since Fr is given by the same p-power map in both instances. Thus we obtain a natural automorphism Fr on any $\operatorname{Spec} k$-scheme X. (See [**Ha**, Chapter 4, Section 2, p. 301] for a slightly different approach to defining Fr. Note that in our situation we simply have $X_p = X$.)

The first key point is to observe that Fr induces the zero map on differentials. The essential reason for this is that on the level of differentials, the map induced by Fr involves multiplication by q, which kills any k-algebra; see [**Si-AEC**, Chapter 2].

Now, let A be an algebraic group. Consider the morphism $A \to A$ which "sends $x \in A$ to $x^{-1}\,\mathrm{Fr}(x)$." (We leave it to the reader to write this down algebraically in terms of the multiplication, inversion and Frobenius morphisms.) We will simply write this morphism as $\mathrm{Fr} - 1$. One now shows that the induced map on differentials is just the sum of the maps induced by Fr and by -1; since Fr induces the zero map and -1 induces isomorphisms, $\mathrm{Fr} - 1$ induces isomorphisms on differentials. Since A is smooth, [**Ha**, Chapter 3, Section 10, Proposition 10.4] now implies that $\mathrm{Fr} - 1$ is étale . Thus, by [**Mi-EC**, Chapter 1, Section 2, Theorem 2.12], it has open image.

Further suppose that A is connected. Choose any $a \in A(\overline{k})$ and consider the map ψ_a sending $x \in A(\overline{k})$ to $x^{-1}a\,\mathrm{Fr}(x)$. This is just the translation of $\mathrm{Fr} - 1$ by a, and thus also has open image. In particular, the image of ψ_a intersects that of $\mathrm{Fr} - 1$, since any two opens on a connected variety intersect. Thus there must be $x_1, x_2 \in A(\overline{k})$ such that

$$(\mathrm{Fr} - 1)(x_1) = \psi_a(x_2)$$

and a little algebra now shows that

$$(\mathrm{Fr} - 1)(x_1 x_2^{-1}) = a.$$

Thus $\mathrm{Fr} - 1$ is surjective, as claimed. □

Corollary 2.2. *If A is an abelian variety over a finite field k, then*

$$A(k)/NA(k) \cong H^1(\mathfrak{g}_k, A[N])$$

for any integer N.

Proof. This follows immediately from Theorem 2.1 and the Kummer sequence. □

2.2. Abelian Schemes over Local Fields. Let S be a scheme. An *abelian scheme* over S is a proper, smooth group scheme over S with connected geometric fibers. (As usual, see [**Sh**, Section 2] for the relevant diagrams.) In particular, for every S scheme X, the set

$$A(X) \stackrel{\text{def}}{=} \text{Hom}_S(X, A)$$

of X-valued points of A is a group; in fact, it turns out that the group structure must be commutative. (See [**Mi-AV**, Section 20, Corollary 20.2]. If $T = \text{Spec}\, R$ is affine we will often just write $A(R)$ for $A(T)$.) Note first that if T is an S-scheme, then

$$A(T) = (A \times_S T)(T),$$

as follows immediately from the universal property of the fiber product. Also, in the case that S is the spectrum of a field K, then an abelian scheme over S is the same as an abelian variety over S; thus any such abelian scheme is necessarily projective, and under any projective embedding it is easy to check that the above notion of $\text{Spec}\, K$-valued points corresponds with the usual notion of points in projective space.

Let K be a local field with ring of integers $\mathcal{O}_K$ and residue field k. Let A be abelian variety over $\text{Spec}\, K$. We will say that A has *good reduction* if it extends to an abelian scheme over $\text{Spec}\, \mathcal{O}_K$; that is, if there is some abelian scheme A' over $\text{Spec}\, \mathcal{O}_K$ such that

$$A' \times_{\text{Spec}\, \mathcal{O}_K} \text{Spec}\, K \cong A.$$

A fundamental result for abelian varieties with good reduction is that all $\text{Spec}\, \mathcal{O}_K$-valued points extend to $\text{Spec}\, K$-valued points. Intuitively the idea is that any point in projective space over K can be "scaled" to have at least one coordinate integral. We give a "coordinate-free" proof instead.

PROPOSITION 2.3. *Let A be an abelian scheme over $\mathcal{O}_K$. Then the natural map $A(\mathcal{O}_K) \to A(K)$ is a bijection.*

PROOF. The valuative criterion for properness ([**Ha**, Chapter 2, Theorem 4.7]) tells us that given any diagram

$$\begin{array}{ccc} \text{Spec}\, K & \longrightarrow & A \\ \downarrow & & \downarrow \\ \text{Spec}\, \mathcal{O}_K & \longrightarrow & \text{Spec}\, \mathcal{O}_K \end{array}$$

there is a unique map $\text{Spec}\, \mathcal{O}_K \to A$ making the diagram commute. Phrased differently, the natural map $A(\mathcal{O}_K) \to A(K)$ is an isomorphism, as required. □

We can use the above result to gain more control over the structure of the K-valued points of an abelian variety. So let A be an abelian scheme over $\text{Spec}\, \mathcal{O}_K$ and let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}_K$. Then we have the equality

$$A(\mathcal{O}_K) = \varprojlim_{\nu} A(\mathcal{O}_K/\mathfrak{m}^\nu).$$

(In fact, this is true for any $\text{Spec}\, \mathcal{O}_K$-scheme X. In the affine case it follows immediately from the universal property of inverse limits and the general case follows from the affine case.) Thus $A(\mathcal{O}_K)$ is a profinite group; in fact, it is a p-adic Lie

group. Define a subgroup A_1 of $A(\mathcal{O}_K)$ to be the kernel of the natural reduction map

$$A(\mathcal{O}_K) \to A(k),$$

so that there is an exact sequences

$$0 \to A_1 \to A(\mathcal{O}_K) \to A(k) \to 0.$$

(The last map is surjective since $\mathcal{O}_K \to k$ is formally smooth.) It is a standard fact for abelian varieties that A_1 can be expressed as the $\mathfrak{m}$-valued points of a certain formal group. (See [**Si-AEC**, Chapter 4, Section 1] for the case of elliptic curves and [**Co2**] for the general case.)

Now, suppose that N is prime to the characteristic of k. Then the map

$$A_1 \xrightarrow{N} A_1$$

is an isomorphism by [**Si-AEC**, Chapter 4, Proposition 2.3], so there is an exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_1 & \longrightarrow & A(\mathcal{O}_K) & \longrightarrow & A(k) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \\
0 & \longrightarrow & A_1 & \longrightarrow & A(\mathcal{O}_K) & \longrightarrow & A(k) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & \longrightarrow & A(\mathcal{O}_K)/NA(\mathcal{O}_K) & \longrightarrow & A(k)/NA(k) & \longrightarrow & 0
\end{array}$$

Combined with Theorem 2.1 and Proposition 2.3 this gives us isomorphisms

$$A(K)/NA(K) \cong A(\mathcal{O}_K)/NA(\mathcal{O}_K) \cong A(k)/NA(k) \cong H^1(\mathfrak{g}_k, A[N]).$$

Now consider the above commutative diagram with K replaced by arbitrary finite extensions L. If L is taken large enough to contain all of $A[N](\bar{K})$, then the kernels of the diagram yield an isomorphism

$$A[N](\bar{K}) \cong A[N](\overline{k}).$$

In fact, this isomorphism is G_K-equivariant, as is easy to check. In particular, $A[N](\bar{K})$ must be unramified as a G_K-module.

2.3. Local Abelian Variety Structures. Let A be an abelian variety over a local field K and suppose that A has good reduction. Let N be an integer prime to the residue characteristic of K. We wish to compare the two exact sequences

$$0 \to A(K)/NA(K) \to H^1(G_K, A[N]) \to H^1(G_K, A(\bar{K}))[N] \to 0$$

and

$$0 \to H^1(\mathfrak{g}_k, A[N]) \to H^1(G_K, A[N]) \to H^1(\mathcal{I}_K, A[N])^{\mathfrak{g}_k} \to 0.$$

In the previous section we defined an isomorphism between the first terms in the exact sequences. We claim that this isomorphism lies in a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(K)/NA(K) & \longrightarrow & H^1(G_K, A[N]) & \longrightarrow & H^1(G_K, A(\bar{K}))[N] & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow & & \\
0 & \longrightarrow & H^1(\mathfrak{g}_k, A[N]) & \longrightarrow & H^1(G_K, A[N]) & \longrightarrow & H^1(\mathcal{I}_K, A[N])^{\mathfrak{g}_k} & \longrightarrow & 0
\end{array}$$

The proof of this is quite easy if A has been embedded in projective space over K in such a way that it "reduces" to an abelian variety over k; the main step becomes identifying the map $A(K) \to A(k)$ with the usual "scaling and reduction" map. (See [**Si-AEC**, Chapter 7, Section 2].) We instead again present a "coordinate-free" proof.

Since A has good reduction it extends to an abelian scheme over $\operatorname{Spec} \mathcal{O}_K$ which we will also denote by A. Note that the group of $\bar{K}$-valued points $A(\bar{K})$ is naturally a G_K-module even when thought of as $\operatorname{Hom}_{\operatorname{Spec} \mathcal{O}_K}(\operatorname{Spec} \bar{K}, A)$, since any $g \in G_K$ induces a $\operatorname{Spec} K$-automorphism

$$\operatorname{Spec} \bar{K} \xrightarrow{g} \operatorname{Spec} \bar{K}.$$

Any choice of projective embedding of A will identify this G_K-module with the usual G_K-module of K-valued points. Similarly $A(k)$ has a natural structure of $\mathfrak{g}_k$-module. Considering $A[N]$ as a group scheme over $\operatorname{Spec} \mathcal{O}_K$ we can realize the G_K-module $A[N](\bar{K})$ as the $\bar{K}$-valued points of the group scheme $A[N]$.

The key to the coordinate-free proof of the commutativity of the above diagram is the following commutative diagram which comes immediately from the fact that A is a group scheme over $\operatorname{Spec} \mathcal{O}_K$ (here L is any finite extension of K, $\mathcal{O}_L$ is its ring of integers and ℓ is its residue field):

$$\begin{array}{ccc} A(L) \times A(L) & \longrightarrow & A(L) \\ \cong \uparrow & & \cong \uparrow \\ A(\mathcal{O}_L) \times A(\mathcal{O}_L) & \longrightarrow & A(\mathcal{O}_L) \\ \downarrow & & \downarrow \\ A(\ell) \times A(\ell) & \longrightarrow & A(\ell) \end{array}$$

Here the vertical maps are the natural maps induced by $\operatorname{Spec} L \to \operatorname{Spec} \mathcal{O}_L$ and $\operatorname{Spec} \ell \to \operatorname{Spec} \mathcal{O}_L$ and the horizontal maps are multiplication; the indicated maps are isomorphisms by Proposition 2.3. Passing to the limit over L and the induced multiplication-by-N diagram, we obtain a commutative diagram of "reduction" maps

$$\begin{array}{ccc} A(\bar{K}) & \xrightarrow{N} & A(\bar{K}) \\ \downarrow & & \downarrow \\ A(\overline{k}) & \xrightarrow{N} & A(\overline{k}) \end{array}$$

Now, note that in order to establish the desired commutativity it will be enough to establish it for the diagram

$$\begin{array}{ccc} A(K) & \longrightarrow & H^1(G_K, A[N](\bar{K})) \\ \downarrow & & \| \\ A(k) & & \| \\ \downarrow & & \| \\ H^1(\mathfrak{g}_k, A[N](\overline{k})) & \xrightarrow{\inf} & H^1(G_K, A[N](\bar{K})) \end{array}$$

since the map of cokernels is simply the one induced by the first two vertical maps. (Here the map $A(K) \to A(k)$ is the reduction map and the other two unlabeled maps are the boundary maps from the Kummer exact sequence.) We recall the definition of the Kummer maps: given $P \in A(K)$, pick a $Q \in A(\bar{K})$ such that $N \cdot Q = P$. Then the image of P in $H^1(G_K, A[N])$ is the cocycle which sends any $g \in G_K$ to $Q^g - Q \in A[N]$. The definition is similar for $A(k)$.

So let P be in $A(K)$ and pick $Q \in A(\bar{K})$ as above. By the commutative diagram for multiplication by N, we find that $N \cdot \bar{Q} = \bar{P}$, where $\bar{P}$ and $\bar{Q}$ are the images of the respective points in $A(k)$. Thus P maps to the G_K-cocycle

$$g \mapsto Q^g - Q$$

and $\bar{P}$ maps to the $\mathfrak{g}_k$-cocycle

$$g \mapsto \bar{Q}^g - \bar{Q} = \overline{Q^g - Q}.$$

To complete the proof we now simply have to use the fact that $A[N](\bar{K}) \cong A[N](\overline{k})$ as G_K-modules. This shows that the two cocycles become the same after inflation, so the diagram really does commute.

2.4. Global Abelian Variety Structures. Let A be an abelian variety defined over a global field F. Let N be an integer and let $M = A[N]$ be the G_F-module of N-torsion points. A fundamental fact about such an A is that it has good reduction at almost all places v of F; that is, the base change

$$A_v = A \times_{\operatorname{Spec} F} \operatorname{Spec} F_v$$

has good reduction for almost all v.

We sketch the proof. For a few more details see [**Mi-AV**, Section 20, Remark 20.9], or for more many more details and a "coordinate-free" approach see [**Co**]. We need to show that there is some finite set S of places such that A extends to an abelian scheme over $\operatorname{Spec} \mathcal{O}_{F,S}$. Recall that any abelian variety is projective. Fix an embedding of A into projective space. Here A is simply the zero set of some finite set of homogeneous polynomials. Since all that matters are the zeros of the polynomials, we can scale them so as to assume that all of the coefficients are integral. Let A' be the projective scheme the equations define over $\operatorname{Spec} \mathcal{O}_F$. A' is automatically proper and is easily seen to be flat, and its generic fiber is A. However, A' need not yet be smooth, a group scheme or have geometrically connected fibers.

By [**Ha**, Chapter 3, Section 10, Theorem 10.2], to get smoothness it is enough to remove all primes which have nonsingular fibers lying over them. A fiber is nonsingular if and only if the Jacobian determinant vanishes modulo the corresponding prime. Since the fibers are all defined by the same equations and by assumption the Jacobian does not vanish in K, it can only vanish for finitely many fibers. Thus we need only remove a finite number of primes to get smoothness.

Next consider the multiplication and inversion morphisms of A. These are given by ratios of homogeneous polynomials with coefficients which we can take to be in $\mathcal{O}_K$, and thus will be regular for almost all primes. Thus by removing a finite number of primes we can get multiplication and inversion morphisms for A' over $\mathcal{O}_{F,S}$, where S is the (finite set) of discarded primes.

Lastly, then, we must consider the geometrically connected fiber condition. Here one shows that the existence of the (group) identity section shows that connected implies geometrically connected, so that it will be enough to establish that

the fibers are connected. Here one again uses the fact that the generic fiber is connected to show that almost all of the fibers are connected. See [**ST**, Section 1, Lemma 3] for the details.

Finally, then, we have constructed an abelian scheme A' over $\operatorname{Spec} \mathcal{O}_{F,S}$ (for some finite set of primes S) with generic fiber A. Base changing A' to the appropriate completion for $v \notin S$ shows that A has good reduction for $v \notin S$, and thus that A has good reduction almost everywhere.

Recall now that we defined the abelian variety structure on M by setting

$$H^1_f(G_v, M) = \operatorname{im}\big(A(F_v)/NA(F_v) \hookrightarrow H^1(G_v, A[N])\big)$$

under the Kummer map. We now immediately see that this really is a finite/singular structure; this follows from the computations of the previous section, which apply whenever A has good reduction at v and v does not divide N. In particular, this completes the proofs of all of the results of Lecture 9, Section 2.2.

Note, however, that the abelian variety structure on M depends on the particular abelian variety A and the isomorphism $A[N] \cong M$ and thus is not an invariant of M as a G_K-module.

CHAPTER 11

Lecture 11

1. L/K Forms

1.1. Definitions and Examples. Let L/K be a finite extension of fields. We assume that L/K is Galois, although that will not really be necessary until later. Let V be an algebraic variety defined over K. We will say that another algebraic variety W, defined over K, is an L/K *form of* V if

$$W \times_{\operatorname{Spec} K} \operatorname{Spec} L \cong V \times_{\operatorname{Spec} K} \operatorname{Spec} L.$$

(Note that the specific isomorphism is not part of the data attached to an L/K form; we merely assume that one exists.) An L/K form W of V, then, is simply an algebraic variety which becomes isomorphic to K after base change to L; this, of course, does not imply that V and W are isomorphic over K. Such a W is often called a *twist* of V. We define $E(L/K, V)$ to be the set of K-isomorphism classes of varieties W, defined over K, which are L/K forms of V. In fact, it is a pointed set, with the class of V itself being the distinguished element.

This notion of L/K form is not in any way restricted to the case of algebraic varieties. Grothendieck was able to extend the key ideas to a much more general situation, replacing L/K with any faithfully flat quasi-compact map of schemes $Y \to X$, and replacing the above twists with certain fibered categories.

We will content ourselves with a few more examples. First, suppose that instead of simply considering a variety V over K, we consider a base-pointed variety V over K; that is, we consider pairs (V, v), where v is a K-valued point of V. L/K forms of V are now pairs (W, w) of a variety W defined over K and a K-valued point w of W such that v maps to w under some isomorphism of V_L and W_L. There is an obvious notion of isomorphism of base-pointed schemes, and we can define $E(L/K, (V, v))$ to be the set of K-isomorphism classes of base-pointed varieties, defined over K, which are L/K forms of (V, v). In the exact same way one can define L/K forms for algebraic groups defined over K, isomorphisms now required to be isomorphism as algebraic groups; or even L/K forms for algebraic varieties with chosen groups of automorphisms.

Moving away from varieties, we note that a central simple algebra over K of rank n^2 which splits over L is nothing more than an L/K form of the central simple K-algebra $\mathcal{M}_n(K)$. Thus $E(L/K, \mathcal{M}_n(K))$ is simply the set of central simples K-algebras which split over L. As another example, let F be a number field and recall the notion of locally free rank 1 $\mathcal{O}_{F,S}$-module introduced in Lecture 10, Section 1.3. If V is such a module, then for some N we have $V^N \cong \mathcal{O}_{F,S}$ since $\operatorname{Pic}(\mathcal{O}_{F,S})$ is finite. Interpreting V as a fractional ideal, we have $V^N = \alpha\mathcal{O}_{F,S}$. It follows easily that V becomes trivial over $F(\alpha^{1/N})$, so that it is a $F(\alpha^{1/N})/F$ form for $\mathcal{O}_{F,S}$.

[0]Last modified September 4, 2003

1.2. The Automorphism Group. We return now to the case of algebraic varieties over K; almost everything we will say remains true in the other situations we mentioned, but this case is the simplest to explain. So let V be a fixed varieity over K. If L is an extension of K, we define the *automorphism group for V over L*, $\mathrm{Aut}_L(V)$, to be the group of automorphisms of $V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$ as an algebraic variety over L. Thus $\mathrm{Aut}_L(V)$ is just the set of isomorphisms

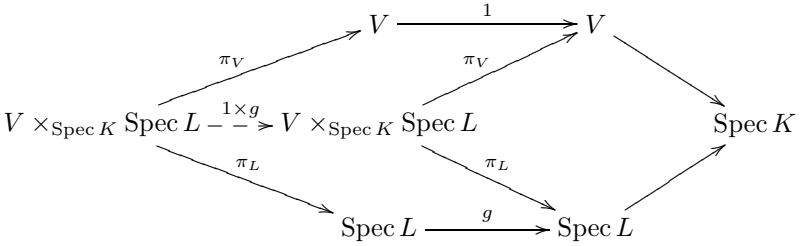
$$\varphi : V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L \to V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$$

of $\mathrm{Spec}\, L$-schemes. (Viewing $\mathrm{Aut}(V)$ as a function of L one obtains a presheaf for the étale topology on $\mathrm{Spec}\, K$; in fact, it is actually a sheaf. See [**Mi-EC**, Chapter 3, Section 4, pp. 134-135]. We will not really need this interpretation, however.)

The (not necessarily abelian) group $\mathrm{Aut}_L(V)$ has a natural left $\mathrm{Gal}(L/K)$-action. Specifically, given $\varphi \in \mathrm{Aut}_L(V)$ and $g \in \mathrm{Gal}(L/K)$, we define $g\varphi \in \mathrm{Aut}_L(V)$ by the following commutative diagram of isomorphisms:

$$\begin{array}{ccc} V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L & \xrightarrow{\varphi} & V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L \\ \downarrow{\scriptstyle 1\times g} & & \downarrow{\scriptstyle 1\times g} \\ V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L & \xrightarrow{g\varphi} & V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L \end{array}$$

That is, $g\varphi$ is the inverse of the isomorphism $1 \times g$ followed by φ followed by $1 \times g$. Here by $1 \times g$ we mean the map on $V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$ making the following diagram commute:



It is easy to check that this is really a group action, so that we have realized $\mathrm{Gal}(L/K)$ as a group of automorphisms of $\mathrm{Aut}_L(V)$. Note that with this definition the identity is $\mathrm{Gal}(L/K)$-invariant. More generally, an important fact is that the subgroup of $\mathrm{Aut}_L(V)$ of automorphisms fixed by every $g \in \mathrm{Gal}(L/K)$ can be canonically identified with $\mathrm{Aut}_K(V)$. If one is willing to work simply with equations this is just standard Galois theory, but the full statement is really that the étale presheaf defined above is actually a sheaf.

If $\mathrm{Aut}_L(V)$ were abelian it would thus be a $\mathrm{Gal}(L/K)$-module in our usual sense. For the next few sections we will amend the definition of $\mathrm{Gal}(L/K)$-module to include modules whose underlying groups are non-abelian, so that any $\mathrm{Aut}_L(V)$ is a $\mathrm{Gal}(L/K)$-module. However, to make the context in which $\mathrm{Aut}_L(V)$ is being used clear, we will write $\underline{\mathrm{Aut}}_L(V)$ for it when we want to regard it as a $\mathrm{Gal}(L/K)$-module.

Let us now generalize the above situation somewhat. We continue to let V be an algebraic variety over K, and we now fix a finite extension L/K and an L/K form W of V. We define $\mathrm{Isom}_L(W, V)$ to be the set of $\mathrm{Spec}\, L$-isomorphisms from

W to V defined over L; that is, the set of isomorphisms

$$W \times_{\operatorname{Spec} K} \operatorname{Spec} L \to V \times_{\operatorname{Spec} K} \operatorname{Spec} L.$$

First note that $\operatorname{Isom}_L(W, V)$ is non-empty, since W is an L/K form for V. It has a natural left $\operatorname{Aut}_L(V)$ action given by postcomposition: if $\psi \in \operatorname{Isom}_L(W, V)$ and $\varphi \in \operatorname{Aut}_L(V)$, then we define $\varphi\psi$ to simply be the composition

$$W \times_{\operatorname{Spec} K} \operatorname{Spec} L \xrightarrow{\psi} V \times_{\operatorname{Spec} K} \operatorname{Spec} L \xrightarrow{\varphi} V \times_{\operatorname{Spec} K} \operatorname{Spec} L.$$

It is easy to see that this action exhibits $\operatorname{Isom}_L(W, V)$ as a principal homogeneous space for $\operatorname{Aut}_L(V)$; that is, it is an $\operatorname{Aut}_L(V)$-torsor.

$\operatorname{Isom}_L(W, V)$ in fact has even more structure. It has a natural $\operatorname{Gal}(L/K)$-action: if $\varphi \in \operatorname{Isom}_L(W, V)$ and $g \in \operatorname{Gal}(L/K)$, we define $g\varphi \in \operatorname{Isom}_L(W, V)$ to be the composition

$$\begin{array}{ccc} W \times_{\operatorname{Spec} K} \operatorname{Spec} L & \xrightarrow{\varphi} & V \times_{\operatorname{Spec} K} \operatorname{Spec} L \\ \downarrow{\scriptstyle 1\times g} & & \downarrow{\scriptstyle 1\times g} \\ W \times_{\operatorname{Spec} K} \operatorname{Spec} L & \xrightarrow{g\varphi} & V \times_{\operatorname{Spec} K} \operatorname{Spec} L \end{array}$$

We will write $\underline{\operatorname{Isom}}_L(W, V)$ when we want to emphasize that $\operatorname{Isom}_L(W, V)$ should be thought of with its $\operatorname{Gal}(L/K)$-action. In fact, the $\operatorname{Gal}(L/K)$-actions on $\operatorname{Isom}_L(W, V)$ and $\underline{\operatorname{Aut}}_L(V)$ are compatible with the action of $\underline{\operatorname{Aut}}_L(V)$ on $\underline{\operatorname{Isom}}_L(W, V)$. We will make this notion precise in the next section.

2. Cohomological Interpretations

2.1. G-action Torsors. In this section we wish to formalize the sort of situation studied in the previous section. Let G be a group and let A be a finite group on which G acts. Let X be a set on which both G and A act. We will say that X is a *G-action torsor* for A if it is a torsor for A in the usual sense and if the A-action is compatible with the G-structures. That is, there is a map

$$A \times X \xrightarrow{\alpha} X$$

exhibiting X as a principal homogeneous space for A and such that

$$\alpha(ga, gx) = g\alpha(a, x)$$

for any $a \in A$, $x \in X$ and $g \in G$.

As a first example (with varieties rather than sets), it is easy to see that the constructions of the previous section exhibit $\underline{\operatorname{Isom}}_L(W, V)$ as a $\operatorname{Gal}(L/K)$-action torsor for $\underline{\operatorname{Aut}}_L(V)$, where V is an algebraic variety over K and W is an L/K form for V.

If G is a group and A is another group on which G acts, we define $T(G, A)$ to be the set of isomorphism classes of G-action torsors for A. $T(G, A)$ is actually a pointed set, with the trivial torsor A as the distinguished element.

The fundamental classification theorem for G-action torsors is the following cohomological expression, which we have essentially seen before.

THEOREM 2.1. *If G is a group and A is a finite group with a G-action, then there is a canonical isomorphism of pointed sets*

$$T(G, A) \cong H^1(G, A).$$

We state this for non-abelian A, even though we have not yet defined $H^1(G, A)$ when A is non-abelian, because it seems unnecessarily restrictive to assume that A is abelian. In fact, the definition of H^1 for non-abelian modules is essentially precisely what makes the proof of the theorem work. We recall it briefly here; for more details on non-abelian cohomology, see [**Se-LF**, Appendix to Chapter 7] or [**Se-GC**, Chapter 1, Section 5] (although the reader should be forewarned that in the second source Serre appears to change his conventions halfway through).

To define non-abelian cohomology we work with cocycles and we must be careful as to what order operations occur in. All actions are left actions, and we will write all G-actions as exponentials on the left. We define the set $\mathrm{CrossHom}(G, A)$ to be the pointed set of maps

$$\varphi : G \to A$$

such that

$$\varphi(g_1 g_2) = \varphi(g_1)\ {}^{g_1}\varphi(g_2)$$

for all $g_1, g_2 \in G$. (We write A multiplicatively, of course.) The distinguished element is the trivial map sending all of G to $1 \in A$.

$\mathrm{CrossHom}(G, A)$ has a natural left A-action: for any $a \in A$ and $\varphi \in \mathrm{CrossHom}(G, A)$ we define $a * \varphi \in \mathrm{CrossHom}(G, A)$ by

$$a * \varphi(g) = a\varphi(g)\ {}^{g}(a^{-1}).$$

(Of course one must check that $a * \varphi$ is still a crossed homomorphism; this is an easy computation. Note also that this action does not preserve the base point of $\mathrm{CrossHom}(G, A)$.) We define $H^1(G, A)$ to be the set of orbits of $\mathrm{CrossHom}(G, A)$ under this action; it is a pointed set with the distinguished element given by the class of the trivial crossed homomorphism. One checks immediately that if A is abelian this yields the usual definition of $H^1(G, A)$.

We now give the proof of Theorem 2.1.

Proof. Let (X, α) be a G-action torsor for A. Choose any $x \in X$. We will use x to define a cocycle

$$c_x : G \to A.$$

Specifically, we define $c_x(g)$ to be the unique element of A such that

$$\alpha(c_x(g), {}^{g}x) = x.$$

$c_x(g)$ exists and is unique since α is a principal homogeneous action.

We check that c_x really is a cocycle. For $g_1, g_2 \in G$,

$$\begin{aligned}
\alpha(c_x(g_2), {}^{g_2}x) &= x \\
{}^{g_1}\alpha(c_x(g_2), {}^{g_2}x) &= {}^{g_1}x \\
\alpha({}^{g_1}c_x(g_2), {}^{g_1 g_2}x) &= {}^{g_2}x \\
\alpha(c_x(g_1), \alpha({}^{g_1}c_x(g_2), {}^{g_1 g_2}x)) &= \alpha(c_x(g_1), {}^{g_2}x) \\
\alpha(c_x(g_1)\ {}^{g_1}c_x(g_2), {}^{g_1 g_2}x) &= x.
\end{aligned}$$

On the other hand, by definition

$$\alpha(c_x(g_1 g_2), {}^{g_1 g_2}x) = x,$$

so

$$c_x(g_1 g_2) = c_x(g_1)\ {}^{g_1}c_x(g_2)$$

which shows that c_x is a cocycle.

We now must check that the cohomology class of c_x is independent of the choice of $x \in X$. So choose any other $y \in X$. Then there is a unique $a \in A$ such that

$$y = \alpha(a, x).$$

We have

$$\begin{aligned} \alpha(c_y(g), {}^g y) &= y \\ \alpha(c_y(g), \alpha({}^g a, {}^g x)) &= \alpha(a, x) \\ \alpha(c_y(g)\ {}^g a, {}^g x) &= \alpha(a, x) \\ \alpha(a^{-1} c_y(g)\ {}^g a, {}^g x) &= x. \end{aligned}$$

Thus

$$c_x(g) = a^{-1} c_y(g)\ {}^g a$$

which shows that c_x and c_y differ by a coboundary. This shows that we have a well-defined map

$$T(G, A) \to H^1(G, A).$$

We now define the inverse map. Given any cocycle $\varphi : G \to A$, we will define a corresponding G-action torsor. In order to get the notation straight we define a new set P_φ to be identical to A as a set; we let

$$p : A \to P_\varphi$$

be the natural map. We let $b \in A$ act on $p(a) \in P_\varphi$ by

$$bp(a) = p(ba).$$

This clearly makes P into a principal homogeneous space for A. We put a twisted G-action on P by

$${}^g p(a) = p({}^g a \varphi(g)^{-1}).$$

We leave it to the reader to check that this really is a G-action torsor; it is not difficult. To show that the isomorphism class of P_φ depends only on the cohomology class of φ, one shows that if $\psi(g) = b\varphi(g)\ {}^g(b^{-1})$, then the map

$$P_\psi \to P_\varphi$$

sending $p_\varphi(a)$ to $p_\varphi(ab)$ is an isomorphism of G-action torsors. We also leave it to the reader to check that the maps are inverses. □

2.2. Descent. We now apply the formalism of the previous section to the particular case of interest. We again let V be an algebraic variety defined over K and let W be an L/K form for V. Recall that $\underline{\mathrm{Isom}}_L(W, V)$ is a $\mathrm{Gal}(L/K)$-action torsor for $\underline{\mathrm{Aut}}_L(V)$.

This fact can be summarized by saying that we have defined a map

$$E(L/K, V) \xrightarrow{\iota} T(\mathrm{Gal}(L/K), \underline{\mathrm{Aut}}_L(V))$$

given by

$$\iota(W) = \underline{\mathrm{Isom}}_L(W, V).$$

We claim that ι is actually injective. To show this, suppose that we have an L/K form W for V and that $\iota(W)$ is isomorphic to $\underline{\mathrm{Aut}}_L(V)$ as an $\underline{\mathrm{Aut}}_L(V)$ torsor. Let φ be the image in $\iota(W)$ of $1 \in \underline{\mathrm{Aut}}_L(V)$. A priori φ is a map $W \to V$ defined over L. In fact, since the $\mathrm{Gal}(L/K)$-actions are compatible and $\mathrm{Gal}(L/K)$ acts trivially on 1, it also acts trivially on φ. This implies that φ is defined over K, and thus that W is the trivial L/K form. Of course, since neither the domain nor the

range of ι need be a group this does not suffice to prove injectivity; however, the general case is quite similar.

The map ι is sometimes but not always surjective. In any case, we have the following fact.

PROPOSITION 2.2. *There is a canonical injection*

$$E(L/K, V) \hookrightarrow H^1(\mathrm{Gal}(L/K), \underline{\mathrm{Aut}}_L(V))$$

and it is an isomorphism if and only if the natural injection

$$E(L/K, V) \hookrightarrow T(L/K, \underline{\mathrm{Aut}}_L(V))$$

is an isomorphism.

PROOF. This follows immediately from Theorem 2.1 and the above discussion. □

If the injection of Proposition 2.2 is actually an isomorphism we will say that we have *descent for* V. A fundamental theorem due to Weil is that if V is a projective variety then we do have descent.

THEOREM 2.3 (Weil). *Let V be a projective variety. Then there is a canonical isomorphism of sets*

$$E(L/K, V) \xrightarrow{\cong} H^1(\mathrm{Gal}(L/K), \mathrm{Aut}_L(V)).$$

PROOF. We sketch the main ideas. For the complete proof in the case of curves, see [**Si-AEC**, Chapter 10, Section 2, Theorem 2.2]. The general case is considerably harder.

Given any cocycle $c : \mathrm{Gal}(L/K) \to \mathrm{Aut}_L(V)$, we must define a twist V^c of V such that V^c becomes isomorphic to V over L and such that V^c gives the correct cohomology class.

To do this, consider $V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$. We define a $\mathrm{Gal}(L/K)$ action on this by first acting on $\mathrm{Spec}\, L$ via g in the usual way, and then acting on the "new" $V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$ by $c(g)$. V^c is then the quotient of $V \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$ by this $\mathrm{Gal}(L/K)$-action. The hard part, of course, is to show that this quotient can be given the structure of an algebraic variety. In the case of curves one can use function fields, but the general case is much more difficult. □

There is a rather peculiar situation that arises when one has descent, in that $E(L/K, V)$ depends only on $\mathrm{Aut}_L(V)$ and not at all on the actual structures involved. This can be exploited in some circumstances. For example, the octonians and G_2 have the same automorphism groups, so given any twist for one structure we ought to be able to obtain a corresponding twist for the other. Another example is central simple algebras and Brauer-Severi varieties; see [**Se-LF**, Chapter 10, Section 6].

As a final example, suppose that $\mathrm{Aut}_L(V)$ is cyclic of order 2. (For example, V could be a general hyperelliptic curve.) A group of order 2 must have trivial Galois action, so $E(L/K, V)$ is independent of the variety V! In particular, it is simply

$$H^1(\mathrm{Gal}(L/K), \pm 1) = \mathrm{Hom}(\mathrm{Gal}(L/K), \pm 1).$$

CHAPTER 12

Lecture 12

1. Torsors for Algebraic Groups

1.1. Algebraic Geometric Torsors. Fix a field K. If V is any variety over K we will write $\overline{V}$ for $V \times_{\operatorname{Spec} K} \operatorname{Spec} K_s$, where K_s is the separable closure of K. Let Γ be an algebraic group over K, with multiplication morphism μ:

$$\Gamma \times_{\operatorname{Spec} K} \Gamma \xrightarrow{\mu} \Gamma.$$

We wish to combine our notion of Γ-torsor from Lecture 5, Section 2.3 with the ideas from Lecture 11. We define an *algebraic geometric torsor* (AG torsor for short) for Γ to be an algebraic variety X defined over K, together with a morphism

$$\Gamma \times_{\operatorname{Spec} K} X \xrightarrow{\alpha} X,$$

which becomes isomorphic to the standard torsor (Γ, μ) over K_s; that is, there is an isomorphism

$$u : \overline{\Gamma} \to \overline{X}$$

fitting into a commutative diagram

$$\begin{array}{ccc} \overline{\Gamma} \times_{\operatorname{Spec} K_s} \overline{\Gamma} & \xrightarrow{\mu} & \overline{\Gamma} \\ \downarrow{\scriptstyle 1\times u} & & \downarrow \\ \overline{\Gamma} \times_{\operatorname{Spec} K_s} \overline{X} & \xrightarrow{\alpha} & \overline{X} \end{array}$$

We will say that X is *trivial* as an AG torsor for Γ is there is such a u which is definable over K. In fact, this happens precisely when X has a point defined over K; choosing this point to be the identity and using α to define multiplication easily establishes this. Note that in any case u is defined by finite data, so it must actually be defined over some finite extension L of K. Thus any AG torsor becomes trivial over some finite extension of K.

For any extension L/K let us define $E(L/K, (\Gamma, \mu))$ to be the pointed set of AG torsors for Γ which become trivial over L. Note that there is a natural mapping

$$E(L/K, (\Gamma, \mu)) \to E(L/K, \Gamma),$$

where $E(L/K, \Gamma)$ is simply the set of L/K forms for Γ thought of as an algebraic variety without its group structure. This map is easily seen to be surjective, but it need not be injective; we will see an example of this later in the lecture.

Recall that we constructed an injection

$$E(L/K, \Gamma) \hookrightarrow H^1(\operatorname{Gal}(L/K), \underline{\operatorname{Aut}}_L(\Gamma)),$$

[0]Last modified September 4, 2003

where $\underline{\mathrm{Aut}}_L(\Gamma)$ is the group of automorphisms of Γ as an algebraic variety over L. Composing with the forgetful map above defines a map

$$E(L/K,(\Gamma,\mu)) \to H^1(\mathrm{Gal}(L/K),\underline{\mathrm{Aut}}_L(\Gamma)).$$

This map is not terribly useful, however, as it is not even an injection. We wish to define a similar map for $E(L/K,(\Gamma,\mu))$ which is somewhat more germane to our situation.

PROPOSITION 1.1. *Let (Γ,μ) be an algebraic group defined over a field K. Then for any L/K there is a natural injection of pointed sets*

$$E(L/K,(\Gamma,\mu)) \xrightarrow{i} H^1(\mathrm{Gal}(L/K),\Gamma(L)),$$

where $\Gamma(L)$ is the group of L-valued points of Γ.

We omit the proof. It is clear from this proof that our various maps fit into a commutative diagram

$$\begin{array}{ccc} E(L/K,(\Gamma,\mu)) & \longrightarrow & E(L/K,\Gamma) \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \iota} \\ H^1(\mathrm{Gal}(L/K),\Gamma(L)) & \longrightarrow & H^1(\mathrm{Gal}(L/K),\underline{\mathrm{Aut}}_L(\Gamma)) \end{array}$$

where the bottom map is induced from the natural $\mathrm{Gal}(L/K)$-module injection

$$\Gamma(L) \to \underline{\mathrm{Aut}}_L(\Gamma)$$

where elements of Γ_L are viewed as translations.

We will say that Γ/K satisfies the *descent propety for torsors* if the map of Proposition 1.1 is an isomorphism.

1.2. Torsors for Abelian Varieties. Let K be a field and let A be an abelian variety defined over K. We have the following fundamental theorem.

THEOREM 1.2. *An abelian variety A over a field K has the descent property for torsors.*

PROOF. The proof of this is quite difficult. For the case of elliptic curves, see [**Si-AEC**, Chapter 10, Theorem 3.6]. □

It follows from this and Proposition 1.1 that for any finite L/K we have an identification

$$E(L/K,(A,\mu)) \cong H^1(\mathrm{Gal}(L/K),A(L)).$$

Since $A(L)$ is abelian, $H^1(G_K,A(L))$ is an abelian group. The induced group structure on $E(L/K,(A,\mu))$ is in fact just the Baer sum; see Lecture 5, Section 2.2. However, it is fairly difficult to see that the necessary quotient operations are really defined.

It is much easier to describe the involution induced on $E(L/K,(A,\mu))$ by inversion in $H^1(G_K,A(L))$. This is done as follows: let $\iota : A \to A$ be the inversion morphism on A and let (X,α) be an algebraic geometric torsor for A. Then the inverse of X, say $X^\sim$, is simply X considered as a torsor with A-action $\alpha \circ (\iota \times 1)$. Note, however, that $X^\sim$ and X give exactly the same element of $E(L/K,A)$, since ι is defined over K. Thus this gives an example of a case in which the forgetful map

$$E(L/K,(A,\mu)) \to E(L/K,A)$$

is not injective. More generally elements of $\mathrm{Aut}_K(\Gamma)$ which are not translations can be used to manufacture such examples.

1.3. The Shafarevich-Tate Group. Let F be a number field. We will now relate torsors to the Shafarevich-Tate group $Ш(A/F)$ defined in Lecture 9, Section 2.1. More generally, we let S be any finite set of places of F and we define the pointed set

$$Ш_S(A/F)$$

to be the set of isomorphism classes of AG torsors for A which are trivial when viewed over the local fields F_v for $v \notin S$. Thus a non-trivial element in $Ш_S(A/F)$ is a torsor for A which has an F_v-rational point for every $v \notin S$ but has no F-rational point.

Using Theorem 1.2 we have the following immediate cohomological interpretation of $Ш_S(A/F)$.

PROPOSITION 1.3. *There is an exact sequence*

$$0 \to Ш_S(A/F) \to H^1(G_F, A(\bar{F})) \xrightarrow{\text{res}} \prod_{v \notin S} H^1(G_v, A(\bar{F}_v)).$$

In particular, $Ш_\emptyset(A/F)$ *can be identified with the Shafarevich-Tate group* $Ш(A/F)$.

PROOF. All that is necessary is, for every L/F, to identify the map

$$E(L/F, (A, \mu)) \to E(L_w/F_v, (A \times_{\mathrm{Spec}\, F} \mathrm{Spec}\, F_v))$$

with the restriction map in cohomology, but this follows easily from the defintions of the isomorphisms of Theorem 1.2. □

Proposition 1.3 gives a geometric interpretation of the Shafarevich-Tate group; however, it is still extremely difficult (both in theory and in practice) to compute it. As an example of the results of one such computation we quote the following theorem which follows from careful consideration of the work of Kolyvagin and Rubin.

THEOREM 1.4. *Let E be the elliptic curve over $\mathbb{Q}$ defined by the equation*

$$x^3 + y^3 + 60z^3 = 0,$$

with origin $(-1, 1, 0)$. *Then*

$$Ш(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

The non-trivial elements of $Ш(E/\mathbb{Q})$ *are represented by*

$$\Sigma_2 : 3x^3 + 4y^3 + 5z^3 = 0;$$
$$\Sigma_3 : 12x^3 + y^3 + 5z^3 = 0;$$
$$\Sigma_4 : 15x^3 + 4y^3 + z^3 = 0;$$
$$\Sigma_5 : 3x^3 + 20y^3 + z^3 = 0;$$

together with the inverses $\Sigma_i^\sim$.

The proof of this theorem is quite difficult.

The group $Ш(A/F)$ can be interpreted as an "obstruction" to the Hasse principle. Recall that the Hasse-Minkowski theorem (see [**Se-CA**, Chapter 4]) states that a quadric curve has a point in $\mathbb{Q}$ if and only if it has a point in each $\mathbb{Q}_p$ and in $\mathbb{R}$. Unfortunately, this results fails for curves of higher genus; this is reflected in the

existence of non-trivial elements of $Ш(A/F)$. The curve Σ_2 is a famous example of Selmer, which he used to demonstrate the explicit failure of the Hasse principle for cubic curves.

CHAPTER 13

Lecture 13

1. The Picard Group of a Curve

1.1. The Picard Group. Let X be a smooth, projective, geometrically irreducible curve defined over a field K. For simplicity assume that K is perfect. The geometric irreducibility condition is equivalent to the function field $K(X)$ being linearly disjoint from $\bar{K}$ over K. In particular, we can identify $G = \mathrm{Gal}(\bar{K}(X)/K(X))$ with G_K.

We recall the definition of the *Picard group* of X, $\mathrm{Pic}(X)$. See [**Ha**, Chapter 2, Section 6] for details. The $\bar{K}$ points of $\mathrm{Pic}(X)$ are easiest to describe: they are in natural bijective correspondence with isomorphism classes of line bundles on $\overline{X} = X \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, \bar{K}$.

There is another interpretation of $\mathrm{Pic}(X)(\bar{K})$ which is somewhat simpler. Recall that a *divisor* on X is a formal sum of points of $X(\bar{K})$; that is, it is an element of the free abelian group $\mathbb{Z}[X(\bar{K})]$. Let $\bar{K}(X)^*$ be the function field of X over $\bar{K}$. There is a natural map

$$\bar{K}(X)^* \xrightarrow{\mathrm{div}} \mathbb{Z}[X(\bar{K})]$$

given by

$$f \mapsto \sum_{x \in X(\bar{K})} \mathrm{ord}_x(f)x,$$

where $\mathrm{ord}_x(f)$ means the order of the zero or pole of f at x. Then

$$\mathrm{Pic}(X)(\bar{K}) \cong \mathbb{Z}[X(\bar{K})]/\,\mathrm{div}(\bar{K}(X)^*).$$

It can be shown that $\mathrm{div}(\bar{K}(X)^*)$ lies in the kernel of the natural summation map

$$\mathbb{Z}[X(\bar{K})] \to \mathbb{Z},$$

so it descends to a map

$$\mathrm{Pic}(X)(\bar{K}) \xrightarrow{\deg} \mathbb{Z}$$

called the *degree map*. This agrees with the usual notion of degree for line bundles. We define

$$\mathrm{Pic}^0(X)(\bar{K})$$

to be the kernel of the degree map.

It can be shown that $\mathrm{Pic}^0(X)$ can be given the structure of an abelian variety over K of dimension equal to the genus of X. Often $\mathrm{Pic}^0(X)$ is called the *Jacobian* of X. See [**Mi-JV**].

[0]Last modified September 4, 2003

If a rational function on $\overline{X}$ has no zeros or pole then it is a constant. Thus there is an exact sequence

$$0 \to \bar{K}^* \to \bar{K}(X)^* \xrightarrow{\text{div}} \mathbb{Z}[X(\bar{K})] \to \text{Pic}(X)(\bar{K}) \to 0.$$

We rewrite this as a short exact sequence

$$0 \to \bar{K}(X)^*/\bar{K}^* \to \mathbb{Z}[X(\bar{K})] \to \text{Pic}(X)(\bar{K}) \to 0;$$

it is actually an exact sequence of G_K-modules (using our identification of G with G_K), as is easy to see.

PROPOSITION 1.1. *There is an exact sequence*

$$\mathbb{Z}[X(\bar{K})]^{G_K} \to \text{Pic}(X)(K) \to \ker\big(\text{Br}_K \to H^2(G, \bar{K}(X)^*)\big).$$

(Here $\text{Pic}(X)(F)$ *is just the* F*-valued "points"* $\mathbb{Z} \times \text{Pic}^0(X)(F)$ *of* $\text{Pic}(X)$*. Note that* $\mathbb{Z}[X(\bar{K})]^{G_K}$ *need not equal* $\mathbb{Z}[X(K)]$*.)*

PROOF. Taking the $G_K = G$ cohomology of

$$0 \to \bar{K}(X)^*/\bar{K}^* \to \mathbb{Z}[X(\bar{K})] \to \text{Pic}(X)(\bar{K}) \to 0$$

yields an exact sequence

$$\mathbb{Z}[X(\bar{K})]^{G_K} \to \text{Pic}(X)(K) \to H^1(G, \bar{K}(X)^*/\bar{K}^*).$$

Thus it will be enough to identify $H^1(G, \bar{K}(X)^*/\bar{K}^*)$ with the kernel of

$$H^2(G_K, \bar{K}^*) \to H^2(G, \bar{K}(X)^*).$$

To do this we take G_K cohomology of

$$0 \to \bar{K}^* \to \bar{K}(X)^* \to \bar{K}(X)^*/\bar{K}^* \to 0,$$

yielding

$$H^1(G, \bar{K}(X)^*) \to H^1(G, \bar{K}(X)^*/\bar{K}^*) \to H^2(G_K, \bar{K}^*) \to H^2(G, \bar{K}(X)^*).$$

By Hilbert's theorem 90 the first term vanishes, which gives the desired identification. □

We now restrict to the case where $K = F$ is a number field and relate the above result to the Shafarevich-Tate group.

PROPOSITION 1.2. *Along with our running hypotheses, suppose further that* X *has an* F_v *rational point for all place* v *of* F*. Then the natural map*

$$\text{Br}_F \to \text{Br}_{\bar{F}(X)}$$

is injective.

PROOF. By global class field theory we have that Br_F injects into $\oplus_v \text{Br}_{F_v}$. The commutative diagram

$$\begin{array}{ccc} \text{Br}_F & \longrightarrow & \text{Br}_{F(X)} \\ \downarrow & & \downarrow \\ \bigoplus_v \text{Br}_{F_v} & \longrightarrow & \bigoplus_v \text{Br}_{F_v(X)} \end{array}$$

now shows that it will suffice to prove that each map $\text{Br}_{F_v} \to \text{Br}_{F_v(X)}$ is injective.

For this we will need to use some of the theory of Brauer groups of schemes developed by Asumaya and Grothendieck. We have a diagram

$$\begin{array}{ccc} \operatorname{Spec} F_v(X) & \longrightarrow & \operatorname{Spec} X_v \\ \downarrow & \swarrow & \\ \operatorname{Spec} F_v & & \end{array}$$

where $X_v = X \times_{\operatorname{Spec} F} \operatorname{Spec} F_v$ and $\operatorname{Spec} F_v(X)$ is the generic point of X_v. This translates to a diagram

$$\begin{array}{ccc} \operatorname{Br}(F_v(X)) & \longleftarrow & \operatorname{Br}(X_v) \\ \uparrow & \nearrow & \\ \operatorname{Br}(F_v) & & \end{array}$$

of Brauer groups. Since X_v is smooth, a theorem of Grothendieck (see [**Mi-EC**, Chapter 4]) implies that the map

$$\operatorname{Br}(X_v) \to \operatorname{Br}(F_v(X))$$

is injective. Thus it will suffice to show that

$$\operatorname{Br}(F_v) \to \operatorname{Br}(X_v)$$

is injective. For this, we use the fact that X_v has an F_v-rational point. This implies that there is a section to the natural map

$$X_v \to \operatorname{Spec} F_v,$$

and injectivity of $\operatorname{Br}(F_v) \to \operatorname{Br}(X_v)$ follows immediately. □

COROLLARY 1.3. *Let X be a smooth, projective, geometrically irreducible curve over a number field F. Suppose further that X has an F_v-rational point for all places v of X. Then any F-rational divisor class is represented by an F-rational divisor; that is, the natural map*

$$\mathbb{Z}[X(\bar{F})]^{G_F} \to \operatorname{Pic}(X)(F)$$

is surjective.

PROOF. By Proposition 1.1 it will suffice to prove that the map

$$\operatorname{Br}_F \to H^2(\operatorname{Gal}(\bar{F}(X)/F(X)), \bar{F}(X)^*)$$

is injective. By Hilbert's theorem 90 and the inflation-restriction sequence, this second group injects into $\operatorname{Br}_{\bar{F}(X)}$, so that the map $\operatorname{Br}_F \to \operatorname{Br}_{\bar{F}(X)}$ factors through the map we are interested in. Proposition 1.2 thus completes the proof. □

1.2. Applications to Shafarevich-Tate Groups. Let E be an elliptic curve defined over a number field F. Let (X, α) be an AG torsor for E and choose a point $P_0 \in X(\bar{F})$. Then the map

$$\mathbb{Z}[X(\bar{F})] \to E(\bar{F})$$

defined by sending a point $P \in X(\bar{F})$ to the unique $Q \in E(\bar{F})$ for which

$$\alpha(Q, P_0) = P$$

descends to an isomorphism of varieties over K

$$\operatorname{Pic}^0(X) \cong E.$$

(See [**Si-AEC**, Chapter 10, Theorem 3.8].)

More generally, let us define $\mathrm{Pic}^m(X)$ to be the inverse image of $m \in \mathbb{Z}$ under the degree map $\mathrm{Pic}(X) \to \mathbb{Z}$. Each of these become isomorphic to $\mathrm{Pic}^0(X)$ over $\bar{F}$. In fact, there is a natural action of $\mathrm{Pic}^0(X)$ on $\mathrm{Pic}^m(X)$, by addition, which is easily seen to be a G_F-equivariant principal homogeneous action. Thus each $\mathrm{Pic}^m(X)$ is an AG torsor for E. In fact, the natural map

$$X \to \mathrm{Pic}^1(X)$$

sending a point of X to its divisor class is an isomorphism of AG torsors for E. We will write X_m for $\mathrm{Pic}^m(X)$.

Now further suppose that X is everywhere locally trivial. Then each X_m is as well, simply by "multiplying" the local point on X by m. Thus each X_m yields an element $\xi_m \in Ш(E/F)$. We claim that ξ_m is just $m\xi_1$. To prove this one must identify the Baer sum of X_m and $X_{m'}$ with $X_{m+m'}$. Since for once we actually have a candidate variety for $X_m \oplus X_{m'}$ it is possible to show that $X_m \oplus X_{m'} \cong X_{m+m'}$ by showing that $X_{m+m'}$ satisfies the appropriate universal property; we omit the details. In any event, this fact immediately implies our claim.

We know that $Ш(E/F)$ is a torsion group, so there is some $n > 0$ such that $n\xi_1 = 0$. Thus $\xi_n = 0$, so $X_n \cong E$ as E-torsors. In particular, X_n has an F-rational point. Thus X has an F-rational divisor class of degree n. By Corollary 1.3 X has an F-rational divisor. Choose one such and call it D.

From here we will begin to omit some more details. Suppose that $n \geq 3$. (The $n = 2$ case is quite interesting but doesn't work for our present arguments.) Let $\mathcal{O}_X(D)$ be the invertible $\mathcal{O}_X$-module of rational functions with poles bounded by D. Then by Riemann-Roch $H^0(X, \mathcal{O}_X(D))$ has dimension n over F, since X has genus 1. Thus we get a map

$$X \to \mathbb{P}^{n-1}_F,$$

where the $\mathbb{P}^{n-1}_F$ is the space of linear functionals on $H^0(X, \mathcal{O}_X(D))$, given by sending $x \in X$ to the "evaluation at x" functional. (The range is projective space over F since D is defined over F.) In fact, one can show that this is actually a closed immersion with projectively normal image. In particular, we can realize X as a curve in $\mathbb{P}^{n-1}_F$ of genus 1 and degree n.

Now let us consider all elements of order n in all Shafarevich-Tate groups of all elliptic curves over F. Our above construction tells us that every such cohomology class is represented by a smooth, projectively normal curve of genus 1 and degree n in $\mathbb{P}^{n-1}_F$. There happens to exist a quasi-projective variety C_n, called the *Chow variety*, defined over $\mathbb{Q}$, whose F-valued points classify all projectively normal curves in $\mathbb{P}^{n-1}_F$ of degree n and genus 1. In fact, there are "Chow coordinates" giving an explicit embedding of C_n in some large projective space. Thus each element of $Ш(E/F)$ for some E/F yields a point in C_n and thus a point in this large projective space. If we could somehow bound the heights of such points in terms of the coefficients of E (as from the example of Lecture 12, Theorem 1.4 may at least seem a reasonable hope), the fact that there are only a finite number of F-rational points of projective space with bounded height would show that $Ш(E/F)$ was finite for all elliptic curves E defined over F.

2. Direct Limits of Selmer Groups

2.1. Passage to the Limit. Let B be an abelian variety over a field F and let N be a positive integer. (The reason for the sudden shift in notation will become apparent in the next section.) We consider the N-torsion $B[N]$ as a G_F-module with its abelian variety finite/singular structure induced by B. (See Lecture 9, Section 2.2.) Thus we have defined (finite) Selmer groups

$$H^1_f(G_F, B[N]) = \mathcal{S}_N(B/F).$$

Now, choose another positive integer M. Then the inclusion $B[N] \hookrightarrow B[NM]$ induces a map

$$H^1_f(G_F, B[N]) \to H^1_f(G_F, B[NM]).$$

(To check that this map exists one just needs to check that the local maps

$$H^1(G_v, B[N]) \to H^1(G_v, B[NM])$$

send finite parts to finite parts for all v; this follows easily from the definition of the abelian variety structure.) Thus we can form the direct limit (over the multiplicative system of positive integers)

$$H^1_f(G_F, B_{\text{tors}}) \stackrel{\text{def}}{=} \varinjlim_N H^1_f(G_F, B[N]).$$

In other notation, this is

$$\mathcal{S}_\infty(B/F) \stackrel{\text{def}}{=} \varinjlim_N \mathcal{S}_N(B/F).$$

Recall that there is an exact sequence

$$0 \to B(F)/NB(F) \to \mathcal{S}_N(B/F) \to Ш(B/F)[N] \to 0.$$

Writing $B(F)/NB(F)$ as $B(F) \otimes \frac{1}{N}\mathbb{Z}/\mathbb{Z}$ we have a natural commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B(F) \otimes \frac{1}{N}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathcal{S}_N(B/F) & \longrightarrow & Ш(B/F)[N] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B(F) \otimes \frac{1}{NM}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathcal{S}_{NM}(B/F) & \longrightarrow & Ш(B/F)[NM] & \longrightarrow & 0 \end{array}$$

Taking the direct limit yields the following proposition.

PROPOSITION 2.1. *There is an exact sequence*

$$0 \to B(F) \otimes \mathbb{Q}/\mathbb{Z} \to \mathcal{S}_\infty(B/F) \to Ш(B/F) \to 0.$$

This construction yields a covariant function in B/F.

2.2. The Shafarevich-Tate Conjecture. We now state the Shafarevich-Tate conjecture, which we have eluded to many times before.

CONJECTURE 2.2 (Shafarevich-Tate). $Ш(B/F)$ *is finite for any abelian variety* B *defined over a number field* F.

Recall that we already know that $Ш(B/F)$ is torsion (since it is a subgroup of the torsion group $H^1(G_F, B(\bar{F}))$). Further, we know that $Ш(B/F)[N]$ is finite for all N, since $\mathcal{S}_N(B/F)$ is. We can break the Shafarevich-Tate conjecture up into two somewhat distinct parts.

CONJECTURE 2.3 (Shafarevich-Tate).

(1) *The p-primary component $Ш(B/F)_p$ of $Ш(B/F)$ has trivial p-divisible part. (We already know that it has finite corank since $Ш(B/F)[p]$ is finite.)*
(2) $Ш(B/F)[p] = 0$ *for almost all p.*

Let E be an elliptic curve over $\mathbb{Q}$. There are two main approaches to the Shafarevich-Tate conjecture. The first, which one might call the classical Fermat descent method, is to fix a prime p and to try to compute $Ш(E/\mathbb{Q})_p$. This sometimes works for small p, but can yield neither (1) nor (2) of Conjecture 2.3. The second method, due to Kolyvagin and Rubin, instead is quite good at showing that $Ш(E/\mathbb{Q})_p$ is trivial for almost all p simultaneously.

We now describe a contravariant limit of the Selmer groups, which works well under the assumption that $Ш(B/F)$ is finite. We use the injection

$$\mathbb{Q}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$$

to get a map

$$B(F) \otimes \mathbb{Q}/\mathbb{Z} \to B(F) \otimes \mathbb{R}/\mathbb{Z}.$$

Next we push out our exact sequence

$$0 \to B(F) \otimes \mathbb{Q}/\mathbb{Z} \to \mathcal{S}_\infty(B/F) \to Ш(B/F) \to 0;$$

that is, we define a group $\mathcal{S}^\dagger(B/F)$ to be the unique group making

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B(F) \otimes \mathbb{Q}/\mathbb{Z} & \longrightarrow & \mathcal{S}_\infty(B/F) & \longrightarrow & Ш(B/F) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & B(F) \otimes \mathbb{R}/\mathbb{Z} & \longrightarrow & \mathcal{S}^\dagger(B/F) & \longrightarrow & Ш(B/F) & \longrightarrow & 0 \end{array}$$

a commutative diagram with exact rows. Since $B(F)$ is finitely generated, $B(F) \otimes \mathbb{R}/\mathbb{Z}$ is a compact topological group. Since $Ш(B/F)$ is assumed to be finite, $\mathcal{S}^\dagger(B/F)$ has a natural structure of compact topological group. Thus its dual

$$\Sigma(B/F) = \mathrm{Hom}(\mathcal{S}^\dagger(B/F), \mathbb{R}/\mathbb{Z})$$

is a finitely generated abelian group, and Σ is contravariant in B/F.

3. Conditions on Galois Representations

3.1. Conditions. In this section we will specify the sorts of Galois representations which we will be considering. Fix a prime $p > 2$ and let A be a local, finite, faithfully flat $\mathbb{Z}_p$-algebra. (Thus A is free of finite rank over $\mathbb{Z}_p$.) For example, A could be the ring of integers of a finite extension of $\mathbb{Q}_p$. We will write $\mathfrak{m}$ for the maximal ideal of A and k for the residue field $A/\mathfrak{m}$.

Let F be a number field with our usual conventions and let Σ be a finite set of places of F. We will always assume that Σ contains p and all archimedean places. Let $\bar{F}^\Sigma$ be the maximal extension of F in the fixed algebraic closure $\bar{F}$ which is unramified outside of Σ and set $G_{F,\Sigma} = \mathrm{Gal}(\bar{F}^\Sigma/F)$.

Let H be a free A-module of rank 2 with an A-linear action of $G_{F,\Sigma}$; thus H is an $A[G_F]$-module which is unramified outside of Σ. We will write ρ for the representation

$$\rho : G_{F,\Sigma} \to \mathrm{Aut}_A(H) \cong \mathrm{GL}_2(A)$$

and $\overline{\rho}$ for the *residual representation*

$$\overline{\rho} : G_{F,\Sigma} \to \mathrm{Aut}_k(H \otimes_A k) \cong \mathrm{GL}_2(k).$$

We are usually only interested in ρ up to conjugation in $\mathrm{GL}_2(A)$, so that the choice of basis is not important.

We wish to specify the determinant of ρ. Recall that the *p-cyclotomic character* χ is the map

$$\chi : \mathrm{Gal}(F(\zeta_{p^\infty})/F) \to \mathbb{Z}_p^*$$

giving the action of the Galois group on the group of p-power roots of unity. We consider χ as a map to A^* by composing with the structure map $\mathbb{Z}_p^* \to A^*$. We require that the determinant

$$\det \rho : G_{F,\Sigma} \to A^*$$

of ρ equal χ.

This requirement has some interesting consequences. First, let λ be a place of F not in Σ. Then we can choose a Frobenius element Fr_λ for λ in $G_{F,\Sigma}$. We will call

$$T_\lambda = \mathrm{tr}\, \rho(\mathrm{Fr}_\lambda) \in A$$

the λ^{th} *Hecke operator* for reasons that will become clear later. $-T_\lambda$ is the coefficent of x in the characteristic polynomial

$$x^2 - T_\lambda x + \det \rho(\mathrm{Fr}_\lambda)$$

of Fr_λ. By the p-cyclotomic determinant condition

$$\det \rho(\mathrm{Fr}_\lambda) = \chi(\mathrm{Fr}_\lambda) = \mathbf{N}_{F/\mathbb{Q}}(\lambda),$$

since Fr_λ is just $\mathbf{N}_{F/\mathbb{Q}}(\lambda)$ powers on residue fields and thus on roots of unity. Thus we have an Eichler-Shimura type relation

$$\mathrm{Fr}_\lambda^2 - T_\lambda \,\mathrm{Fr}_\lambda + \mathbf{N}_{F/\mathbb{Q}}(\lambda) = 0.$$

Next, assume that F has at least one real embedding. Then let c be any choice of complex conjugation for this embedding; equivalently c is the non-trivial element of a decomposition group of a real valuation. Since c has order 2, $\overline{\rho}(c)$ has order 2 in $\mathrm{GL}_2(k)$. However, $\chi(c) = -1$ since complex conjugation acts as inversion on roots of unity, so $\det \overline{\rho}(c) = -1$. It now follows from an easy computation that $\overline{\rho}(c)$ is not a scalar matrix, so $\overline{\rho}$ is called an *odd* representation.

3.2. An Example : Tate Modules of Elliptic Curves. Let E be an elliptic curve over F. Let Σ consist of p, the archimedean places and those places at which E/F has bad reduction. Take $A = \mathbb{Z}_p$ and set

$$H = \varprojlim_{\nu} E[p^\nu],$$

the maps of the inverse system being

$$E[p^{\nu+1}] \xrightarrow{p} E[p^\nu].$$

Then by [**Si-AEC**, Chapter 3, Proposition 7.1] H is free of rank 2 over $\mathbb{Z}_p$. H has a natural G_F action which by [**Si-AEC**, Chapter 7, Proposition 4.1] is unramified outside of Σ. Further the Weil pairing shows that the determinant

$$G_{F,\Sigma} \to \wedge_A^2 H$$

is just the p-cyclotomic character χ. (See [**Si-AEC**, Chapter 3, Proposition 8.3].) So H satisfies all of our conditions. The Hecke operators T_λ for $\lambda \notin \Sigma$ are computed in [**Si-AEC**, Chapter 5, Proposition 2.3]; they are given by

$$T_\lambda = 1 + \mathbf{N}_{F/\mathbb{Q}}(\lambda) - |E(k_\lambda)| \in \mathbb{Z} \subseteq \mathbb{Z}_p,$$

where k_λ is the residue field of F_λ. (Note that this is independent of the choice of p.)

3.3. Principal Polarizations. We continue to let A and H be as before. In this section we consider pairings

$$(\cdot,\cdot) : H \otimes_{\mathbb{Z}_p} H \to \mathbb{Z}_p(1).$$

We say that $(\cdot,\cdot)$ is $G_{F,\Sigma}$-*equivariant* if

$$(gm, gn) = g(m,n)$$

for all $m, n \in H$ and $g \in G_{F,\Sigma}$. We say that $(\cdot,\cdot)$ is A-*Hermetian* if

$$(am, n) = (m, an)$$

for all $m, n \in H$ and $a \in A$. Finally, we say that $(\cdot,\cdot)$ is *skew-symmetric* if

$$(m,n) = -(n,m)$$

for all $m, n \in H$.

LEMMA 3.1. *Let*

$$(\cdot,\cdot)_\psi : H \otimes_{\mathbb{Z}_p} H \to \mathbb{Z}_p(1)$$

be a $G_{F,\Sigma}$-equivariant, A-Hermetian, skew-symmetric self-pairing on H. Let

$$\psi : H \to \mathrm{Hom}_{\mathbb{Z}_p}(H, \mathbb{Z}_p(1))$$

be the induced map, given by sending $m \in H$ to the map sending $n \in H$ to $(m,n)_\psi$. Then if ψ is an isomorphism of $\mathbb{Z}_p$-modules, it is also an isomorphism of $A[G_{F,\Sigma}]$-modules.

PROOF. Note that $\mathbb{Z}_p$ acts on the $\mathbb{Z}_p(1)$ (or equivalently on the H) in $\mathrm{Hom}_{\mathbb{Z}_p}(H, \mathbb{Z}_p(1))$, while A acts only on the H and $G_{F,\Sigma}$ acts on both factors in the usual adjoint way. The lemma now follows immediately from some easy computations. □

LEMMA 3.2. *An A-Hermetian, skew-symmetric pairing*

$$(\cdot,\cdot) : H \otimes_{\mathbb{Z}_p} H \to \mathbb{Z}_p(1)$$

is automatically $G_{F,\Sigma}$-equivariant.

PROOF. A pairing as above is by definition the same as a $\mathbb{Z}_p$-homomorphism

$$\wedge^2_A H \to \mathbb{Z}_p(1),$$

where $\wedge^2_A H$ is the second exterior power of H. Furthermore, it follows immediately from the definitions that $G_{F,\Sigma}$-equivariance of the pairing is the same as $G_{F,\Sigma}$-equivariance of the map on the exterior power. But here $G_{F,\Sigma}$-equivariance is automatic: by the p-cyclotomic determinant condition, $G_{F,\Sigma}$ acts on $\wedge^2_A H$ via the cyclotomic character, which is exactly how $G_{F,\Sigma}$ acts on $\mathbb{Z}_p(1)$. $\mathbb{Z}_p$-linearity now completes the proof. □

LEMMA 3.3 (Schur's Lemma). *Let Π be a profinite group and $\rho : \Pi \to \mathrm{GL}_n(R)$ a continuous homomorphism, where R is a complete local ring with residue field k. Suppose that the residual representation $\overline{\rho}$ is absolutely irreducible. Then the only matrices which commute with the image of ρ are the scalar matrices.*

PROPOSITION 3.4. *Let*

$$(\cdot,\cdot)_\psi : H \otimes_{\mathbb{Z}_p} H \to \mathbb{Z}_p(1)$$

be a $G_{F,\Sigma}$-equivariant, A-hermetian, skew-symmetric pairing on H. Let

$$\psi_0 : \wedge^2_A H \to \mathbb{Z}_p(1)$$

be the induced map on the exterior square. Then $(\cdot,\cdot)_\psi$ is perfect if and only if $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge^2_A H, \mathbb{Z}_p(1))$ is free of rank 1, generated by ψ_0.

PROOF. First suppose that $(\cdot,\cdot)_\psi$ is perfect. Let

$$\psi : H \xrightarrow{\cong} \mathrm{Hom}_{\mathbb{Z}_p}(H, \mathbb{Z}_p(1))$$

be the map induced by $(\cdot,\cdot)_\psi$ and let

$$f : H \to \mathrm{Hom}_{\mathbb{Z}_p}(H, \mathbb{Z}_p(1))$$

be any other $G_{F,\Sigma}$-equivariant homomorphism induced from some map

$$f_0 : \wedge^2_A H \to \mathbb{Z}_p(1).$$

Then

$$\psi^{-1} \circ f : H \to H$$

is a $G_{F,\Sigma}$-equivariant endomorphism of H. In other words, the matrix of $\psi^{-1} \circ f$ commutes with the image of $G_{F,\Sigma}$ in $\mathrm{Aut}_A(H)$. Thus, by Lemma 3.3, $\psi^{-1} \circ f$ is a scalar. So $f = a\psi$ for some $a \in A$, so $f_0 = a\psi_0$. Thus ψ_0 is an A-generator of $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge^2_A H, \mathbb{Z}_p(1))$. (The above argument in fact shows that every $G_{F,\Sigma}$-equivariant, A-Hermetian self-pairing from H to $\mathbb{Z}_p(1)$ is skew-symmetric.)

It remains to show that $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge^2_A H, \mathbb{Z}_p(1))$ is free of rank 1 over A. This, however, is clear from the fact that $\wedge^2_A H$ is free of rank 1 over A, so that $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge^2_A H, \mathbb{Z}_p(1))$ has the same rank over $\mathbb{Z}_p$ as A does.

For the converse, we suppose that ψ_0 is an A-generator of the free rank 1 A-module $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge^2_A H, \mathbb{Z}_p(1))$. The $G_{F,\Sigma}$-action plays no role here, so we choose an A-basis x, y of H and a $\mathbb{Z}_p$-generator ζ of $\mathbb{Z}_p(1)$. Now

$$\wedge^2_A H = (x \wedge y)A$$

and

$$\mathbb{Z}_p(1) = \zeta\mathbb{Z}_p.$$

$\psi_0 : (x \wedge y)A \to \zeta\mathbb{Z}_p$ can thus be simply written as

$$(x \wedge y)A \mapsto \zeta \,\mathrm{tr}(a),$$

where

$$\mathrm{tr} : A \to \mathbb{Z}_p$$

is a generator of the free rank 1 A-module $\mathrm{Hom}(A, \mathbb{Z}_p)$. (tr is called a *Gorenstein trace*.)

We now recover $(\cdot,\cdot)_\psi$ by $(x,x)_\psi = 0$, $(y,y)_\psi = 0$ and $(x,y)_\psi = \zeta\,\mathrm{tr}(1)$. The map

$$\psi : xA \oplus yA \to \mathrm{Hom}_{\mathbb{Z}_p}(yA, \zeta\mathbb{Z}_p) \oplus \mathrm{Hom}_{\mathbb{Z}_p}(xA, \zeta\mathbb{Z}_p)$$

can now be computed as

$$(xa, yb) \mapsto (a \cdot \mathrm{tr}, b \cdot \mathrm{tr}),$$

and this is an isomorphism since tr is an A-basis for $\mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Z}_p)$. This completes the proof. □

DEFINITION 7. A $G_{F,\Sigma}$-equivariant, A-Hermetian, skew-symmetric perfect pairing

$$H \otimes_{\mathbb{Z}_p} H \to \mathbb{Z}_p(1)$$

will be called a *principal polarization* or simply a *polarization*.

In fact, it follows from Proposition 3.4 that a principal polarization exists if and only if A is Gorenstein. See [**Ti**, Section 1].

3.4. Moment Representations. We let A and H be as before. For any $\nu > 0$, $\mathrm{Sym}^\nu_A H$ is a free A-module of rank $\nu+1$; however, in order to get the theory to work properly we need to twist the symmetric powers. Precisely, if $\nu = 2m+1$ is odd we define

$$W^\nu = \mathrm{Sym}^\nu_A H \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(-m)$$

and if $\nu = 2m+2$ is even we define

$$W^\nu = \mathrm{Sym}^\nu_A H \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(-m).$$

(Note that W^1 and W^2 are still just $\mathrm{Sym}^1_A H$ and $\mathrm{Sym}^2_A H$ respectively.) So W^ν is free of rank $\nu+1$ over A.

We will write

$$W_\nu = (W^\nu)^* = \mathrm{Hom}(W^\nu, \mu_{p^\infty}) = \mathrm{Hom}(\mathrm{Sym}^\nu_A H, \mu_{p^\infty}(m))$$

for the Cartier dual of W^ν. We will also write ρ_ν for the representation

$$G_{F,\Sigma} \to \mathrm{Aut}_{A/J}(W_\nu)$$

induced by H and ρ^J_ν for the restriction of ρ^ν to $W_\nu[J]$.

If H has a principal polarization, it is not difficult to show that

$$W_2 \cong \mathrm{End}^0_A(H) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p,$$

where $\mathrm{End}^0_A(H)$ is the module of A-linear endomorphisms of H of trace 0. For relations of this fact to the deformation theory of Galois representations see [**Maz**, Chapters 4 and 5].

3.5. Properties of Representations. In this section we summarize some properties of representations which will be useful to us. Let A be a ring as before. Let W^* be a free A-module of finite rank n with an A-linear action of $G = G_{F,\Sigma}$. Let $W = \mathrm{Hom}(W^*, \mu_{p^\infty})$ be its Cartier dual. W is made into an A-module by the action of A on W^*. For any ideal J of A of finite index we define

$$W[J] = \cap_{\alpha \in J} W[\alpha],$$

where $W[\alpha]$ is the kernel of multiplication by α on W. Note that $W[J]$ and W^*/JW^* are Cartier dual.

LEMMA 3.5. *Let $\alpha \in A$ be a non-zero divisor. Then α divides some power of l in A and αA has finite index in A.*

PROOF. Since A is finite over $\mathbb{Z}_l$ and α is a non-zero divisor, α necessarily satisfies some monic linear equation of the form

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

with $a_i \in \mathbb{Z}_l$ and $a_0 \neq 0$. Thus α divides a_0, which proves the first statement. Since $a_0 A \subseteq \alpha A$ and $a_0 A$ visibly has finite index in A (as A is free of finite rank over $\mathbb{Z}_l$), the second statement is now clear as well. □

LEMMA 3.6. *Let W be an A-module and let t be a non-zero element of W annihilated by some power of l. Then there exists $\alpha \in A$ such that $\alpha t \neq 0$ and $\alpha t \in W[\mathfrak{m}]$.*

PROOF. Since t is l-power torsion, there is a largest power l^n of l such that $t_0 = l^n t \neq 0$; thus $t_0 \in W[l]$. Note that $W[l]$ is a module over the artinian ring A/lA. Let $\alpha_1, \ldots, \alpha_m$ be generators of $\mathfrak{m}$ in A; they also generate the maximal ideal of A/lA and are therefore nilpotent in this ring. It follows that some power of α_1 annihilates t_0; let n_1 be the smallest such power, and set $t_1 = \alpha_1^{n_1-1} t_0$. Continuing in this way, we obtain a non-zero element $t_m = \alpha t$ where $\alpha = l^n \alpha_1^{n_1-1} \cdots \alpha_m^{n_m-1}$. This t_m is killed by every generator of $\mathfrak{m}$, so it is clearly in $W[\mathfrak{m}]$. □

LEMMA 3.7. *Let W be a $\mathbb{Z}_l$-torsion A-module. If $W[\mathfrak{m}] = 0$, then $W = 0$.*

PROOF. Suppose that $W \neq 0$ and let t be a non-zero element of W. By Lemma 3.6 there is some $\alpha \in A$ such that αt is non-zero and annihilated by $\mathfrak{m}$. Thus $W[\mathfrak{m}] \neq 0$, which yields the desired contradiction. □

CHAPTER 14

Lecture 14

1. Structures on Galois Representations

1.1. Finite/Singular Structures. Let p be a prime number. Fix a global field F and a finite set Σ of places of F containing p and all archimedean places. Let A be as in Lecture 13, Section 3.1 and let W^* be a free A-module of rank n with an A-linear action of $G_{F,\Sigma}$, where $G_{F,\Sigma}$ is the Galois group of the maximal extension of F unramified outside of Σ. We can realize this action as a representation

$$\rho^* : G_{F,\Sigma} \to \mathrm{Aut}_A(W^*) \cong \mathrm{GL}_n(A),$$

the last isomorphism given by any choice of any A-basis for W^*.

Since W is free of finite rank over $\mathbb{Z}_p$, its Cartier dual $W = \mathrm{Hom}(W^*, \mu_{p^\infty})$ is a discrete, torsion A-module with an A-linear $G_{F,\Sigma}$-action. We will write

$$\rho : G_{F,\Sigma} \to \mathrm{Aut}_A(W)$$

for the representation of $G_{F,\Sigma}$ on W.

Let $\mathfrak{m}$ be the maximal ideal of A and let k be the residue field $A/\mathfrak{m}$. We make the assumption that the residual representation

$$\overline{\rho}^* : G_{F,\Sigma} \to \mathrm{Aut}_k(W^* \otimes_A k)$$

is *absolutely irreducible*; this just means that the representation

$$\overline{\rho}^* \otimes_k \overline{k} : G_{F,\Sigma} \to \mathrm{Aut}_{\overline{k}}(W^* \otimes_A \overline{k})$$

is irreducible. This is in fact equivalent to $\overline{\rho} : G_{F,\Sigma} \to \mathrm{Aut}_k(W[\mathfrak{m}])$ being absolutely irreducible, as is easily seen.

Suppose that we are given a finite/singular structure on W. That is, for all places v of F we have chosen subgroups

$$H^1_f(G_v, W) \subseteq H^1(G_v, W)$$

which agree with the standard choices for almost all v. This in turn induces a Cartier dual finite/singular structure on W^*, so that $H^1_f(G_v, W)$ and $H^1_f(G_v, W^*)$ are orthogonal complements under Tate local duality for all v.

Let J be an ideal of A such that A/J is finite, and thus artinian. We will write $W[J]$ for the "kernel" of multiplication by J on W; that is,

$$W[J] = \cap_{\alpha \in J} W[\alpha],$$

where $W[\alpha]$ is the kernel of multiplication by α on W. One can use the given finite/singular structures on W to induce structures on $W[J]$ as follows: one simply

[0]Last modified September 4, 2003

defines $H^1_f(G_v, W[J])$ to be the unique subgroup of $H^1(G_v, W)$ making the diagram

$$\begin{array}{ccc} H^1_f(G_v, W[J]) & \longrightarrow & H^1_f(G_v, W) \\ \big\downarrow & & \big\downarrow \\ H^1(G_v, W[J]) & \xrightarrow{j} & H^1(G_v, W) \end{array}$$

cartesian. That is, one sets

$$H^1_f(G_v, W[J]) = \{h \in H^1(G_v, W[J]) \mid j(h) \in H^1_f(G_v, W)\}.$$

Of course, we must show that this definition really does give a finite/singular structure on $W[J]$. This follows from the commutative diagram with exact columns

$$\begin{array}{ccc} 0 & & 0 \\ \big\downarrow & & \big\downarrow \\ H^1(\mathfrak{g}_v, W[J]) & \longrightarrow & H^1(\mathfrak{g}_v, W) \\ \big\downarrow & & \big\downarrow \\ H^1(G_v, W[J]) & \longrightarrow & H^1(G_v, W) \\ \big\downarrow & & \big\downarrow \\ \mathrm{Hom}(\mathcal{I}_v, W[J]) & \hookrightarrow & \mathrm{Hom}(\mathcal{I}_v, W) \end{array}$$

Specifically, an easy diagram chase shows that the middle square is cartesian; thus if W is unramified and has the standard finite/singular structure at v (both of which are true for almost all v by assumption), then this identifies our choice of $H^1_f(G_v, W[J])$ with the standard choice $H^1(\mathfrak{g}_v, W[J])$.

In addition, since W^*/JW^* is Cartier dual to $W[J]$, we get an induced finite/singular structure on W^*/JW^*. We will always assume that all $W[J]$ and W^*/JW^* have finite/singular structures induced from some fixed structure on W in this way.

We will write

$$\rho_J : G_{F,\Sigma} \to \mathrm{Aut}_{A/J}(W[J])$$

and

$$\rho^*_J : G_{F,\Sigma} \to \mathrm{Aut}_{A/J}(W^*/JW^*)$$

for the representations induced by ρ and ρ^*.

The Selmer groups of W and $W[J]$ are related in a particularly simple way.

LEMMA 1.1. *For any ideal J of A of finite index we have*

$$H^1(G_F, W[J]) = H^1(G_F, W)[J]$$

and

$$H^1_f(G_F, W[J]) = H^1_f(G_F, W)[J].$$

PROOF. Let $0 \neq \alpha \in J$ and consider the exact sequences

$$0 \to W[\alpha] \to W \to \alpha W \to 0$$

and

$$0 \to \alpha W \to W \to W/\alpha W \to 0.$$

The rows and columns in the commutative diagram

$$\begin{array}{ccccccc} & & & & & & (W/\alpha W)^{G_F} \\ & & & & & & \downarrow \\ (\alpha W)^{G_F} & \longrightarrow & H^1(F, W[\alpha]) & \longrightarrow & H^1(F, W) & \longrightarrow & H^1(F, \alpha W) \\ & & & & & \searrow^{\alpha} & \downarrow \\ & & & & & & H^1(F, W) \end{array}$$

are exact. One cheks that the absolute irreducibility of $W[\mathfrak{m}]$ implies that $(\alpha W)^{G_F} = (W/\alpha W)^{G_F} = 0$. Thus by the above diagram $H^1(F, W[\alpha])$ injects into $H^1(F, W)$ and identifies with $H^1(F, W)[\alpha]$. This gives the first equality in the case that J is principal, and since A is noetherian and $W^{G_F} = 0$, Lemma 1.2 below finishes the proof.

For the second equality, we just use the commutative diagram with exact columns

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ H^1_f(G_F, W[J]) & \longrightarrow & H^1_f(G_F, W)[J] \\ \downarrow & & \downarrow \\ H^1(G_F, W[J]) & \xrightarrow{\cong} & H^1(G_F, W)[J] \\ \downarrow & & \downarrow \\ \oplus_v H^1_s(G_v, W[J]) & \longrightarrow & \oplus_v H^1_s(G_v, W)[J] \end{array}$$

A diagram chase and the definition of the induced finite singular structure on $W[J]$ show that the top square is cartesian, and thus that the first horizontal arrow is an isomorphism. □

LEMMA 1.2. *Let M and N be submodules of a G-module W. Suppose that $H^1(G, M)$ and $H^1(G, N)$ inject into $H^1(G, W)$. If also $W^G = 0$, then $H^1(G, M \cap N)$ injects into $H^1(G, W)$ and is equal to the intersection of $H^1(G, M)$ and $H^1(G, N)$.*

PROOF. Let Z, Z_M, Z_N, B, B_M, B_N be the cocycles and coboundaries for W, M and N respectively. Z_M and Z_N are naturally submodules of Z, and the injectivity assumption means exactly that $B_M = Z_M \cap B$ and $B_N = Z_N \cap B$. (That is, every coboundary ${}^g w - w$ which has image in M or N has a representative with w in M or N respectively.) Thus

$$H^1(G, M) \cap H^1(G, N) = Z_M/(Z_M \cap B) \cap Z_N/(Z_N \cap B) = Z_M \cap Z_N/(Z_M \cap Z_N \cap B).$$

Clearly $Z_M \cap Z_N$ is just the cocycles for $M \cap N$, so it remains to show that $Z_M \cap Z_N \cap B$ are the coboundaries. It is clear that it contains the coboundaries, so suppose that we have $w \in W$ such that ${}^g w - w \in M \cap N$ for every g. Then, since $B_M = Z_M \cap B$ and $B_N = Z_N \cap B$, we can find $m \in M$ and $n \in N$ such that

$${}^g w - w = {}^g m - m = {}^g n - n$$

for all g. But then

$$^g(m-n) = m-n,$$

so $m-n \in W^G$. By assumption, then, $m-n=0$, so $m=n \in M \cap N$. This completes the proof. □

1.2. The Δ-Hypothesis. We keep the notation and assumptions of the previous section. Since $W[J]$ is finite (since W has finite corank and J has finite index in A), ρ_J factors through some finite extension F_J of F; that is, ρ_J induces an injection

$$\rho_J : \mathrm{Gal}(F_J/F) \hookrightarrow \mathrm{Aut}_{A/J}(W[J]).$$

We will write Δ_J for $\mathrm{Gal}(F_J/F)$.

The natural exact sequence

$$1 \to G_{F_J} \to G_F \to \Delta_J \to 1$$

induces an inflation/restriction sequence

$$0 \to H^1(\Delta_J, W[J]) \to H^1(G_F, W[J]) \to \mathrm{Hom}(G_{F_J}^{\mathrm{ab}}, W[J])^{\Delta_J}.$$

In fact, the last term can be though of as Δ_J-equivariant homomorphisms if $G_{F_J}^{\mathrm{ab}}$ is given the correct Δ_J-action. Specifically, if $\delta \in \Delta_J$ then choose any lifting $\tilde{\delta}$ of δ to G_F. For any $x \in G_{F_J}^{\mathrm{ab}}$, we define $^\delta x$ to be $\tilde{\delta} x \tilde{\delta}^{-1}$; since $G_{F_J}^{\mathrm{ab}}$ is abelian this does not depend on the choice of lifting of δ. It follows immediately from the relevant definitions that with this action on $G_{F_J}^{\mathrm{ab}}$ and the usual action on $W[J]$, $\mathrm{Hom}(G_{F_J}^{\mathrm{ab}}, W[J])^{\Delta_J}$ is just the Δ_J-equivariant homomorphisms from $G_{F_J}^{\mathrm{ab}}$ to $W[J]$.

Now suppose that $H^1(\Delta_J, W[J]) = 0$. Then we have an injection

$$H^1(G_F, W[J]) \hookrightarrow \mathrm{Hom}_{\Delta_J}(G_{F_J}^{\mathrm{ab}}, W[J]),$$

which we write as $h \mapsto \varphi_h$. Given this, to show that an $h \in H^1(G_F, W[J])$ is 0 it is in turn enough to show that φ_h is 0; to do this it is enough to show that φ_h vanishes on a set of Frobenius elements of density 1. Thus the assumption that $H^1(\Delta_J, W[J]) = 0$ is a very useful one; by the Δ-*hypothesis* we will mean the assumption that $H^1(\Delta_J, W[J]) = 0$ for *every* ideal J of A of finite index.

In fact, this is not a particularly restrictive assumption. To give an example, we consider a slightly more general situation: let M be a free R-module of finite rank n for some finite local ring R of residue characteristic p and let Δ be a subgroup of $\mathrm{GL}_n(R)$. (To relate this to the above situation just take $R = A/J$, $M = W[J]$ and $\Delta = \Delta_J$; Δ_J is a subgroup of $\mathrm{Aut}_{A/J}(W[J]) = \mathrm{GL}_n(R)$.) We will give one condition under which $H^1(\Delta, M) = 0$.

Lemma 1.3 (Sah). *Suppose that there is a non-trivial subgroup C of Δ, of order prime to p, which consists entirely of scalar matrices. Then $H^r(\Delta, M) = 0$ for all r.*

Proof. We have a Hochschild-Serre spectral sequence

$$H^p(\Delta/C, H^q(C, M)) \Rightarrow H^{p+q}(\Delta, M);$$

this makes sense since C is in the center of Δ and thus normal. This shows that it will suffice to show that $H^q(C, M) = 0$ for all q. If $q > 0$ this follows from Lecture 5, Lemma 2.4.

For $q = 0$ we must show that $M^C = 0$. By hypothesis $C \subseteq R^*$. So suppose that there is a non-zero $m \in M$ such that $cm = m$ for all $c \in C$. Then

$$(c-1)m = 0,$$

so $c-1$ is not a unit. Thus $c-1$ lies in the maximal ideal of R, so C is a subgroup of the multiplicative group $1 + \mathfrak{m}$. But this group has order a power of p, while C has order prime to p, which is a contradiction. So $M^C = 0$. □

2. Depth and Kolyvagin-Flach Systems

2.1. Depth. We continue to let A and W be as before. Fix a non-unit ideal J of A of finite index. The induced finite/singular structure on W^*/JW^* yields an exact sequence

$$0 \to H^1_f(G_F, W^*/JW^*) \to H^1(G_F, W^*/JW^*) \to H^1_s(G_F, W^*/JW^*) \to 0.$$

We will now begin to use the notation of Lecture 8, Section 1.2. Let C be some set of elements of the Kolyvagin group $H^1_s(G_F, W^*/JW^*)$. Fix a place v of F and let C' be the A/J-submodule of $H^1_s(G_v, W^*/JW^*)$ generated by $\mathrm{res}_{v,s}(c)$ for $c \in C$. If I is an ideal of A containing J, we will say that C is *of depth I at v* if the quotient of $H^1_s(G_v, W^*/JW^*)$ by C' is annihilated by I.

Let $\mathcal{L}$ be a (not necessarily finite) set of places of F disjoint from Σ. If I is some ideal of A containing J, a *Kolyvagin-Flach system of classes of depth I for W^*/JW^* for $\mathcal{L}$* is an assignment of some subset $C^{(v)}$ of $H^1_s(G_F, W^*/JW^*)$ for each $v \in \mathcal{L}$ such that

- $\mathrm{Supp}\, c = \{v\}$ for all $c \in C^{(v)}$;
- $C^{(v)}$ is of depth I at v.

2.2. The Main Theorem. We will need two more hypotheses in order to get the main theorem. First, we assume that $p \neq 2$; this seems to be a necessary condition for this exposition and not just the result of a lack of care. Second, we assume that there is an involution τ in the image of

$$\overline{\rho} : G_{F,\Sigma} \to \mathrm{Aut}_k(W[\mathfrak{m}])$$

which is *not* a scalar.

In particular, this implies that such a non-scalar involution exists for the representation

$$\rho_J : G_{F,\Sigma} \to \mathrm{Aut}_k(W[J])$$

for any ideal J of finite index in A. To see this, first note that

$$\mathrm{Aut}_{A/J}(W[J]) \to \mathrm{Aut}_k(W[\mathfrak{m}])$$

is surjective with kernel a p-group. Thus we can lift our given τ to an element of $\mathrm{Aut}_{A/J}(W[J])$ in the image of $G_{F,\Sigma}$. It will be of order 2 times a power of p, so taking an appropriate power of this yields the desired non-scalar involution. (It is non-scalar since it still reduces to τ modulo $\mathfrak{m}$, as p is odd.)

Fix such a τ for our fixed ideal J. Let $\mathcal{L}_\tau$ be the set of places of F over which there is a place whose associated Frobenius in F_J is τ; equivalently, $\mathcal{L}_\tau$ is the set of places of F with Frobenius in F_J the conjugacy class of τ. Note that the Tchebatorev density theorem ([**La-ANT**, Chapter 8, Theorem 10]) implies that $\mathcal{L}_\tau$ has positive density; in particular, it is infinite.

THEOREM 2.1. *Let A, W and J be as above. Suppose that the residual representation $\overline{\rho}$ is absolutely irreducible; that the Δ-hypothesis holds; and that there exists a non-scalar involution τ in the image of $\overline{\rho}$. Further suppose that there exists a Kolyvagin-Flach system of classes of depth I for W^*/JW^* for $\mathcal{L}_\tau$, for some ideal I containing J. Then*

$$H^1_f(G_F, W[I]) = H^1_f(G_F, W[J]).$$

Note that the statement of this theorem is very much in the spirit of Mazur's comments in Lecture 8, Section 2.

CHAPTER 15

Lecture 15

1. The Main Theorem

1.1. Statement of the Main Theorem. We briefly recall our running hypotheses. Fix a prime $p \neq 2$. Let F be a number field with absolute Galois group G_F and let $G_{F,\Sigma}$ be the maximal quotient of G_F unramified outside of a finite set Σ of places of F (containing p and the archimedean places). Let A be a local, finite, faithfully flat $\mathbb{Z}_p$-algebra with maximal ideal $\mathfrak{m}$ and residue field k. Let W^* be a free A-module of finite rank (at least 2) with a continuous A-linear action of $G_{F,\Sigma}$. Let $W = \mathrm{Hom}(W^*, \mu_{p^\infty})$ be its Cartier dual. We let

$$\rho : G_{F,\Sigma} \to \mathrm{Aut}_A(W)$$

be the representation of $G_{F,\Sigma}$ on W, and for any ideal J of A of finite index we let

$$\rho_J : G_{F,\Sigma} \to \mathrm{Aut}_{A/J}(W[J])$$

be the restriction of ρ to the submodule

$$W[J] = \cap_{\alpha \in J} W[\alpha].$$

We make three hypotheses on this data. First, we assume that $\overline{\rho}$ is absolutely irreducible. This implies that $W^G = 0$, by Corollary 3.7 of Lecture 13. (Here we need the fact that W has rank at least 2.) Second, for any ideal J, let F_J be the splitting field of ρ_J; it is a finite extension of F. Set $\Delta_J = \mathrm{Gal}(F_J/F)$. We assume that

$$H^1(\Delta_J, W[J]) = 0$$

for all J. Lastly, we suppose that there is a non-scalar involution τ in the image of

$$\overline{\rho} : G_{F,\Sigma} \to \mathrm{Aut}_k(W[\mathfrak{m}]);$$

we can lift this τ to $\mathrm{Aut}_{A/J}(W[J])$ for any ideal $J \subseteq \mathfrak{m}$ of A of finite index, since p is odd. We fix such a τ.

THEOREM 1.1 (Kolyvagin). *With the above notation and hypotheses, suppose in addition that there is a Kolyvagin-Flach system of depth I for W^*/JW^* for $\mathcal{L}_\tau$. Then*

$$H^1_f(G_F, W)[I] = H^1_f(G_F, W)[J].$$

If one does not assume that $H^1(\Delta_J, W[J]) = 0$, then one finds that the product of I and any annihilator of $H^1(\Delta_J, W[J])$ annihilates $H^1_f(G_F, W)[J]$. This will be clear from the proof below.

We will prove this theorem in two stages. Recall that for any place v of F there is a natural restriction map

$$\mathrm{res}_v : H^1(G_F, W[J]) \to H^1(G_v, W[J]).$$

[0]Last modified September 4, 2003

This map sends $H^1_f(G_F, W[J])$ to $H^1_f(G_v, W[J])$, so we also obtain a natural map

$$\mathrm{res}_{s,v} : H^1_s(G_F, W[J]) \to H^1_s(G_v, W[J]).$$

LEMMA 1.2. *With the hypotheses of Theorem 1.1, if $x \in H^1_f(G_F, W[J])$ and $\alpha \in I$, then*

$$\mathrm{res}_v(\alpha x) = 0$$

for all $v \in \mathcal{L}_\tau$.

LEMMA 1.3. *Continue to suppose the hypotheses of Theorem 1.1. Let $X \in H^1_f(G_F, W[J])$ be such that $\mathrm{res}_v(X) = 0$ for all $v \in \mathcal{L}_\tau$. Then $X = 0$.*

It is clear that Lemma 1.2 and Lemma 1.3 suffice to prove the theorem. We note also that the proof of Lemma 1.3 will not require the existence of the Kolyvagin-Flach system.

As a corollary, we obtain the following:

COROLLARY 1.4. *In addition to the hypotheses of Theorem 1.1, suppose that $\mathfrak{m}I \supseteq J$. Then*

$$H^1_f(G_F, W)[I] = H^1_f(G_F, W).$$

PROOF. Everything in $H^1_f(G_F, W)$ is killed by some power of $\mathfrak{m}$, so we prove the corollary for each $H^1_f(G_F, W)[\mathfrak{m}^m]$ by induction on m. The result is clear for $m = 1$, since $J \subseteq \mathfrak{m}$. So suppose that we know the result for $m < n$. Take $x \in H^1_f(G_F, W)[\mathfrak{m}^n]$. Then $\mathfrak{m}^{n-1}(\mathfrak{m}x) = 0$, so by the induction hypothesis we have $I(\mathfrak{m}x) = 0$. So, since $I\mathfrak{m} \supseteq J$, we have $Jx = 0$. Now, by Theorem 1.1, we have $Ix = 0$. This complete the induction. □

1.2. Proof of Lemma 1.2. Fix $v \in \mathcal{L}_\tau$. Since $W[J]$ and W^*/JW^* are Cartier dual, Tate local duality (Lecture 6, Theorem 2.2) yields a perfect cup product pairing

$$H^1_f(G_v, W[J]) \otimes H^1_s(G_v, W^*/JW^*) \to \mathbb{Q}/\mathbb{Z}.$$

Since $v \in \mathcal{L}_\tau$, we have a set $C^{(v)}$ of Kolyvagin-Flach classes such that $\mathrm{res}_{s,v'}(c) = 0$ for $c \in C^{(v)}$ and $v \neq v'$, and if C' is the A-submodule of $H^1_s(G_v, W^*/JW^*)$ generated by $C^{(v)}$, then

$$H^1_s(G_v, W^*/JW^*)/C'$$

is annihilated by I.

Next recall that under our global pairing (see Lecture 8, Section 2)

$$H^1_f(G_F, W[J]) \otimes \oplus_v H^1_s(G_v, W^*/JW^*) \to \mathbb{Q}/\mathbb{Z},$$

$H^1_f(G_F, W[J])$ and $H^1_s(G_F, W^*/JW^*)$ are orthogonal. Since $\mathrm{res}_{s,v'}(c) = 0$ for $c \in C^{(v)}$ and $v' \neq v$, the definition of the pairing and the above orgthogonality imply that

$$\mathrm{res}_v(x) \cup \mathrm{res}_{s,v}(c) = 0$$

for all $c \in C^{(v)}$. Thus, $\mathrm{res}_v(x)$ is contained in the orthogonal complement of C' in $H^1_f(G_v, W[J])$ under Tate local duality. Since Tate local duality is a perfect pairing and I annihilates

$$H^1_s(G_v, W^*/JW^*)/C',$$

it follows immediately that I annihilates $\mathrm{res}_v(x) \in H^1_f(G_v, W[J])$, as desired.

1.3. Proof of Lemma 1.3. Consider the exact sequence

$$1 \to G_{F_J} \to G_F \to \Delta_J \to 1.$$

This yields an inflation-restriction sequence

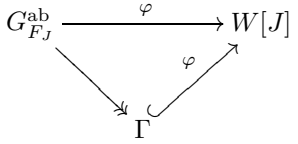
$$0 \to H^1(\Delta_J, W[J]) \to H^1(G_F, W[J]) \to \mathrm{Hom}_{\Delta_J}(G_{F_J}^{\mathrm{ab}}, W[J]).$$

(See Lecture 14, Section 1.2 for a discussion of the Δ_J action on $G_{F_J}^{\mathrm{ab}}$.) By hypothesis, $H^1(\Delta_J, W[J]) = 0$, so it will be enough to show that the image

$$\varphi : G_{F_J}^{\mathrm{ab}} \to W[J]$$

of X in $\mathrm{Hom}_{\Delta_J}(G_{F_J}^{\mathrm{ab}}, W[J])$ is trivial.

Let L be the fixed field of $\ker \varphi$, and set $\Gamma = \mathrm{Gal}(L/F_J)$.



There is an exact sequence

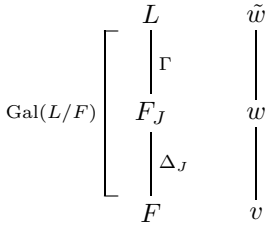
$$1 \to \Gamma \to \mathrm{Gal}(L/F) \to \Delta_J \to 1.$$

Since Γ injects into $W[J]$, it is a finite abelian p-group.

Let τ be our fixed non-scalar involution in Δ_J. Since Γ has odd order we can lift τ to a non-scalar involution $\tilde{\tau} \in \mathrm{Gal}(L/F)$. Let g be any element of Γ and consider $\tilde{\tau}g \in \mathrm{Gal}(L/F)$. By the Tchebatorev density theorem ([**La-ANT**, Chapter 8, Theorem 10]) there exists an unramified place $\tilde{w}$ of L such that

$$\mathrm{Fr}_{L/F}(\tilde{w}) = \tilde{\tau}g.$$

Set $w = \tilde{w}|_{F_J}$ and $v = w|_F$.



By standard properties of Frobenius, we have

$$\mathrm{Fr}_{F_J/F}(w) = \mathrm{Fr}_{L/F}(\tilde{w})|_{F_J} = \tilde{\tau}g|_{F_J} = \tau$$

(so in particular $v \in \mathcal{L}_\tau$), and

$$\mathrm{Fr}_{L/F_J}(\tilde{w}) = (\mathrm{Fr}_{L/F}(\tilde{w}))^{\deg(w/v)} = (\tilde{\tau}g)^2.$$

Here by $\deg(w/v)$ we mean the degree of the local field extension $F_{J,w}/F_v$; it is 2 since τ has order 2 and w/v is unramified.

We claim that since $\mathrm{res}_v(x) = 0$, we have

$$\varphi(\mathrm{Fr}_{L/F_J}(\tilde{w})) = 0.$$

To see this, begin with the commutative diagram

$$\begin{array}{ccc} X \in H^1(G_F, W[J]) & \xrightarrow{\mathrm{res}_v} & H^1(G_v, W[J]) \\ \downarrow & & \downarrow \\ \varphi \in \mathrm{Hom}(G_{F_J}, W[J]) & \longrightarrow & \mathrm{Hom}(G_{F_J,w}, W[J]) \end{array}$$

Since φ factors through $\Gamma = \mathrm{Gal}(L/F_J)$, $\varphi|_{G_{F_J,w}}$ factors through $\mathrm{Gal}(L_{\tilde{w}}/F_{J,w})$, which is generated by $\mathrm{Fr}_{L/F_J}(\tilde{w})$ since $\tilde{w}/w$ is unramified. But $\mathrm{res}_v(X) = 0$, so $\varphi|_{G_{F_J,w}} = 0$; thus $\varphi(\mathrm{Fr}_{L/F_J}(\tilde{w})) = 0$ as claimed.

Combining all of this we have

$$\varphi(\tilde{\tau} g \tilde{\tau} g) = 0.$$

But $\tilde{\tau}^2 = 1$, so $\tilde{\tau} g \tilde{\tau} g = \tilde{\tau} g \tilde{\tau}^{-1} g$. By the definition of the Δ_J-action on Γ, this is none other than ${}^{\tau}g \cdot g$. Thus

$$\varphi({}^{\tau}g) + \varphi(g) = 0,$$

so by Δ_J-equivariance

$$\tau\varphi(g) = -\varphi(g) \in W[J].$$

This is true for all $g \in \Gamma$, so if we let $\mathcal{H}$ be the A-submodule of $W[J]$ generated by $\varphi(\Gamma)$, we have

$$\mathcal{H} \subseteq W[J]^-.$$

Here $W[J]^-$ is the minus eigenspace for τ acting on $W[J]$:

$$W[J]^- = \{z \in W[J] \mid \tau z = -z\}.$$

Note that $W[J]^- \neq W[J]$ since τ is non-scalar. Since φ is Δ_J-equivariant and Δ_J acts A-linearly, $\mathcal{H}$ is Δ_J-stable. But if we consider $\mathcal{H}[\mathfrak{m}] \subseteq W[\mathfrak{m}]^-$, we must have $\mathcal{H}[\mathfrak{m}] = 0$, since $W[\mathfrak{m}]$ is irreducible as a $G_{F,\Sigma}$-representation space and $W[\mathfrak{m}]^- \neq W[\mathfrak{m}]$. But if $\mathcal{H}[\mathfrak{m}] = 0$, then $\mathcal{H} = 0$, by Corollary 3.7 of Lecture 13. Thus $\varphi = 0$ as desired.

2. The Main Theorem for Rank 1 Modules

The end of the proof of Lemma 1.3, and thus the proof of Theorem 1.1, relied very heavily on the fact that $W^G = 0$. Thus need not be true in the case that W has rank 1, even if $\overline{\rho}$ is absolutely irreducible. In fact, the version of the theorem which is useful for rank 1 A-modules is somewhat simpler than the main theorem; essentially, one is able to take $\tau = 1$. We state the result for all W even though it is only useful in practice for W of rank 1.

We keep all of the definitions of the first paragraph of Section 15.1, except that we now allow W to have rank 1. We need not assume that $\overline{\rho}$ is absolutely irreducible or that there is a non-scalar involution τ. The only extra hypothesis we need is the Δ-hypothesis

$$H^1(\Delta_J, W[J]) = 0.$$

We let $\mathcal{L} = \mathcal{L}_1$ be the set of unramified places of F with trivial Frobenius in F_J.

Theorem 2.1. *With the above notation and hypotheses, suppose in addition that there is a Kolyvagin-Flach system of depth I for W^*/JW^* for $\mathcal{L}$. Then*

$$H^1_f(G_F, W)[I] = H^1_f(G_F, W)[J].$$

PROOF. The proof is actually somewhat simpler than the proof of Theorem 1.1. Lemma 1.2 goes through with no changes; Lemma 1.3 in fact simplifies greatly, as one finds that

$$\mathrm{Fr}_{L/F_J}(\tilde{w}) = g,$$

and thus $\varphi(g) = 0$ immediately by Lemma 1.2. □

This theorem is only useful in the case where W has rank 1; in the higher rank cases there are no Kolyvagin-Flach systems for trivial τ.

CHAPTER 16

Lecture 16

1. Other Versions of the Main Theorem

1.1. Characters. We briefly review the theory of eigenspaces of group modules; since it will be sufficient for our applications we restrict attention to the simplest case. So let p be a fixed prime number and let G be an abelian group of order dividing $p-1$. We will write $\widehat{G}$ for the group of characters of G. Since G is of order dividing $p-1$, the image of any character of G lies in μ_{p-1}. Thus, in this set-up, we can identify $\widehat{G}$ with $\mathrm{Hom}(G, \mathbb{Z}_p^*)$.

Let ε be a character of G and define the *ε-idempotent* of $\mathbb{Z}_p[G]$ by

$$e_\varepsilon = \frac{1}{|G|} \sum_{g \in G} \varepsilon^{-1}(g) g \in \mathbb{Z}_p[G].$$

One checks easily that

$$e_\varepsilon e_{\varepsilon'} = \begin{cases} e_\varepsilon & \varepsilon = \varepsilon' \\ 0 & \varepsilon \neq \varepsilon'. \end{cases}$$

Thus the e_ε form a system of idempotents of $\mathbb{Z}_p[G]$, yielding a decomposition

$$\mathbb{Z}_p[G] = \oplus_{\varepsilon \in \widehat{G}} \mathbb{Z}_p[G] e_\varepsilon.$$

Since each $\mathbb{Z}_p[G]e_\varepsilon$ is non-zero (it contains e_ε), it follows from the fact that $\widehat{G}$ has the same order as G that each $\mathbb{Z}_p[G]e_\varepsilon$ is free of rank 1 over $\mathbb{Z}_p$. One also notes that for all $g \in G$,

$$g e_\varepsilon = \varepsilon(g) e_\varepsilon,$$

so that G acts on $\mathbb{Z}_p[G]e_\varepsilon$ via ε.

Now let M be a G-module which is a finite p-group. Then M can be viewed as a $\mathbb{Z}_p[G]$-module, since each element of M is killed by some power of p. The above decomposition of $\mathbb{Z}_p[G]$ yields a decomposition

$$M = \oplus_{\varepsilon \in \widehat{G}} M e_\varepsilon.$$

In fact, one shows easily from the fact that $g e_\varepsilon = \varepsilon(g) e_\varepsilon$ that $M e_\varepsilon$ can also be realized as

$$M e_\varepsilon = \{ m \in M \mid gm = \varepsilon(g) m \text{ for all } g \in G \}.$$

We will also write M^ε for $M e_\varepsilon$, and call it the *ε-eigenspace* of M.

In the case that G has order 2, we will write M^+ and M^- for the eigenspace of the trivial character and the eigenspace of the non-trivial character respectively.

[0]Last modified September 4, 2003

1.2. Galois Groups Acting on Cohomology. We now return to the notation of the previous lecture, although we do not yet assume any hypotheses on W. Let us suppose that we are also given a subfield F_0 of F of index 2, so that F/F_0 is a quadratic extension. Set

$$\mathcal{G} = \mathrm{Gal}(F/F_0).$$

We assume that the G_F-action on W is the restriction of a continuous, A-linear action of G_{F_0} on W.

Let J be an ideal of A of finite index. We claim that $H^1(G_F, W[J])$ has the structure of a $\mathcal{G}$-module. In fact, it has the structure of G_{F_0}-modules, where G_{F_0} acts on G_F by inverse conjugation and on $W[J]$ by the given action. Further, the action of G_F on $H^1(G_F, W[J])$ in this way is trivial ([**Se-LF**, Chapter 7, Section 5, Proposition 3]), so that the G_{F_0}-action factors through $\mathcal{G}$, as claimed. In the same way we can consider $H^1(G_F, W^*/JW^*)$ as a $\mathcal{G}$-module. Given this, the discussion of the previous section yields eigenspace decompositions

$$H^1(G_F, W[J]) = H^1(G_F, W[J])^+ \oplus H^1(G_F, W[J])^-$$

and

$$H^1(G_F, W^*/JW^*) = H^1(G_F, W^*/JW^*) \oplus H^1(G_F, W^*/JW^*)^-.$$

Unfortunately, $H^1_f(G_F, W[J])$ is not necessarily a $\mathcal{G}$-module. In order to give conditions under which it is, we first must consider the $\mathcal{G}$-action induced on the local cohomology groups. So let v be a place of F. Then the action of $\tau \in \mathcal{G}$ yields a map

$$H^1(G_{\tau^{-1}v}, W[J]) = H^1(\tau^{-1}G_v\tau, W[J]) \to H^1(G_v, W[J]).$$

Thus, if $v|_{F_0}$ is inert or ramified in F/F_0, $\mathcal{G}$ does act on $H^1(G_v, W[J])$. However, if $v|_{F_0}$ splits over F into v and v', then $\mathcal{G}$ acts on the direct sum

$$H^1(G_v, W[J]) \oplus H^1(G_{v'}, W[J])$$

by interchanging the factors. In any event, there is a natural $\mathcal{G}$-action on

$$\oplus_v H^1(G_v, W[J])$$

and the natural map

$$\mathrm{res} : H^1(G_F, W[J]) \to \prod_v H^1(G_v, W[J])$$

is $\mathcal{G}$-equivariant, essentially by definition of the action on the local factors.

We make the assumption for the remainder of this section that the $\mathcal{G}$-action respects the finite/singular structure, in the sense that

$$\oplus_v H^1_f(G_v, W[J])$$

is $\mathcal{G}$-stable. The next lemma shows that this is a reasonable condition; the proof is straightforward and we omit it.

LEMMA 1.1. *Let M be a G_{F_0}-module. Let v_0 be a place of F_0 which is unramified in F and let v be a place of F above v_0. Then $H^1(\mathfrak{g}_v, M^{\mathcal{I}_v})$ is $\mathcal{G}$-stable. (In the case that v_0 is inert the meaning of this is clear; if v_0 splits into v and v', this means that the $\mathcal{G}$-action interchanges $H^1(G_v, M^{\mathcal{I}_v})$ and $H^1(G_{v'}, M^{\mathcal{I}_{v'}})$.)*

With this assumption on our finite/singular structures,

$$\oplus_v H^1_s(G_v, W[J])$$

is also a $\mathcal{G}$-module, and $\mathcal{G}$-equivariance of

$$\mathrm{res}_s : H^1(G_F, W[J]) \to \oplus_v H^1_s(G_v, W[J])$$

implies that $H^1_f(G_F, W[J])$ is a $\mathcal{G}$-module as well. In the same way one can impose conditions on the finite/singular structure on W^*/JW^* in order to insure that $H^1_f(G_F, W^*/JW^*)$ is a $\mathcal{G}$-module; we make this assumption as well. We will show in a moment that this assumption is compatible with the usual Cartier dual finite/singular requirements.

Let v be a place of F so that $v|_{F_0}$ is either inert or ramified in F_{v_0}. Then $\mathcal{G}$ acts on $H^1(G_v, W[J])$, and we claim that the Tate local pairing

$$H^1(G_v, W[J]) \otimes H^1(G_v, W^*/JW^*) \to \mathbb{Q}_p/\mathbb{Z}_p$$

is $\mathcal{G}$-invariant. (Equivalently, it is $\mathcal{G}$-equivariant when $\mathbb{Q}_p/\mathbb{Z}_p$ is given the trivial $\mathcal{G}$-action.) To do this it suffices to check equivariance of cup product, Cartier duality and the invariant map. The first follows from functoriality and the second from an easy direct computation. For the last one must go back to the definition of the invariant map (see [**Se-LF**, Chapter 13, Section 3]) and see that each step is $\mathcal{G}$-equivariant; we omit the details.

It follows immediately from this invariance and the fact that p is odd that $H^1(G_v, W[J])^\varepsilon$ and $H^1(G_v, W^*/JW^*)^{-\varepsilon}$ pair to 0, where ε is some choice of sign. Thus Tate local duality restricts to perfect pairings

$$H^1(G_v, W[J])^+ \otimes H^1(G_v, W^*/JW^*)^+ \to \mathbb{Q}_p/\mathbb{Z}_p$$

and

$$H^1(G_v, W[J])^- \otimes H^1(G_v, W^*/JW^*)^- \to \mathbb{Q}_p/\mathbb{Z}_p.$$

These in turn restrict to perfect pairings

$$H^1_f(G_v, W[J])^+ \otimes H^1_s(G_v, W^*/JW^*)^+ \to \mathbb{Q}_p/\mathbb{Z}_p$$

and

$$H^1_f(G_v, W[J])^- \otimes H^1_s(G_v, W^*/JW^*)^- \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Among other things these show that, at least when $v|_{F_0}$ is inert or ramified, the various requirements on finite/singular structures are compatible. We also note that in the same way one can show that the Tate local pairing is $\mathcal{G}$-equivariant for $v|_{F_0}$ which split completely, in the sense that the pairing

$$\big(H^1(G_v, W[J]) \otimes H^1(G_v, W^*/JW^*)\big) \oplus \big(H^1(G_{v'}, W[J]) \otimes H^1(G_{v'}, W^*/JW^*)\big) \to \mathbb{Q}_p/\mathbb{Z}_p \oplus \mathbb{Q}_p/\mathbb{Z}_p$$

is $\mathcal{G}$-equivariant, where the non-trivial element of $\mathcal{G}$ acts on $\mathbb{Q}_p/\mathbb{Z}_p \oplus \mathbb{Q}_p/\mathbb{Z}_p$ by interchanging the factors. This again shows that the requirements on the finite/singular structures at these places are compatible.

Given the above pairings, it is now possible to define Kolyvagin-Flach systems for these eigenspaces. We let Σ be a finite set of places of F and $\mathcal{L}$ a (not necessarily finite) set of places of F disjoint from Σ. We also let I be some ideal of A containing J and ε some choice of sign.

Definition 8. A *Kolyvagin-Flach system of classes of depth I for $(W^*/JW^*)^\varepsilon$ for $\mathcal{L}$* is an assignment of some subset $C^{(v)}$ of $H^1_s(G_F, W^*/JW^*)^\varepsilon$ for each $v \in \mathcal{L}$ such that $\mathrm{Supp}\, c = \{v\}$ for all $c \in C^{(v)}$ and, if C' is the A-submodule of $H^1_s(G_v, W^*/JW^*)^\varepsilon$ generated by $C^{(v)}$, then

$$H^1_s(G_v, W^*/JW^*)^\varepsilon/C'$$

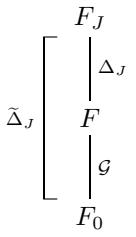
is annihilated by I.

1.3. The Main Theorem for $\pm$ Eigenspaces. We continue with the usual notation. We also continue to assume that $\overline{\rho}$ is absolutely unramified and that $H^1(\Delta_J, W[J]) = 0$ for all ideals J of finite index in A. We substitute a new condition for the existence of a non-scalar involution.

Specificially, let $\widetilde{\Delta}_J$ be the Galois group of F_J over F_0. There is an exact sequence

$$1 \to \Delta_J \to \widetilde{\Delta}_J \to \mathcal{G} \to 1$$

and a field diagram



We make the hypothesis that there is an involution $\tilde{\tau} \in \widetilde{\Delta}_J$ which projects to the non-trivial element in $\mathcal{G}$ and acts on $W[\mathfrak{m}]$ (and thus on $W[J]$) as a non-scalar. We define $\tilde{\mathcal{L}}_{\tilde{\tau}}$ to be the set of places v of F such that there is a place w of F_J lying above v such that

$$\mathrm{Fr}_{F_J/F_0}(w) = \tilde{\tau} \in \widetilde{\Delta}_J.$$

Note that any place $v \in \tilde{\mathcal{L}}_{\tilde{\tau}}$ is inert in F/F_0 since $\tilde{\tau}$ projects to the non-trivial element of $\mathcal{G} = \mathrm{Gal}(F/F_0)$.

THEOREM 1.2 (Kolyvagin). *Let ε be some choice of sign. With the above notation and hypotheses, suppose in addition that there is a Kolyvagin-Flach system of depth I for $(W^*/JW^*)^\varepsilon$ for $\tilde{\mathcal{L}}_{\tilde{\tau}}$. Then*

$$H^1_f(G_F, W)[I]^\varepsilon = H^1_f(G_F, W)[J]^\varepsilon.$$

Note that the hypothesis of Theorem 1.2 are neither clearly weaker nor stronger than those of Theorem 1.1 of Lecture 15, but the conclusion is weaker. Nevertheless, this version is the appropriate one to apply in many situations.

1.4. Proof of Theorem 1.2. The proof of Theorem 1.2 is quite similar to the proof of Theorem 1.1 of Lecture 15. We will again prove it through two lemmas.

LEMMA 1.3. *With the hypotheses of Theorem 1.2, if $x \in H^1_f(G_F, W[J])^\varepsilon$ and $\alpha \in I$, then*

$$\mathrm{res}_v(\alpha x) = 0$$

for all $v \in \tilde{\mathcal{L}}_{\tilde{\tau}}$.

The proof of Lemma 1.3 is almost identical to that of Lemma 1.2 of Lecture 15; we leave the details to the reader.

LEMMA 1.4. *Continue to suppose the hypotheses of Theorem 1.2. Let $X \in H^1_f(G_F, W[J])^\varepsilon$ be such that*

$$\mathrm{res}_v(X) = 0$$

for all $v \in \tilde{\mathcal{L}}_{\tilde{\tau}}$. Then $X = 0$.

PROOF. This proof is the same as that of Lemma 1.3 of Lecture 15 at many points. We again begin with the exact sequence

$$1 \to G_{F_J} \to G_F \to \Delta_J \to 1,$$

which, by the inflation-restriction sequence and the Δ-hypothesis, yields an injection

$$H^1(G_F, W[J]) \hookrightarrow \mathrm{Hom}_{\Delta_J}(G_{F_J}^{\mathrm{ab}}, W[J]).$$

In fact, this map is $\mathcal{G}$-equivariant (it is just restriction), so we get an injection

$$H^1(G_F, W[J])^{\varepsilon} \hookrightarrow \mathrm{Hom}_{\Delta_J}(G_{F_J}^{\mathrm{ab}}, W[J])^{\varepsilon}.$$

Thus it will again be enough to show that the image

$$\varphi : G_{F_J}^{\mathrm{ab}} \to W[J]$$

of X in $\mathrm{Hom}_{\Delta_J}(G_{F_J}^{\mathrm{ab}}, W[J])^{\varepsilon}$ is trivial.

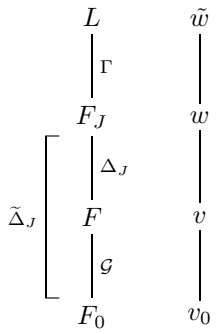
We again let L/F be the splitting field of φ and set $\Gamma = \mathrm{Gal}(L/F_J)$. Thus φ is now thought of as an injection

$$\varphi : \Gamma \hookrightarrow W[J].$$

So Γ is a p-group, and as before it follows that we can lift $\tilde{\tau}$ to an involution $\tilde{\tau}' \in \mathrm{Gal}(L/F_0)$. Now, choose some $g \in \Gamma$ and let $\tilde{w}$ be some place of L such that

$$\mathrm{Fr}_{L/F_0}(\tilde{w}) = \tilde{\tau}' g \in \mathrm{Gal}(L/F_0).$$

($\tilde{w}$ exists by the Tchebatorev density theorem, as usual.) We let w, v and v_0 be the restriction of $\tilde{w}$ to F_J, F and F_0 respectively.



We now have

$$\mathrm{Fr}_{F_J/F_0}(w) = \mathrm{Fr}_{L/F_0}(\tilde{w})|_{F_J} = \tilde{\tau}' g|_{F_J} = \tilde{\tau} \in \widetilde{\Delta}_J,$$

so $v \in \tilde{\mathcal{L}}_{\tilde{\tau}}$. Also,

$$\mathrm{Fr}_{L/F_J}(\tilde{w}) = (\mathrm{Fr}_{L/F_0}(\tilde{w}))^{\deg(w/v_0)} = (\tilde{\tau}' g)^2,$$

since $\tilde{\tau} = \mathrm{Fr}_{F_J/F_0}(w)$ has order 2. Furthermore, exactly as in the proof of Lemma 1.3 of Lecture 15, we have

$$\varphi(\mathrm{Fr}_{L/F_J}(\tilde{w})) = 0,$$

so that

$$\varphi(\tilde{\tau}' g \tilde{\tau}' g) = 0.$$

Thus,

$$\varphi({}^{\tilde{\tau}} g) + \varphi(g) = 0.$$

Now, φ is Δ_J-equivariant, but not necessarily $\widetilde{\Delta}_J$-equivariant. However, it does lie in

$$\mathrm{Hom}_{\Delta_J}(G_{F_J}^{\mathrm{ab}}, W[J])^{\varepsilon}.$$

From this it follows easily, since $\tilde{\tau}$ projects non-trivially to $\mathcal{G}$, that

$$\varphi({}^{\tilde{\tau}}g) = \varepsilon\tilde{\tau}\varphi(g).$$

Thus $\varphi(g)$ lies in the subspace of $W[J]$ on which $\tilde{\tau}$ acts by $-\varepsilon$ and the A-module $\mathcal{H}$ generated by $\varphi(\Gamma)$ lies in $W[J]^{-\varepsilon}$. (Here by $W[J]^{-\varepsilon}$ we mean the $-\varepsilon$ eigenspace for $\tilde{\tau}$.) $\mathcal{H}$ is also Δ_J-stable, since φ is Δ_J-equivariant, so from here one proceeds as before, using the fact that $\tilde{\tau}$ acts as a non-scalar on $W[\mathfrak{m}]$ to conclude that $W[\mathfrak{m}]^{-\varepsilon} \neq W[\mathfrak{m}]$. □

1.5. A Generalization of the Main Theorem. In this section we give one last version of the main theorem. We keep the usual notation and continue to assume that $\overline{\rho}$ is absolutely irreducible and that $H^1(\Delta_J, W[J]) = 0$ for all ideals J of finite index in A. We no longer assume that $p \neq 2$, and instead of assuming that we have a non-scalar involution τ, we simply assume that there is some $\tau \in \Delta_J$ such that

$$W[\mathfrak{m}]/(\tau - 1)W[\mathfrak{m}] \neq 0.$$

THEOREM 1.5 (Rubin). *With the above notation and hypotheses, suppose in addition that there is a Kolyvagin-Flach system of depth I for W^*/JW^* for $\mathcal{L}_\tau$. Then*

$$H^1_f(G_F, W)[I] = H^1_f(G_F, W)[J].$$

PROOF. The proof is quite similar to that of Theorem 1.1 of Lecture 15. Lemma 1.2 of Lecture 15 goes through with no changes. For Lecture 15, Lemma 1.3, we proceed as follows. As usual, it suffices to show that the homomorphism $\varphi : G_{F_J} \to W[J]$ is trivial. However, now we choose also a representative cocycle $c : G_F \to W[J]$ for the cohomology class X. Let L be some finite extension of F through which c factors; then φ necessarily factors through $\mathrm{Gal}(L/F_J) = \Gamma$. That is, we now have maps

$$c : \mathrm{Gal}(L/F) \to W[J]$$

and

$$\varphi : \Gamma \to W[J].$$

Note that φ need no longer be injective on Γ.

Choose any $g \in \Gamma$ and some lifting $\tilde{\tau}$ of τ to $\mathrm{Gal}(L/F)$. By the Tchebatorev density theorem we can find some place $\tilde{w}$ of L such that

$$\mathrm{Fr}_{L/F}(\tilde{w}) = \tilde{\tau}g.$$

Let w and v be the restriction of $\tilde{w}$ to F_J and F respectively. As usual we have

$$\mathrm{Fr}_{F_J/F}(w) = \tau,$$

so that $v \in \mathcal{L}_\tau$.

Now, $c|_{\mathrm{Gal}(L_{\tilde{w}}/F_v)}$ is a coboundary, since $\mathrm{res}_v(X) = 0$. Thus

$$c(\mathrm{Fr}_{L/F}(\tilde{w})) \in (\mathrm{Fr}_{L/F}(\tilde{w}) - 1)W[J];$$

that is,

$$c(\tilde{\tau}g) \in (\tilde{\tau}g - 1)W[J] = (\tau - 1)W[J],$$

since $\tilde{\tau}$ acts on $W[J]$ as τ and g acts trivially on $W[J]$. Since c is a cocycle,

$$c(\tilde{\tau}g) = c(\tilde{\tau}) + \tilde{\tau}c(g) = c(\tilde{\tau}) + \tau c(g) \in (\tau - 1)W[J].$$

Furthermore, this is true for all $g \in \Gamma$. Taking $g = 1$ we find that

$$c(\tilde{\tau}) \in (\tau - 1)W[J].$$

Thus

$$\tau c(g) \in (\tau - 1)W[J].$$

Since also

$$(\tau - 1)c(g) \in (\tau - 1)W[J],$$

we conclude that

$$c(g) \in (\tau - 1)W[J].$$

Thus the image of c, and therefore the image of φ, lies in $(\tau - 1)W[J]$. Letting $\mathcal{H}$ be the A-submodule of $(\tau - 1)W[J]$ generated by $\varphi(\Gamma)$, the proof continues in the usual way, using the fact that

$$(\tau - 1)W[\mathfrak{m}] \neq W[\mathfrak{m}]$$

to show that $\mathcal{H} = 0$. □

CHAPTER 17

Lecture 17

1. Modular Curves

In this section we summarize the main properties of modular curves which will be of interest to us. We will refer primarily to [**DI**], which provides more extensive references and some proofs. Other standard references are (in rough order of difficulty) [**Se-CA**, Chapter 7], [**Si-2**, Chapter 1], [**La-MF**] and [**Shi**].

1.1. Definitions. Let $\mathfrak{H}$ be the upper half plane in $\mathbb{C}$; that is,

$$\mathfrak{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}.$$

Recall that there is a natural left action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{H}$, given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

(In fact, $-1 \in \mathrm{SL}_2(\mathbb{Z})$ acts trivially, so that this action can be viewed as an action of $\mathrm{PSL}_2(\mathbb{Z})$.)

Fix an integer N and let $\Gamma_0(N)$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \pmod{N} \right\}.$$

Then one can show that the quotient

$$\Gamma_0(N) \backslash \mathfrak{H}$$

has the structure of a Riemann surface. (See [**DI**, Section 7].) In fact, this Riemann surface can be given the structure of a smooth, affine algebraic curve defined over $\mathbb{Q}$, which we denote by $Y_0(N)$. (See [**DI**, Section 8].) Thus

$$Y_0(N)(\mathbb{C}) \cong \Gamma_0(N) \backslash \mathfrak{H}.$$

The projective closure of $Y_0(N)$ is denoted by $X_0(N)$; the complement of $Y_0(N)$ in $X_0(N)$ are called the *cusps*. $X_0(N)$ is a smooth, projective curve defined over $\mathbb{Q}$.

The importance of $X_0(N)$ and $Y_0(N)$ to us comes from the fact that they are a (partial) solution to the problem of classifying *modular pairs* $(E/S, C_N)$, where S is some $\mathbb{Q}$-scheme, E is an elliptic curve over S (that is, E is an abelian scheme over S of dimension 1) and C_N is a finite, flat subgroup scheme of E, all of whose geometric fibers are cyclic groups of order N. (If S is the spectrum of a field K, then this is just a pair of an elliptic curve defined over K and a cyclic subgroup of order N of $E(\bar{K})$. For simplicity we shall always refer to C_N as above as "cyclic subgroups of order N".) More precisely, we define a functor F_N from $\mathbb{Q}$-schemes to sets by sending a $\mathbb{Q}$-scheme S to the set of isomorphism classes of modular pairs

[0]Last modified September 4, 2003

$(E/S, C_N)$. (Two modular pairs $(E/S, C_N)$ and $(E'/S, C'_N)$ are isomorphic if there is an isomorphism (over S) of E and E' taking C_N to C'_N.) This functor is not actually representable, but $Y_0(N)$ is what is called the *representable hull*. This means that if $F_{Y_0(N)}$ is the functor from $\mathbb{Q}$-schemes to sets

$$S \mapsto \mathrm{Hom}_{\mathrm{Spec}\,\mathbb{Q}}(S, Y_0(N)) = Y_0(N)(S),$$

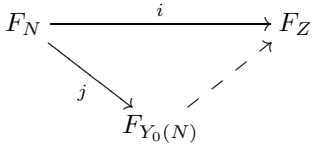
then there is a natural transformation of functors

$$j : F_N \to F_{Y_0(N)}$$

with the following universal property: If Z is any other $\mathbb{Q}$-scheme such that there is a natural transformation

$$i : F_N \to F_Z,$$

where F_Z is the functor sending $\mathbb{Q}$-schemes to $\mathrm{Hom}_{\mathrm{Spec}\,\mathbb{Q}}(S, Z)$, then i factors uniquely through j:



Note that any natural transformation $F_{Y_0(N)} \to F_Z$ must come from some map of schemes

$$Y_0(N) \to Z;$$

specifically, the image of the identity map in $F_{Y_0(N)}(Y_0(N))$ yields an element of $F_Z(Y_0(N)) = \mathrm{Hom}_{\mathrm{Spec}\,\mathbb{Q}}(Y_0(N), Z)$, and one easily checks that this map $Y_0(N) \to Z$ induces the given natural transformation $F_{Y_0(N)} \to F_Z$.

Now, j yields a map j_S from pairs $(E/S, C_N)$ to $Y_0(N)(S)$. In general this map need be neither injective nor surjective. However, if K is an extension of $\mathbb{Q}$ (not necessarily finite), then the map j_K from $(E/K, C_N)$ to $Y_0(N)(K)$ is surjective. If K is algebraically closed, then it is a bijection.

1.2. Modular Curves over $\mathbb{C}$. In order to better illustrate the modular interpretation of $Y_0(N)$, let us return to the case of modular curves over the complex numbers. We assume in this section that the reader is familiar with the theory of elliptic curves over $\mathbb{C}$ as in [**Si-AEC**, Chapter 6].

Recall that an elliptic curve over $\mathbb{C}$ is isomorphic to the quotient of $\mathbb{C}$ by a lattice $\Lambda \subseteq \mathbb{C}$. From this point of view, $Y_0(N)(\mathbb{C})$ classifies isomorphism classes of pairs of lattices $(\Lambda \subseteq \Lambda')$ where Λ'/Λ is cyclic of order N. Specifically, to such a pair we associate the pair

$$(\mathbb{C}/\Lambda, \Lambda'/\Lambda)$$

of an elliptic curve and a subgroup of order N, and two pairs of lattices are isomorphic if the give rise to isomorphic pairs. By [**Si-AEC**, Chapter 6, Corollary 5.1.1] this occurs if and only if the pairs are homothetic.

Let us now consider pairs $(\Lambda \subseteq \Lambda')$ more explicitly. It is not difficult to see that one can choose a $\mathbb{Z}$-basis $\omega_1, \omega_2 \in \mathbb{C}$ of Λ such that

$$\mathrm{Im}(\omega_1/\omega_2) > 0$$

and $\omega_1, \frac{\omega_2}{N}$ is a $\mathbb{Z}$-basis of Λ'. Since lattice pairs are defined only up to homothety, we obtain a map τ from pairs $(\omega_1, \omega_2) \in \mathbb{C} \times \mathbb{C}$ with $\mathrm{Im}(\omega_1/\omega_2) > 0$ to the upper half plane, given by

$$(\omega_1, \omega_2) \mapsto \frac{\omega_1}{\omega_2}.$$

To complete our analysis, we must determine what other pairs (ω_1, ω_2) give rise to the *same* lattice pair

$$(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2, \mathbb{Z}\omega_1 \oplus \mathbb{Z}\frac{\omega_2}{N}).$$

(The map τ already takes care of homothety.) If (ω_1', ω_2') is some other pair (with $\mathrm{Im}(\omega_1'/\omega_2') > 0$ as always), it is a basis for Λ if and only if there is some matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}.$$

(The matrix must be in $\mathrm{SL}_2(\mathbb{Z})$ rather than $\mathrm{GL}_2(\mathbb{Z})$ in order to preserve the upper half-plane condition.) Furthermore, it is easy to see that it gives rise to the same Λ' if and only if

$$c \equiv 0 \pmod{N};$$

that is, if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Thus the set of isomorphism classes of lattice pairs is in bijection with the quotient of the upper half-plane by the action of $\Gamma_0(N)$; that is, they are in bijection with

$$\Gamma_0(N) \backslash \mathfrak{H} \cong Y_0(N)(\mathbb{C}).$$

Since isomorphism classes of lattice pairs correspond to isomorphism classes of modular pairs $(E/\mathbb{C}, C_N)$, this shows that the points of $Y_0(N)(\mathbb{C})$ really do correspond to such pairs, in a canonical way.

One can also give an explicit description of the cusps

$$X_0(N)(\mathbb{C}) - Y_0(N)(\mathbb{C}).$$

To do this, one considers the extended upper half-plane

$$\mathfrak{H}^* = \mathfrak{H} \coprod \mathbb{P}^1(\mathbb{Q}).$$

One defines an action of $\Gamma_0(N)$ on $\mathbb{P}^1(\mathbb{Q})$ in the natural way: thinking of elements of $\mathbb{P}^1(\mathbb{Q})$ as homogeneous pairs $\begin{pmatrix} a \\ b \end{pmatrix}$, the action is just by multiplication on the left; thinking of $\mathbb{P}^1(\mathbb{Q})$ as $\mathbb{Q} \coprod \{\infty\}$ (as we usually will), one has

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d},$$

with the convention that

$$\frac{a\infty + b}{c\infty + d} = \frac{a}{c}.$$

With this action, one has

$$X_0(N)(\mathbb{C}) = \Gamma_0(N) \backslash \mathfrak{H}^*,$$

so that the cusps correspond to the $\Gamma_0(N)$-orbits on $\mathbb{P}^1(\mathbb{Q})$.

In the case that N is prime, one easily checks that there are only two cusps:

$$0 = \left\{ \frac{a}{b} \in \mathbb{Q} \mid b \not\equiv 0 \pmod{N} \right\}$$

$$\infty = \left\{ \frac{a}{b} \in \mathbb{Q} \mid b \equiv 0 \pmod{N} \right\} \coprod \{\infty\}.$$

Any time that we need a base point for $X_0(N)$ (whether N is prime or not) we will use the cusp containing the class of ∞.

1.3. Functions on Modular Curves. We consider briefly here the theory of functions and differential forms on modular forms; this a moderately important area in modern number theory[1], and we give here a complete treatment[2].

Note that for any integer N, the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ lies in $\Gamma_0(N)$. This matrix acts on $\mathfrak{H}$ by

$$\tau \mapsto \tau + 1.$$

Thus any function or differential form on $X_0(N)$, when considered as a $\Gamma_0(N)$-invariant function or differential form on $\mathfrak{H}^*$, can be expanded in terms of the parameter

$$q = e^{2\pi i \tau}.$$

We can therefore expand functions $f : X_0(N)(\mathbb{C}) \to \mathbb{C}$ as Laurent series

$$f(\tau) = \sum_n a_n q^n$$

(these are modular forms of weight 0 and level N) and differential forms $f d\tau$ as

$$f(\tau) d\tau = \sum_n a_n q^n \frac{dq}{q}$$

(these are modular forms of weight 2 and level N).

2. Operators on Modular Curves

2.1. Degeneracy operators. We are going to construct operators on modular curves by defining the operators on the underlying problems which the modular curves "classify". It will be useful to refer to the following formal argument. Let F_1 and F_2 be two functors from $\mathbb{Q}$-schemes to sets which have $\mathbb{Q}$-schemes Y_1 and Y_2 as representable hulls; thus, if F_{Y_1} and F_{Y_2} are the functors represented by Y_1 and Y_2 respectively, we have natural transformations

$$j_1 : F_1 \to F_{Y_1}$$

and

$$j_2 : F_2 \to F_{Y_2}.$$

Suppose that we define a natural transformation

$$i : F_1 \to F_2.$$

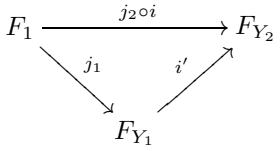
Composition with j_2 yields a natural transformation

$$j_2 \circ i : F_1 \to F_{Y_2},$$

[1] Sarcasm.

[2] Extreme sarcasm.

so since Y_1 is a representable hull for F_1 we obtain a commutative diagram of natural transformations



i' in turn comes from a map

$$Y_1 \to Y_2.$$

Thus any natural transformation of functors yields a canonical map of their representable hulls. If in addition the Y_i are smooth with projective closures X_i, one obtains a map

$$X_1 \to X_2.$$

For any integer N, we let F_N be the functor from $\mathbb{Q}$-schemes to sets associating to a $\mathbb{Q}$-scheme S isomorphism classes of pairs (E, C_N) as in Section 1.1. Thus F_N has $Y_0(N)$ as a representable hull. Also, for simplicity we will only give constructions over fields, or sometimes even only over algebraically closed fields, with references to [**DI**] for the general construction.

Now, let N be an integer dividing another integer M. Let d be an integer dividing the quotient M/N; $d = 1$ is permitted. We will define a map

$$B_d : X_0(M) \to X_0(N)$$

called a *degeneracy operator*. We will do this by defining a natural transformation of the functors F_M and F_N. So let K be a field containing $\mathbb{Q}$ and let $(E/K, C_M)$ be a pair of an elliptic curve defined over K and a cyclic subgroup of order M of $E(\bar{K})$. C_M has a unique subgroup C_d of order d. Furthermore, the cyclic subgroup C_M/C_d of order M/d on the elliptic curve E/C_d has a unique subgroup C_N of order N, since N divides M/d. (See [**Si-AEC**, Chapter 3, Section 4] for basics on quotients of elliptic curves.) We let B_d (as a natural transformation of functors) be the correspondence

$$(E, C_M) \mapsto (E/C_d, C_N).$$

As above, B_d induces a map, which we shall also call B_d, from

$$X_0(M) \to X_0(N).$$

(See [**DI**, Sections 6.3 and 7.3] for the general case.)

In the case $K = \mathbb{C}$, one can ask what effect B_d has on q-expansions. If q_M is the parameter on $X_0(M)$ and q_N is the parameter on $X_0(N)$, it is not difficult to show (from the analysis in Section 1.2) that under B_d, q_N pulls back to q_M^d.

2.2. Atkin-Lehner Involutions. We now define maps from modular curves to themselves. So fix an integer N, and let $N = ab$ be a factorization of N with a and b relatively prime. We will define a map

$$w_a : X_0(N) \to X_0(N)$$

called an *Atkin-Lehner operator*, again by defining a natural transformation from F_N to F_N. (See [**DI**, Section 4 and Remark 8.4.1] for the general case.)

So let K be a field containing $\mathbb{Q}$ and let $(E/K, C_N)$ be a modular pair. The group C_N has a unique decomposition (since a and b are relatively prime)

$$C_N = C_a + C_b$$

as a product of a cyclic group of order a and a cyclic group of order b. Also recall that the full a-torsion $E[a]$ of E is free of rank 2 over $\mathbb{Z}/a\mathbb{Z}$. We define w_a to be the natural transformation

$$(E, C_N) \mapsto (E/C_a, E[a] + C_b/C_a);$$

since $E[a]/C_a$ is cyclic of order N and $C_a \cap C_b = \{1\}$ this makes sense.

We further claim that

$$w_a^2 = 1.$$

To see this, note that

$$w_a^2(E, C_N) = w_a(E/C_a, E[a] + C_b/C_a) = (E/E[a], (E/C_a)[a] + C_b/E[a]).$$

One checks easily that multiplication by a

$$a : E/E[a] \to E$$

yields the desired isomorphism with (E, C_N).

In the case $K = \mathbb{C}$, we can also interpret w_a in terms of an action on the upper half-plane. Going through the analysis in Section 1.2, one finds that there is a commutative diagram

$$\begin{array}{ccc} \mathfrak{H} & \longrightarrow & \mathfrak{H} \\ \downarrow & & \downarrow \\ Y_0(N)(\mathbb{C}) & \xrightarrow{w_n} & Y_0(N)(\mathbb{C}) \end{array}$$

where the vertical maps are the quotient maps and the top horizontal map is

$$\tau \mapsto -\frac{1}{a\tau}.$$

Note that it is completely unclear what the operation on q-expansions is; to determine it, one must find the q-expansion

$$e^{-2\pi i/a\tau},$$

which is rather mysterious.

2.3. Jacobians of Curves. We briefly recall some mapping properties of jacobians of curves. (See Lecture 13, Section 1.1 for the basics on jacobians.) So let X and Y be smooth, proper, irreducible curves over some field K with jacobians J_X and J_Y respectively. Suppose that we have a non-constant map

$$\varphi : X \to Y;$$

thus φ has finite degree. It induces both a covariant map

$$\varphi_* : J_X \to J_Y$$

and a contravariant map

$$\varphi^* : J_Y \to J_X.$$

See [**Si-AEC**, Chapter 2, Section 3] for the corresponding maps on divisors. The composition

$$\varphi_*\varphi^* : J_Y \to J_Y$$

is simply multiplication by the degree of φ.

We will write $J_0(N)$ for the jacobian of the modular curve $X_0(N)$. We fix the embedding

$$X_0(N) \hookrightarrow J_0(N)$$

so that the cusp ∞ of $X_0(N)$ maps to the origin of $J_0(N)$. Thus an arbitrary point $x \in X_0(N)$ maps to the divisor class of

$$(x) - (\infty).$$

2.4. Hecke Correspondences. Fix an integer N and a prime number l not dividing N. We will define a correspondence T_l on $X_0(N)$ called the l^{th} *Hecke correspondence* or the l^{th} *Hecke operator*. For our purposes, a correpondence will simply be a many-valued

$$X_0(N) - - \to X_0(N).$$

Alternately, and somewhat more accurately, a self-correspondence on $X_0(N)$ is a subscheme T_l of the product $X_0(N) \times_{\operatorname{Spec} \mathbb{Q}} X_0(N)$. See [**DI**, Section 3.2] for more details on correspondences, and [**DI**, Section 3 and Section 8.3] for details on Hecke operators.

For our first definition, we work on the level of the functor F_N over an algebraically closed field K. Let (E, C_N) be a modular pair over K. Recall that $E[l] \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$. We consider the subgroups of $E[l]$ of order $l+1$; there are $l+1$ of them and they are naturally classified by $\mathbb{P}^1(\mathbb{F}_l)$. (See [**Se-CA**, Chapter 7, Section 5] for all combinatorial analysis in this section.) We define T_l by sending (E, C_N) to the $l+1$ values

$$(E/C_l, C_l + C_N/C_l),$$

where C_l runs over the subgroups of $E[l]$ of order l.

In the case $K = \mathbb{C}$ we have $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathfrak{H}$ and we can be a bit more explicit. If $\tau \in \Gamma_0(N)\backslash\mathfrak{H}$, $T_l(\tau)$ is the set of values

$$\frac{\tau}{l}, \frac{\tau+1}{l}, \cdots, \frac{\tau+l-1}{l}, l\tau.$$

The advantage of this expression is that the number N does not appear; the Hecke correspondence T_l is thus in some sense the same on all modular curves.

We can also use the above analysis to determine the effect of T_l on q-expansions. We consider the case of a differential form

$$f\frac{dq}{q} = \sum a_n q^n \frac{dq}{q}.$$

The Hecke correspondence is clearly linear, so it will suffice to consider the case of

$$q^n \frac{dq}{q} = e^{2\pi i n\tau} \frac{dq}{q}.$$

Under T_l, this goes to

$$\frac{1}{l}\sum_{j=0}^{l-1} e^{2\pi i n(\tau+j)/l} \frac{dq}{q} + l e^{2\pi i n l\tau} \frac{dq}{q} = \frac{1}{l}\sum_{j=0}^{l-1} e^{2\pi i n j/l} \cdot e^{2\pi i n\tau/l} \frac{dq}{q} + l e^{2\pi i n l\tau} \frac{dq}{q}.$$

But

$$\sum_{j=0}^{l-1} e^{2\pi i n j/l} = \begin{cases} 0 & l \nmid n \\ l & l \mid n, \end{cases}$$

so the above expression reduces to

$$q^{n/l} \frac{dq}{q} + l q^{nl} \frac{dq}{q},$$

where we interpret $q^{n/l}$ as 0 if l does not divide n. In general, then,

$$T_l\left(\sum a_n q^n \frac{dq}{q}\right) = \sum (a_{nl} + l a_{n/l}) q^n \frac{dq}{q},$$

where we set $a_{n/l} = 0$ if l does not divide n.

One can also define T_l in terms of the operator

$$B_1 : X_0(Nl) \to X_0(N)$$

and the Atkin-Lehner involution w_l on $X_0(Nl)$. We write π for B_1 for this section. Consider the (many-valued) composition

$$X_0(N) \xrightarrow{\pi^{-1}} X_0(Nl) \xrightarrow{w_l} X_0(Nl) \xrightarrow{\pi} X_0(N).$$

The first map sends a modular pair (E, C_N) to the set of all pairs $(E, C_N + C_l)$, where C_l is a cyclic subgroup of E of order l. w_l then sends $(E, C_N + C_l)$ to $(E/C_l, E[l] + C_N/C_l)$, which is mapped by π to $(E/C_l, C_l + C_N/C_l)$. Thus this composition is precisely the Hecke correspondence T_l.

This interpretation allows us to interpret T_l as an endomorphism of the Jacobian $J_0(N)$. Specifically, the commutative diagram

$$\begin{array}{ccc} X_0(Nl) & \xrightarrow{w_l} & X_0(Nl) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ X_0(N) & \xrightarrow{T_l} & X_0(N) \end{array}$$

is reinterpreted as a commutative diagram

$$\begin{array}{ccc} J_0(Nl) & \xrightarrow{w_l^*} & J_0(Nl) \\ \uparrow{\scriptstyle \pi^*} & & \downarrow{\scriptstyle \pi_*} \\ J_0(N) & \xrightarrow{T_{l*}} & J_0(N) \end{array}$$

(That is, we take $\pi_* w_{l*} \pi^*$ as the definition of T_{l*}.) We could also define T_l^* by this method, but note that since w_l is an involution we have $w_{l*} = w_l^*$, so

$$T_l^* = \pi_* w_l^* \pi^* = T_{l*}.$$

We will often just write T_l for the map on $J_0(N)$ induced by the Hecke correspondence.

There is also a double coset decomposition definition of Hecke operators, which is quite useful for generalizations. Ask the local Gross student or see [**DI**, Section 3.1].

CHAPTER 18

Lecture 18

1. Representations on Torsion Points

1.1. The Tree of a Modular Pair. For this section fix a modular pair (E, C_N) defined over the complex numbers $\mathbb{C}$. (The precise choice of C_N will only come into play later.) We associate to this pair a graph (actually a building) $\Gamma(E, N)$ in the following way. The vertices of $\Gamma(E, N)$ are in bijection with the cyclic subgroups of $E(\mathbb{C})$ of order relatively prime to N. Two vertices C_1 and C_2 are joined by an edge if one is contained in the other with index some prime l. We will consider this edge to have weight l.

For any prime l not dividing N, we also define a subgraph $\Gamma_l(E)$ consisting of those vertices of $\Gamma(E, N)$ corresponding to cyclic subgroups of l-power order (and all of the edges in $\Gamma(E, N)$ connecting them). $\Gamma_l(E)$ is in fact a tree, as one easily sees.

For any l not dividing N, we define a *Hecke correspondence* T_l on the vertices $\mathrm{vert}(\Gamma(E, N))$ by sending a vertex v to all vertices which are joined to v by an edge of weight l. This induces a homomorphism on divisor groups

$$T_l : \mathbb{Z}[\Gamma(E, N)] \to \mathbb{Z}[\Gamma(E, N)];$$

here by $\mathbb{Z}[\Gamma(E, N)]$ we mean the free abelian group on the vertices of $\Gamma(E, N)$.

Most Hecke correspondences do not restrict to $\Gamma_l(E)$; the only one that does is T_l.

1.2. Galois Actions on $\Gamma(E, N)$. Suppose now that the modular pair (E, C_N) is defined over a subfield K of $\mathbb{C}$. We let $E^{(N)}_{\mathrm{tors}}$ be the subgroup of the torsion points of E of order relatively prime to N. Define $K(E, N)$ to be the splitting field of the natural G_K-action on $E^{(N)}_{\mathrm{tors}}$; equivalently, $K(E, N)$ is generated over K by the coordinates of all of the prime to N torsion points of $E(\mathbb{C})$. If K is a number field, then $K(E, N)$ is certainly an infinite extension of K.

Note that $\mathrm{Aut}(E^{(N)}_{\mathrm{tors}})$ also acts on the graph $\Gamma(E, N)$: if $\varphi \in \mathrm{Aut}(E^{(N)}_{\mathrm{tors}})$ and $v \in \mathrm{vert}(\Gamma(E, N))$ corresponds to the cyclic group $C \subseteq E^{(N)}_{\mathrm{tors}}$, then φv is the vertex corresponding to $\varphi(C)$. One easily checks that this action preserves edges, so that it really is an automorphism of the graph $\Gamma(E, N)$.

[0]Last modified September 4, 2003

FIGURE 1. The Beginning of the Graph Γ for $l = 2$

Now, any choice of isomorphism

$$E_{\mathrm{tors}}^{(N)} \cong \prod_{l \nmid N} \mathbb{Q}_l/\mathbb{Z}_l \times \mathbb{Q}_l/\mathbb{Z}_l$$

yields an isomorphism

$$\mathrm{Aut}(E_{\mathrm{tors}}^{(N)}) \cong \prod_{l \nmid N} \mathrm{GL}_2(\mathbb{Z}_l).$$

Note that the subgroup of scalar matrices is independent of the choice of "basis"of $E_{\mathrm{tors}}^{(N)}$ (it is just those elements of the automorphism group which act on each $E[M]$ as a scalar), and furthermore that it acts trivially on $\Gamma(E,N)$, since any cyclic subgroup is taken to itself by scalars. Thus the map

$$\prod_{l \nmid N} \mathrm{GL}_2(\mathbb{Z}_l) \cong \mathrm{Aut}(E_{\mathrm{tors}}^{(N)}) \to \mathrm{Aut}(\Gamma(E,N))$$

factors through $\prod \mathrm{PGL}_2(\mathbb{Z}_l)$:

$$\begin{array}{ccc} \prod_{l\nmid N} \mathrm{GL}_2(\mathbb{Z}_l) & \longrightarrow & \mathrm{Aut}(\Gamma(E,N)) \\ & \searrow \quad \nearrow & \\ & \prod_{l\nmid N} \mathrm{PGL}_2(\mathbb{Z}_l) & \end{array}$$

Of course, $\mathrm{Gal}(K(E,N)/K)$ acts in a natural way on $E_{\mathrm{tors}}^{(N)}$, yielding a representation

$$\rho_{E,N} : \mathrm{Gal}(K(E,N)/K) \to \mathrm{Aut}(E_{\mathrm{tors}}^{(N)}) \cong \prod_{l \nmid N} \mathrm{GL}_2(\mathbb{Z}_l).$$

The action of $\mathrm{Aut}(E_{\mathrm{tors}}^{(N)})$ on $\Gamma(E,N)$ yields a second representation

$$p\rho_{E,N} : \mathrm{Gal}(K(E,N)/K) \to \mathrm{Aut}(\Gamma(E,N)) \cong \prod_{l \nmid N} \mathrm{PGL}_2(\mathbb{Z}_l);$$

of course, $p\rho_{E,N}$ is just the composition of $\rho_{E,N}$ with the natural quotient map

$$\prod_{l \nmid N} \mathrm{GL}_2(\mathbb{Z}_l) \to \prod_{l \nmid N} \mathrm{PGL}_2(\mathbb{Z}_l).$$

Let us now connect all of this. Let $\Gamma(E,N)$ be the graph associated to a modular pair (E, C_N) defined over a subfield K of $\mathbb{C}$. Then we can define a natural map

$$\mathrm{vert}(\Gamma(E,N)) \to X_0(N)(\mathbb{C})$$

by sending a vertex corresponding to a cyclic group C of order prime to N to the modular pair

$$(E/C, C_N + C/C).$$

In fact, the modular pair is defined over $K(E,N)$, since C is, so the image of the map is contained in $X_0(N)(K(E,N))$. Furthermore, this mapping is compatible with the Hecke correspondences on $\Gamma(E,N)$ and $X_0(N)(\mathbb{C})$, as is clear from the definitions. Composing with the natural map

$$X_0(N)(K(E,N)) \to J_0(N)(K(E,N)),$$

(this map is an embedding if $X_0(N)$ has genus greater than zero, and is trivial if $X_0(N)$ has genus 0) we obtain a Hecke equivariant map

$$\mathrm{vert}(\Gamma(E,N)) \to J_0(N)(K(E,N)).$$

1.3. The Image of $\rho_{E,1}$. We now consider the case $N = 1$ above. Thus we have an elliptic curve E, defined over some field K, and we are considering the respresentation of G_K on E_{tors}, which we will just write as ρ_E. The image of this representation turns out to depend very much on whether or not E has complex multiplication. Recall that E is said to have *complex multiplication* (or CM for short) if $\mathrm{End}_{\mathbb{C}}(E)$ is strictly larger than $\mathbb{Z}$. It follows that $\mathrm{End}_{\mathbb{C}}(E)$ is an order in an imaginary quadratic field. (See [**Si-AEC**, Chapter 6, Theorem 5.5]. For a nice introduction to the theory of complex multiplication, see [**Si-2**, Chapter 2]. Unfortunately, it does not cover complex multiplication in the generality in which we will need it. We will comment more on that later.) In the non-CM case, we have the following theorem of Serre.

THEOREM 1.1 (Serre). *Let K be a number field and let E be an elliptic curve over K without complex multiplication. Then the representation*

$$\rho_E : G_K \to \prod \mathrm{GL}_2(\mathbb{Z}_l) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

has open image. In particular, the image has finite index, and the composition

$$G_K \to \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_l)$$

is surjective for almost all primes l.

PROOF. See [**Se-EC**] or [**La-EF**, Chapter 17]. □

In the CM case, ρ_E is very far from surjective; to see this, note that the image of ρ_E must commute with all elements of $\mathrm{End}_K(E)$. Thus

$$\rho_E(G_K) \subseteq \mathrm{Aut}_{\mathrm{End}_K(E)}(E_{\mathrm{tors}}) \subseteq \mathrm{Aut}(E_{\mathrm{tors}}).$$

If $\mathrm{End}_K(E)$ is larger than $\mathbb{Z}$, then this subgroup is much smaller than the whole of $\mathrm{Aut}(E_{\mathrm{tors}})$. Furthemore, although $\mathrm{End}_K(E)$ need not be larger than $\mathbb{Z}$ even though E has complex multiplication, there exists a finite extension L/K such that $\mathrm{End}_L(E)$ is larger than $\mathbb{Z}$ (see [**Si-2**, Chapter 2, Theorem 2.2]), which is enough to force $\rho_E(\mathrm{GL})$ to be small.

One can actually characterize $\rho_E(G_K)$ fairly precisely in the CM case. Let F be the quadratic imaginary field by which E has complex multiplication, with Galois group $\mathfrak{g} = \mathrm{Gal}(F/\mathbb{Q}) = \{1, \tau\}$. Consider the group

$$(\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*/\mathbb{Z}_l^*;$$

here $\mathcal{O}_F$ is the ring of integers in F, and

$$\mathbb{Z}_l^* \hookrightarrow (\mathcal{O}_F \otimes \mathbb{Z}_l)^*$$

is induced by the natural inclusion

$$\mathbb{Z} \hookrightarrow \mathcal{O}_F.$$

We define $\mathcal{D}_l$ to be the semi-direct product

$$\mathcal{D}_l = \mathfrak{g} \ltimes (\mathcal{O}_F \otimes \mathbb{Z}_l)^*/\mathbb{Z}_l^*,$$

where $\tau \in \mathfrak{g}$ acts on $(\mathcal{O}_F \otimes \mathbb{Z}_l)^*/\mathbb{Z}_l^*$ by inversion.

$\mathcal{D}_l$ can actually be realized as a subgroup of $\mathrm{PGL}_2(\mathbb{Z}_l)$. This is done by first choosing a $\mathbb{Z}$-basis of $\mathcal{O}_F$, which is a free rank 2 $\mathbb{Z}$-module. The action of $(\mathcal{O}_F \otimes \mathbb{Z}_l)^*$ on $\mathcal{O}_F \otimes \mathbb{Z}_l$ now yields an embedding

$$(\mathcal{O}_F \otimes \mathbb{Z}_l)^* \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_l)$$

which in turn yields

$$(\mathcal{O}_F \otimes \mathbb{Z}_l)^*/\mathbb{Z}_l^* \hookrightarrow \mathrm{PGL}_2(\mathbb{Z}_l).$$

Next, one observes that this group is a *Cartan subgroup* of $\mathrm{PGL}_2(\mathbb{Z}_l)$, meaning that it becomes a maximal torus over the algebraic closure. (Recall that a *torus* is a group isomorphic to a product of multiplicative groups.) In this situation, it is a general fact that the group has index 2 in its normalizer, and that non-trivial elements of the normalizer act by inversion. Thus we have realized

$$\mathcal{D}_l \hookrightarrow \mathrm{PGL}_2(\mathbb{Z}_l)$$

as the normalizer of

$$(\mathcal{O}_F \otimes \mathbb{Z}_l)^*/\mathbb{Z}_l^* \hookrightarrow \mathrm{PGL}_2(\mathbb{Z}_l).$$

The relevance of $\mathcal{D}_l$ to us rests on the fact that $\rho_E(G_K)$ is conjugate to a subgroup of $\mathcal{D}_l$.

2. Heegner Points

2.1. Ring class fields. For an excellent introduction to orders and ring class fields and proofs of the results in this section, see [**Cox**, Chapter 2, Sections 7 and 9].

Let F be an imaginary quadratic field. A subring R of the ring of integers $\mathcal{O}_F$ is called an *order* if it is finitely generated and if it generates all of F over $\mathbb{Q}$. It follows easily that R is a lattice in $\mathbb{C}$. One can also show that all orders are of the form

$$\mathcal{O}_{F,n} = \mathbb{Z} + n\mathcal{O}_F$$

for some integer n.

The ideal theory of $\mathcal{O}_{F,n}$ is quite similar to that of $\mathcal{O}_F$; in particular, if $\mathfrak{a}$ is an ideal of $\mathcal{O}_F$ relatively prime to n, then $\mathfrak{a} \cap \mathcal{O}_{F,n}$ is an invertible ideal in $\mathcal{O}_{F,n}$. Furthermore, the ideal class group $\mathrm{Pic}(\mathcal{O}_{F,n})$ of $\mathcal{O}_{F,n}$ (this is not defined exactly as one might expect; see [**Cox**, p. 136]) is an extension of the ideal class group of $\mathcal{O}_F$ by the abelian group

$$(\mathcal{O}_F/n\mathcal{O}_F)^*/(\mathbb{Z}/n\mathbb{Z})^*.$$

Orders have important connections to the class field theory of F. Specifically, for any positive integer n we define the *ring class field* $F^{(n)}$ *of conductor* n to be the unique abelian extension of F, unramified away n, such that a prime $\mathfrak{p}$ of $\mathcal{O}_F$ splits completely in $F^{(n)}$ if and only if $\mathfrak{p}$ is principal with a generator α such that α is congruent to a rational integer modulo n. (That $F^{(n)}$ exists follows from the usual statements of class field theory; see [**Cox**, p. 145 and pp. 179–180].)

Note that $F^{(1)}$ is just the Hilbert class field of F. Furthermore, it follows from the definition that $\mathrm{Gal}(F^{(n)}/F)$ is isomorphic to the ideal class group of $\mathcal{O}_{F,n}$; from this and the computation of the ideal class group of $\mathcal{O}_{F,n}$, we see that

$$\mathrm{Gal}(F^{(n)}/F^{(1)}) \cong (\mathcal{O}_F/n\mathcal{O}_F)^*/(\mathbb{Z}/n\mathbb{Z})^*.$$

$F^{(n)}$ is also Galois over $\mathbb{Q}$; here one finds that

$$\mathrm{Gal}(F^{(n)}/\mathbb{Q}) \cong \mathfrak{g} \rtimes \mathrm{Pic}(\mathcal{O}_{F,n})$$

where $\tau \in \mathfrak{g}$ operates on $\mathrm{Pic}(\mathcal{O}_{F,n})$ in the natural way, which works out to just be by inversion. In fact, $F^{(n)}$ can also be characterized as the maximal generalized dihedral extension of $\mathbb{Q}$ of conductor n; see [**Cox**, Chapter 2, Section 9, Part D].

2.2. Heegner Points. We will now need some of the theory of complex multiplication over non-integrally closed fields. Most of what we need is contained in [**Cox**, Chapter 3, Section 11, esp. Theorem 11.1]; alternately, [**La-EF**] and [**Shi**] have extensive treatments of the theory of complex multiplication.

Let N be a positive integer and let F be a quadratic imaginary field in which every prime dividing N splits completely. (The existence of such an F follows easily from the quadratic reciprocity law.) For simplicity, we assume that F is not $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$; the existence of non-trivial units complicates things somewhat. We also must fix an embedding $F \hookrightarrow \mathbb{C}$. Our hypothesis on F implies that there is an ideal $\mathcal{N}$ of $\mathcal{O}_F$ such that $\mathcal{O}_F/\mathcal{N}$ is cyclic of order N. Fix such an ideal $\mathcal{N}$. We also have that $\mathcal{N}^{-1}/\mathcal{O}_F$ is cyclic of order N.

Now, let n be an integer relatively prime to N. We consider the order $\mathcal{O}_{F,n}$ and the ideal $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_{F,n}$. $\mathcal{N}_n$ is invertible in $\mathcal{O}_{F,n}$ (see the previous section), and we still have that $\mathcal{N}_n^{-1}/\mathcal{O}_{F,n}$ is cyclic of order N.

We associate to each pair $(\mathcal{O}_{F,n}, \mathcal{N}_n^{-1})$ the modular pair

$$(\mathbb{C}/\mathcal{O}_{F,n}, \mathcal{N}_n^{-1}/\mathcal{O}_{F,n})$$

defined over $\mathbb{C}$; note that $\mathcal{O}_{F,n}$ is a lattice, so $\mathbb{C}/\mathcal{O}_{F,n}$ really is an elliptic curve, and that $\mathcal{N}_n^{-1}/\mathcal{O}_{F,n}$ is a cyclic subgroup of order N. This modular pair then defines a *Heegner point*

$$x^{(n)} \in X_0(N)(\mathbb{C}).$$

For our applications, we will need the following theorem, which is essentially [**Cox**, Theorem 11.1].

THEOREM 2.1. *Let n be relatively prime to N. Let E be the elliptic curve over $\mathbb{C}$ defined by $\mathbb{C}/\mathcal{O}_{F,n}$ and let C be the cyclic subgroup of order N of E defined by $\mathcal{N}_n^{-1}/\mathcal{O}_{F,n}$. Then the modular pair (E, C) is defined over the ring class field $F^{(n)}$. In particular,*

$$x^{(n)} \in X_0(N)(F^{(n)}).$$

CHAPTER 19

Lecture 19

1. Hecke Operators on Heegner Points

1.1. Galois Actions on Cyclic Subgroups. Let us review briefly our notation and hypotheses. N is a fixed positive integer and F is a quadratic imaginary extension of $\mathbb{Q}$ in which each prime dividing N splits completely. We further require that F is not $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. We fix an embedding $F \hookrightarrow \mathbb{C}$ and an ideal $\mathcal{N}$ of F such that $\mathcal{O}_F/\mathcal{N}$ is cyclic of order N. For each n relatively prime to N we let $\mathcal{O}_{F,n}$ be the order $\mathbb{Z} + n\mathcal{O}_F$ of conductor n in $\mathcal{O}_F$, and we let $F^{(n)}$ be the ring class field of F of conductor n. Thus

$$\mathrm{Gal}(F^{(n)}/F) \cong \mathrm{Pic}(\mathcal{O}_{F,n})$$

and

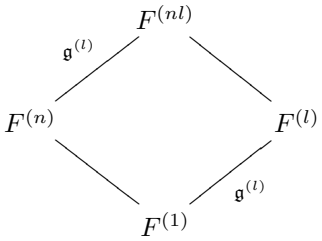
$$\mathrm{Gal}(F^{(n)}/F^{(1)}) \cong (\mathcal{O}_F/n\mathcal{O}_F)^*/(\mathbb{Z}/n\mathbb{Z})^*.$$

We now further assume that $X_0(N)$ has positive genus and we fix an embedding $X_0(N) \hookrightarrow J_0(N)$. $x^{(n)}$ is the point of $X_0(N)$ corresponding to the modular pair $(\mathcal{E}^{(n)}, C_N^{(n)})$, where $\mathcal{E}^{(n)} = \mathbb{C}/\mathcal{O}_{F,n}$, $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_{F,n}$ and $C_N^{(n)} = \mathcal{N}_n^{-1}/\mathcal{O}_{F,n}$. $x^{(n)}$ actually lies in $X_0(N)(F^{(n)})$, and we will also regard it as an element of $J_0(N)(F^{(n)})$ via our fixed embedding.

Fix a prime l not dividing N. We claim that for any n relatively prime to lN,

$$\mathrm{Gal}(F^{(nl)}/F^{(n)}) = \mathrm{Gal}(F^{(l)}/F^{(1)}).$$

This follows from the fact that $F^{(n)} \cap F^{(l)} = F^{(1)}$, which is true since the two fields have relatively prime conductor (in the sense of class field theory; see [**Cox**, Exercise 9.20]). We denote this Galois group by $\mathfrak{g}^{(l)}$.



Fix such an n. As we have said, the elliptic curve $\mathcal{E}^{(n)}$ has a model over $F^{(n)}$; in fact, it is defined over an index 2 subfield of $F^{(n)}$ (see [**Shi**, Theorem 5.7]) and thus the model over $\mathcal{E}^{(n)}$ is only well-defined up to twisting by a quadratic character. In any event, fixing such a model yields a Galois representation

$$G_{F^{(n)}} \to \mathrm{Aut}(\mathcal{E}^{(n)}[l]).$$

[0]Last modified September 4, 2003

The image of $G_{F^{(n)}}$ must commute with the endomorphisms of $\mathcal{E}^{(n)}$ defined over $F^{(n)}$, which is all of $\mathcal{O}_{F,n}$ (see [**Si-2**, Theorem 2.2.6]). Thus the image of the Galois representation actually lies in

$$\mathrm{Aut}_{\mathcal{O}_{F,n}/l\mathcal{O}_{F,n}}(\mathcal{E}^{(n)}[l]).$$

$\mathcal{E}^{(n)}[l]$ is free of rank 1 over $\mathcal{O}_{F,n}/l\mathcal{O}_{F,n} \cong \mathcal{O}_F/l\mathcal{O}_F$, so we have a Galois representation

$$G_{F^{(n)}} \to \mathrm{Aut}_{\mathcal{O}_{F,n}/l\mathcal{O}_{F,n}} \cong (\mathcal{O}_{F,n}/l\mathcal{O}_{F,n})^* \cong (\mathcal{O}_F/l\mathcal{O}_F)^*.$$

We are actually only interested in the action of $G_{F^{(n)}}$ on the cyclic subgroups of $\mathcal{E}^{(n)}$ of order l, so we need only consider the induced map

$$G_{F^{(n)}} \to (\mathcal{O}_F/l\mathcal{O}_F)^*/\mathbb{F}_l^*$$

since scalars act trivially on the set of cyclic subgroups. This map is surjective and factors through $\mathrm{Gal}(F^{(nl)}/F^{(n)})$ ([**Shi**, Theorem 5.7]), yielding a map

$$\mathfrak{g}^{(l)} \to (\mathcal{O}_F/l\mathcal{O}_F)^*/\mathbb{F}_l^*$$

which is now an isomorphism, since each group has the same order.

Let us now assume that l is inert in $F/\mathbb{Q}$. Then $\mathcal{O}_F/l\mathcal{O}_F \cong \mathbb{F}_{l^2}$. Now, $\mathcal{E}^{(n)}[l]$ is an $\mathbb{F}_{l^2}$ vector space of dimension 1, and thus an $\mathbb{F}_l$ vector space of dimension 2. One thus sees immediately that $\mathbb{F}_{l^2}^*/\mathbb{F}_l^*$ acts simply transitively on the collection $\mathbb{P}_{\mathbb{F}_l}(\mathcal{E}^{(n)}[l])$ of one dimensional $\mathbb{F}_l$ subspaces of $\mathcal{E}^{(n)}[l]$, which are precisely the cyclic subgroups of $\mathcal{E}^{(n)}$ of order l. Combining all of this, we have seen that $\mathfrak{g}^{(l)}$ acts simply transitively on the collection of cyclic subgroups of $\mathcal{E}^{(n)}$ of order l.

In order to restate our above analysis in a more useful way we first must define a trace map

$$\mathrm{Tr}_{(nl,n)} : J_0(N)(F^{(nl)}) \to J_0(N)(F^{(n)}).$$

This is nothing more than the natural map

$$x \mapsto \sum_{\sigma \in \mathfrak{g}^{(l)}} \sigma x.$$

Proposition 1.1. *With the above notation and hypothesis (in particular, l is inert in $F/\mathbb{Q}$), we have*

$$T_l x^{(n)} = \mathrm{Tr}_{(nl,n)}\, x^{(nl)},$$

where T_l is the usual Hecke operator on $J_0(N)$.

Proof. By definition,

$$T_l x^{(n)} = \sum_{C_l \subseteq \mathcal{E}^{(n)}[l]} (\mathcal{E}^{(n)}/C_l, C_N^{(n)} + C_l/C_l),$$

where the sum is over all cyclic subgroups of $\mathcal{E}^{(n)}$ of order l. On the other hand,

$$\begin{aligned}
\mathrm{Tr}_{(nl,n)}\, x^{(nl)} &= \sum_{\sigma \in \mathfrak{g}^{(l)}} \sigma x^{(nl)} \\
&= \sum_{\sigma \in \mathfrak{g}^{(l)}} \sigma(\mathcal{E}^{(nl)}, C_N^{(nl)}) \\
&= \sum_{\sigma \in \mathfrak{g}^{(l)}} \sigma(\mathbb{C}/\mathcal{O}_{F,nl}, \mathcal{N}_{nl}^{-1}/\mathcal{O}_{F,nl})
\end{aligned}$$

Note that

$$(\mathbb{C}/\mathcal{O}_{F,nl}, \mathcal{N}_{nl}^{-1}/\mathcal{O}_{F,nl}) = ((\mathbb{C}/\mathcal{O}_{F,n})/C_l, (\mathcal{N}_n^{-1}/\mathcal{O}_{F,n})/C_l)$$

for some unique cyclic group of order l $C_l \in \mathcal{E}^{(n)}$, since $\mathcal{O}_{F,n}/\mathcal{O}_{F,nl}$ is cyclic of order l. Furthermore, by definition

$$\sigma((\mathbb{C}/\mathcal{O}_{F,n})/C_l, (\mathcal{N}_n^{-1}/\mathcal{O}_{F,n})/C_l) = (\mathbb{C}/\mathcal{O}_{F,n})/\sigma C_l, (\mathcal{N}_n^{-1}/\mathcal{O}_{F,n})/\sigma C_l);$$

combined with the two expressions above and the transitivity of the action of $\mathfrak{g}^{(l)}$ on the cyclic subgroups of $\mathcal{E}^{(n)}$ of order l, this proves the proposition. □

Although we will not use it, we sketch the corresponding result in the case that l splits in $F/\mathbb{Q}$. Let λ and $\bar{\lambda}$ be the primes of F lying over l. In this case,

$$\mathfrak{g}^{(l)} = \mathbb{F}_l^* \times \mathbb{F}_l^*/\mathbb{F}_l^*,$$

the last $\mathbb{F}_l^*$ being the diagonal copy of $\mathbb{F}_l^*$. So $\mathfrak{g}^{(l)}$ is cyclic of order $l-1$, and it acts on the $\mathbb{P}_{\mathbb{F}_l}(\mathcal{E}^{(n)}[l])$ of cyclic subgroups of order l in $\mathcal{E}^{(n)}$. Of course, $\mathfrak{g}^{(l)}$ can not act on this projective space principally homogeneously. In fact, it fixes the two distinguished subgroups $\mathcal{E}^{(n)}[\lambda]$ and $\mathcal{E}^{(n)}[\lambda']$, and then acts principally homogeneously on $\mathbb{P}_{\mathbb{F}_l}(\mathcal{E}^{(n)}[l]) - \{\mathcal{E}^{(n)}[\lambda], \mathcal{E}^{(n)}[\lambda']\}$. In this case, then, the formula of Proposition 1.1 must be modified slightly. Specifically, if one denotes by σ_λ and $\sigma_{\bar{\lambda}}$ the elements of $\mathrm{Gal}(F^{(n)}/F)$ produced by $\lambda \cap \mathcal{O}_{F,n}$ and $\bar{\lambda} \cap \mathcal{O}_{F,n}$ under the isomorphism

$$\mathrm{Pic}(\mathcal{O}_{F,n}) \cong \mathrm{Gal}(F^{(n)}/F),$$

then one has the formula

$$\begin{aligned} \mathrm{Tr}_{(nl,n)}\, x^{(nl)} &= (T_l - \sigma_\lambda - \sigma_{\bar{\lambda}})x^{(n)} \\ &= (T_l - \sigma_\lambda - \sigma_\lambda^{-1})x^{(n)}. \end{aligned}$$

With a little care, then, one can derive the general formula

$$\mathrm{Tr}_{(nl,n)}\big(-\sigma_\lambda x^{(nl)} + \sigma_\lambda^2 x^{(n)}\big) = \big(1 - T_l\sigma_\lambda + l\sigma_\lambda^2\big)x^{(n)}$$

of Mazur and Rubin, which works independently of the behaivor of l in $F/\mathbb{Q}$.

1.2. Hecke Algebras. We will now relate all of our data to our earlier notation. For simplicity we now require that N is squarefree. Let $\mathbb{T} \subset \mathrm{End}_{\mathbb{Q}}(J_0(N))$ be the subalgebra generated by 1, T_l for l prime not dividing N, and U_q for q dividing N. $\mathbb{T}$ is a commutative, finite, free $\mathbb{Z}$-algebra. (See [**DI**, Sections 3.3-3.4].)

Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ such that $\mathbb{T}/\mathfrak{m}$ has characteristic $p \neq 2$. Let B be the abelian variety $J_0(N)$, and let

$$W = \bigcup_r B(\overline{\mathbb{Q}})[\mathfrak{m}^r]$$

be the $\mathfrak{m}$-divisible subgroup of $B(\overline{\mathbb{Q}})$. W is of course also p-divisible. Both $\mathbb{T}$ and $G_{\mathbb{Q}}$ act on W, and the actions commute since $\mathbb{T}$ is defined over $\mathbb{Q}$.

W is actually a module over

$$\mathbb{T}_{\mathfrak{m}} = \varprojlim\ \mathbb{T}/\mathfrak{m}^r.$$

We will write A for this ring; it satisfies all of our usual hypotheses. Let H be the Cartier dual of W; it is a free A module of finite rank. We have a Galois representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}_A(H)$$

and a residual representation

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{Aut}_k(H \otimes_A k),$$

where $k = \mathbb{T}/\mathfrak{m} = \mathbb{T}_{\mathfrak{m}}/\mathfrak{m}\mathbb{T}_{\mathfrak{m}}$.

We make two hypothesis on the maximal ideal $\mathfrak{m}$. First, we assume that H is free of rank 2 over $\mathbb{T}_{\mathfrak{m}}$. Second, we assume that

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$$

is surjective. We call any maximal ideal with these properties *good*. We will see later that these hypotheses imply all of the hypotheses of Kolyvagin's theorem.

We also assume that there is an $\eta \in \mathbb{T}$ such that $\eta\mathbb{T} \in \mathfrak{m}$, $\eta : B \to B$ is an isogeny and

$$\mathbb{Z} \cap \eta\mathbb{T} = p^s\mathbb{Z}$$

for some $s \geq 1$. We will say that a prime l (inert in $F/\mathbb{Q}$ and not dividing N) is *good* for η if

$$T_l \in \eta A$$

and

$$l + 1 \in \eta A.$$

Note that in particular this implies that p^s divides $l + 1$, and thus that p^s divides the order of $\mathfrak{g}^{(l)}$.

1.3. Computations. We continue with the above notation, and we suppose that we have a good maximal ideal $\mathfrak{m}$, an η as above, and a prime l which is good for η. We define

$$P^{(l)} = \sum_{g \in \mathfrak{g}^{(l)}} gx^{(l)} \otimes g \in B(F^{(l)}) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathfrak{g}^{(l)}].$$

Let $P_\eta^{(l)}$ be the "reduction of $P^{(l)}$ modulo η"; that is, $P_\eta^{(l)}$ is the image of $P^{(l)}$ in

$$\mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathfrak{g}^{(l)}].$$

Note that

$$\mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)})$$

is killed by p^s since $\mathbb{T}/\eta$ is, so

$$\mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathfrak{g}^{(l)}] = \mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z}[\mathfrak{g}^{(l)}].$$

Next, let $I^{(l)}$ be the augmentation ideal of $\mathbb{Z}/p^s\mathbb{Z}[\mathfrak{g}^{(l)}]$, so that there is an exact sequence

$$0 \to I^{(l)} \to \mathbb{Z}/p^s\mathbb{Z}[\mathfrak{g}^{(l)}] \to \mathbb{Z}/p^s\mathbb{Z} \to 0,$$

the last map being given by evaluating each $g \in \mathfrak{g}^{(l)}$ at 1. Each of these groups is free over $\mathbb{Z}/p^s\mathbb{Z}$, so the exact sequence splits over $\mathbb{Z}/p^s\mathbb{Z}$. In particular, the sequence

$$\begin{aligned} 0 \longrightarrow \quad & \mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} I^{(l)} \longrightarrow \mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z}[\mathfrak{g}^{(l)}] \\ \longrightarrow \ & \mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z} \longrightarrow 0 \end{aligned}$$

is still exact.

We claim that

$$P_\eta^{(l)} \in \mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} I^{(l)}.$$

To prove this, it suffices to show that $P_\eta^{(l)}$ is in the kernel of the summation map

$$\mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z}[\mathfrak{g}^{(l)}] \to \mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z}.$$

Equivalently, we must show that the image of $P^{(l)}$ under

$$B(F^{(l)}) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathfrak{g}^{(l)}] \to B(F^{(l)}) \otimes_{\mathbb{Z}} \mathbb{Z} = B(F^{(l)})$$

is contained in $\eta B(F^{(l)})$. This image is

$$\begin{aligned}\sum_{g\in\mathfrak{g}^{(l)}} gx^{(l)} \otimes 1 &= \sum_{g\in\mathfrak{g}^{(l)}} gx^{(l)} \\ &= \mathrm{Tr}_{(l,1)}\, x^{(l)} \\ &= T_l x^{(l)}\end{aligned}$$

by Proposition 1.1. But by hypothesis,

$$T_l \in \eta\mathbb{T},$$

so this establishes the claim.

Next, let $\mathcal{P}_\eta^{(l)}$ be the image of $P_\eta^{(l)}$ in

$$\mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} I^{(l)}/(I^{(l)})^2.$$

Note that the map

$$\mathfrak{g}^{(l)} \to I^{(l)}$$

sending g to $g-1$ induces an isomorphism

$$\mathfrak{g}^{(l)} \otimes_{\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z} \to I^{(l)}/(I^{(l)})^2.$$

Thus we can (and do) regard $\mathcal{P}_\eta^{(l)}$ as an element of

$$\mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} \left(\mathfrak{g}^{(l)} \otimes_{\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z}\right).$$

Note also that $\mathfrak{g}^{(l)} \otimes \mathbb{Z}/p^s\mathbb{Z}$ is cyclic of order p^s, so

$$\mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}) \otimes_{\mathbb{Z}/p^s\mathbb{Z}} \left(\mathfrak{g}^{(l)} \otimes_{\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z}\right) \cong \mathbb{T}/\eta \otimes_{\mathbb{T}} B(F^{(l)}),$$

at least as abelian groups.

We claim that $\mathcal{P}_\eta^{(l)}$ is fixed under the action of $\mathfrak{g}^{(l)}$ on the $B(F^{(l)})$ coordinate. To see this, we compute for $\sigma \in \mathfrak{g}^{(l)}$

$$\begin{aligned}\sigma P^{(l)} - P^{(l)} &= \sum_{g\in\mathfrak{g}^{(l)}} \sigma g x^{(l)} \otimes g - \sum_{g\in\mathfrak{g}^{(l)}} gx^{(l)} \otimes g \\ &= \sum_{g\in\mathfrak{g}^{(l)}} gx^{(l)} \otimes g\sigma^{-1} - \sum_{g\in\mathfrak{g}^{(l)}} gx^{(l)} \otimes g \\ &= \sum_{g\in\mathfrak{g}^{(l)}} gx^{(l)} \otimes g(\sigma^{-1}-1)\end{aligned}$$

CHAPTER 20

Lecture 20

1. The Euler System for $X_0(11)$

1.1. The Set-Up. For simplicity we now restrict our investigations to the case $N = 11$; it is in many ways typical of the general case, and it will help to cut down on the notation. Recall that $X_0(11)$ is a curve of genus 1 with good reduction away from 11, and we make it into an elliptic curve by using the cusp at infinity as the base point. This yields a canonical isomorphism

$$X_0(11) \cong J_0(11),$$

and we will also use B to denote this elliptic curve.

$X_0(11)$ can actually be realized by the Weierstrass equation

$$y^2 + y = x^3 - x^2 - 10x - 20,$$

and the group $B(\mathbb{Q})$ of rational points is cyclic of order 5. The standard everywhere regular differential on $X_0(11)$ has a Fourier expansion

$$\begin{aligned}\omega(q) &= \eta(q)^2\eta(11q)^2 \\ &= q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 \\ &= \sum_{n=1}^{\infty} a_n q^n \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + \cdots .\end{aligned}$$

The image $\mathbb{T}$ of the Hecke algebra in $\mathrm{End}_{\mathbb{Q}}(J_0(11)) = \mathbb{Z}$ is just $\mathbb{Z}$, and the Hecke operator T_l (for $l \neq 11$) on $J_0(11)$ can be identified with its eigenvalue a_l. For $l = 11$, U_{11} is identified with $a_{11} = 1$. The Atkin-Lehner involution w_{11} is the negative of this, and thus is the involution -1.

For every p, we obtain a Galois representation

$$\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{Aut}(B[p]) \cong \mathrm{GL}_2(\mathbb{F}_p).$$

$\overline{\rho}_p$ is surjective for all $p \neq 2, 5, 11$. For $p = 5$ this lack of surjectivity is forced by the fact that B has a rational point of order 5; the image of $\overline{\rho}_5$ in $\mathrm{GL}_2(\mathbb{F}_5)$ is simply the subgroup of diagonal matrices with 1 in the upper left coordinate.

We let F be any quadratic imaginary field $\mathbb{Q}(\sqrt{-d})$ in which 11 is inert; by quadratic reciprocity, this condition says precisely that

$$d \equiv -1, 2, -3, -4, -5 \pmod{11}.$$

[0]Last modified September 4, 2003

(Note that this automatically eliminates the fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$.) We also fix a factorization $11 = \mathcal{N} \cdot \bar{\mathcal{N}}$ in $\mathcal{O}_F$.

Now fix a prime $p \neq 2, 3, 5, 11$. Our maximal ideal $\mathfrak{m}$ is just (p), and it is easily seen to be good. Our element η is a power p^s of p, and a prime l, inert in $F/\mathbb{Q}$, is good for η if and only if

$$l + 1 \equiv a_l \equiv 0 \pmod{p^s}.$$

Fix such an l.

For later use, we define the *basic Heegner point* $P \in B(F)$ by

$$P = \mathrm{Tr}_{F^1/F}\, x^1.$$

1.2. The Construction. We now briefly review our construction of Lecture 19 in this simplified notation. We begin with a point

$$P^{(l)} = \sum_{g \in \mathfrak{g}^{(l)}} g x^{(l)} \otimes g \in B(F^{(l)}) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathfrak{g}^{(l)}].$$

We now "reduce $P^{(l)}$ modulo p^s"; that is, we take $P_\eta^{(l)}$ to be image of $P^{(l)}$ in

$$B(F^{(l)}) \otimes_{\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z}[\mathfrak{g}^{(l)}].$$

As discussed in Lecture 19, Section 1.3, $P_\eta^{(l)}$ actually lies in the submodule

$$B(F^{(l)}) \otimes_{\mathbb{Z}} I^{(l)}.$$

We define $\mathcal{P}_\eta^{(l)}$ to be the image of $P_\eta^{(l)}$ in

$$B(F^{(l)}) \otimes_{\mathbb{Z}} I^{(l)}/(I^{(l)})^2 \cong B(F^{(l)}) \otimes_{\mathbb{Z}} (\mathfrak{g}^{(l)} \otimes_{\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z}).$$

We also fix an isomorphism

$$\mathfrak{g}^{(l)} \otimes_{\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z} \cong \mathbb{Z}/p^s\mathbb{Z};$$

this allows us to consider $\mathcal{P}_\eta^{(l)}$ as an element of

$$B(F^{(l)}) \otimes_{\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z} = B(F^{(l)})/p^s B(F^{(l)}).$$

Letting $\mathfrak{g}^{(l)}$ act on $B(F^{(l)})/p^s B(F^{(l)})$ in the natural way, we have as before

$$\mathcal{P}_\eta^{(l)} \in \left(B(F^{(l)})/p^s B(F^{(l)})\right)^{\mathfrak{g}^{(l)}}.$$

We now relate $\mathcal{P}_\eta^{(l)}$ to Galois cohomology and in particular to our abelian variety finite/singular structure on $B[p^s]$. We begin with the exact sequence

$$0 \to B[p^s] \to B \xrightarrow{p^s} B \to 0.$$

Taking the long exact sequence for $G_{F^{(1)}}$ and $G_{F^{(l)}}$ cohomology yields a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B(F^{(1)})/p^s B(F^{(1)}) & \longrightarrow & H^1(G_{F^{(1)}}, B[p^s]) & \longrightarrow & H^1(G_{F^{(1)}}, B)[p^s] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & B(F^{(l)})/p^s B(F^{(l)}) & \longrightarrow & H^1(G_{F^{(l)}}, B[p^s]) & \longrightarrow & H^1(G_{F^{(l)}}, B)[p^s] & \longrightarrow & 0
\end{array}$$

Note that the two horizontal sequences are simply our finite/singular sequences for the Galois module $B[p^s]$ over $F^{(1)}$ and $F^{(l)}$ respectively. In particular, we have an identification

$$H^1(G_{F^{(1)}}, B)[p^s] = H^1_s(G_{F^{(1)}}, B[p^s]).$$

In fact, the vertical maps all have image in the $\mathfrak{g}^{(l)}$-invariant subgroups, yielding a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B(F^{(1)})/p^sB(F^{(1)}) & \longrightarrow & H^1(G_{F^{(1)}}, B[p^s]) & \longrightarrow & H^1(G_{F^{(1)}}, B)[p^s] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & (B(F^{(l)})/p^sB(F^{(l)}))^{\mathfrak{g}^{(l)}} & \longrightarrow & H^1(G_{F^{(l)}}, B[p^s])^{\mathfrak{g}^{(l)}} & \longrightarrow & H^1(G_{F^{(l)}}, B)[p^s]^{\mathfrak{g}^{(l)}} & & \end{array}$$

Consider the map

$$\varphi : H^1(G_{F^{(1)}}, B[p^s]) \to H^1(G_{F^{(l)}}, B[p^s])^{\mathfrak{g}^{(l)}}.$$

By the inflation-restriction sequence, this has kernel $H^1(\mathfrak{g}^{(l)}, B(F^{(l)})[p^s])$ and cokernel $H^2(\mathfrak{g}^{(l)}, B(F^{(l)})[p^s])$. However, we must have $B(F^{(l)})[p^s] = 0$, since if B had rational p^s-torsion in a dihedral extension of $\mathbb{Q}$, the image of the representation $\overline{\rho}_p$ would factor through this dihedral group and an abelian subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, and thus be solvable. Since $\mathrm{GL}_2(\mathbb{F}_p)$ is not solvable for $p \neq 2, 3$, our assumptions imply that this is not possible. In particular, this implies that φ is an isomorphism. The same is not true of ψ, but at the very least we can identify its kernel as $H^1(\mathfrak{g}^{(l)}, B(F^{(l)}))[p^s]$.

Let us now push our element $\mathcal{P}_\eta^{(l)}$ of $(B(F^{(l)})/p^sB(F^{(l)}))^{\mathfrak{g}^{(l)}}$ around the diagram. It yields an element of of $H^1(G_{F^{(l)}}, B[p^s])^{\mathfrak{g}^{(l)}}$, and thus via φ^{-1} an element of $H^1(G_{F^{(1)}}, B[p^s])$. Pushing this forward we obtain an element

$$c_\eta^{(l)} \in H^1(G_{F^{(1)}}, B)[p^s]$$

which maps to 0 under ψ, and thus also an element

$$d_\eta^{(l)} \in H^1(\mathfrak{g}^{(l)}, B(F^{(l)}))[p^s].$$

We are now in a position to define our long awaited Kolyvagin-Flach system. We define

$$\kappa_\eta^{(l)} \in H^1_s(G_F, B[p^s])$$

to be the image of $c_\eta^{(l)}$ under the corestriction map

$$\mathrm{cor} : H^1_s(G_{F^{(1)}}, B[p^s]) \to H^1_s(G_F, B[p^s]).$$

We will now summarize the main remaining results; proofs will be given (hopefully) in later lectures.

THEOREM 1.1. *Let ε be the eigenvalue $-a_{11}$ of W_{11}. Then $\kappa_\eta^{(l)}$ is in the $-\varepsilon$ eigenspace of $H^1_s(G_F, B[p^s])$.*

Recall that P is the basic Heegner point and lies in $B(F)$. We let F_l be the completion of F at l; since l is inert this makes sense. We also restrict now to the case $\eta = p$.

THEOREM 1.2. *If $P \in pB(F_l)$, then $\mathrm{Supp}\,\kappa_\eta^{(l)}$ is empty. If $P \notin pB(F_l)$, then $\mathrm{Supp}\,\kappa_\eta^{(l)} = \{l\}$ and the depth of $\kappa_\eta^{(l)}$ is 1.*

COROLLARY 1.3. *Let* $F = \mathbb{Q}(\sqrt{-d})$ *where* $d \equiv -1, 2, -3, -4, -5 \pmod{11}$. *Let* p *be a prime distinct from* $2, 3, 5, 11$. *Then if* P *is not divisible by* p *in* $J_0(11)(F)$, *we have*

$$Ш(J_0(11)/\mathbb{Q}) = 0.$$

COROLLARY 1.4. *If there exists a field* F *as above for which* P *is of infinite order, then the* p*-primary component of* $Ш(J_0(11)/\mathbb{Q})$ *vanishes for almost all* p.

CHAPTER 21

Lecture 21

1. Local Behavior of Cohomology Classes

1.1. $X_0(11)$ over Finite Fields. We continue with the analysis of the classes

$$c_\eta^{(l)} \in H^1(G_{F^{(1)}}, B)[p]$$

$$d_\eta^{(l)} \in H^1(\mathfrak{g}^{(l)}, B(F^{(l)}))[p]$$

$$\kappa_\eta^{(l)} \in H^1_s(G_F, B[p])$$

for the modular curve $B = X_0(11) = J_0(11)$. We begin by considering the action of Fr_l on $B[p]$. (Here by Fr_l we mean the Frobenius of l in the extension of F generated by the coordinates of $B[p]$. This makes sense since B has good reduction at l and $l \neq p$.) Fr_l has characteristic polynomial $x^2 - a_l x + l$ on the two-dimensional $\mathbb{F}_p$-vector space $B[p]$; since l is good for p, we have

$$x^2 - a_l x + l \equiv x^2 - 1 \pmod{p}.$$

In particular, we see immediately that Fr_l is a non-scalar involution on $B[p]$. (It is non-scalar since it has distinct eigenvalues.)

Next consider the points of B over the residue fields k_0 and k of $\mathbb{Q}_l$ and F_l respectively; of course, $k_0 = \mathbb{F}_l$ and $k = \mathbb{F}_{l^2}$ since l is inert in $F/\mathbb{Q}$. It is a standard fact that

$$|B(k_0)| = 1 + l - a_l$$

and

$$|B(k)| = (1 + l)^2 - a_l^2.$$

In particular, since l is good for p we see that $B(k_0)$ has a point of order p, and all of $B[p]$ is contained in $B(k)$. Note that $B(k_0)$ does not contain all of $B[p]$, since Fr_l projects to the non-trivial element of $\mathrm{Gal}(k/k_0)$ and acts as a non-scalar, and thus in particular is non-trivial.

If we consider the eigenspaces of $B(k)$ under the action of Fr_l (or equivalently under the action of the non-trivial element of $\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(k/k_0)$), we obtain a decomposition

$$\begin{aligned} B(k)_p &= B(k)_p^+ \oplus B(k)_p^- \\ &= B(k_0)_p \oplus B(k)_p^- \end{aligned}$$

where $B(k)_p$ is the p-primary component of $B(k)$; we do not actually obtain such a decomposition of all of $B(k)$ because of problems with 2. In any event, we do find that

$$B(k)[p] = B(k_0)[p] \oplus B(k)[p]^-$$

[0]Last modified September 4, 2003

and our above analysis shows that both direct summands are cyclic of order p. This implies that $B(k_0)_p$ and $B(k)_p^-$ are themselves cyclic, and combining all of this yields the following lemma.

LEMMA 1.1. *$B(k)_p^+ = B(k_0)_p$ is cyclic of order*

$$p^{\mathrm{ord}_p(1+l-a_l)}$$

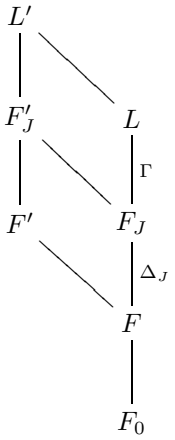
and $B(k)_p^-$ is cyclic of order

$$p^{\mathrm{ord}_p(1+l+a_l)}.$$

1.2. The Kolyvagin-Flach Theorem. Recall that our eventual goal is to prove Lecture 20, Theorem 1.2 and to derive Lecture 20, Corollary 1.3 from it. For the moment let us discuss this second issue. The difficulty is that Theorem 1.2 only yields Kolyvagin-Flach classes for primes l such that the basic Heegner point P is not a p^{th}-power in $B(F_l)$. Using the notation from earlier in the course, our Kolyvagin-Flach theorems to this point have required that we have such classes for all $l \in \mathcal{L}_\tau$, where $\mathcal{L}_\tau$ is the set of places of F for which there exists a place w of F_J over v such that $\mathrm{Fr}_{F_J/F}(w)$ is the fixed non-scalar involution $\tau \in \mathrm{Gal}(F_J/\mathbb{Q})$. In our case we can identify $\mathcal{L}_\tau$ with the set of l which are good for p. (This essentially comes from the fact that for any $l \neq p$, the action of Fr_l on $B[p]$ has characteristic polynomial $x^2 - a_l x + l$; which ones yield non-scalar involutions is then clear.) We, however, only have Kolyvagin-Flach classes for the subset $\mathcal{L}'_\tau$ of $\mathcal{L}_\tau$ for which P is not a p^{th}-power locally.

Let us define this set $\mathcal{L}'_\tau$ purely field theoretically. Let F' be a (probably non-Galois) extension of F generated by some p^{th} root of P. Then $\mathcal{L}'_\tau$ is precisely the set of place of F which are good for p and which have no degree 1 places of F' over them. (The existence of such a place means exactly that P is a p^{th}-power over the completion of F.)

We will sketch the proof of the Kolyvagin-Flach theorem in this new situation. Abstractly, we add a new field F'/F and we define $F'_J = F'F_J$ and $L' = F'L$. (Again we are using our earlier notation.) We make the hypothesis that $F_J \neq F'_J$.



We claim that in this situation it is enough to have a Kolyvagin-Flach system for $\mathcal{L}'_\tau$ (as defined above). Specifically, we want to show that if $\varphi(\mathrm{Fr}_w) = 0$ for some w dividing each $v \in \mathcal{L}'_\tau$, then $\varphi = 0$. To see this, we first lift $\tilde{\tau}$ to an element

$\tilde{\tau}' \in \mathrm{Gal}(L'/F_0)$. We now consider $\varphi((g'\tilde{\tau}')^2)$ only for those $g' \in \mathrm{Gal}(L'/F_J) - \mathrm{Gal}(L'/F'_J)$. The exact same proof works for these g' to show that

$$\varphi(\mathrm{Gal}(L'/F_J) - \mathrm{Gal}(L'/F'_J)) = 0.$$

But this implies that φ vanishes on all of $\mathrm{Gal}(L'/F_J)$, since we already know that it vanishes on the group minus a proper subgroup (since we assumed $F'_J \neq F_J$) and φ is a homomorphism. This completes the proof of the Kolyvagin-Flach theorem in this restricted situation.

1.3. Finiteness of the Kolyvagin-Flach Classes. The first step in proving Theorem 1.2 is the following lemma. For the remainder of the lecture we assume that $F^{(1)} = F$, for purely notational reasons; the general proofs are the same except that we can avoid a few corestrictions.

LEMMA 1.2. *If $v \neq l$, then $\mathrm{res}_v(\kappa_\eta^{(l)}) \in H^1_s(G_v, B[p])$ is trivial.*

PROOF. Recall that we had a class $d_\eta^{(l)} \in H^1(\mathfrak{g}^{(l)}, B(F^{(l)}))$ which mapped to $\kappa_\eta^{(l)} = c_\eta^{(l)} \in H^1_s(G_F, B[p])$. The commutative diagram

$$\begin{array}{ccc} H^1(\mathfrak{g}^{(l)}, B(F^{(l)})) & \longrightarrow & H^1(D_w, B(F^{(l)})) \\ \downarrow & & \downarrow \\ H^1(G_F, B) & \longrightarrow & H^1(G_v, B) \end{array}$$

where w is a place of $F^{(l)}$ lying over v and D_w is the decomposition group of w in $\mathfrak{g}^{(l)}$, shows that it will suffice to show that $\mathrm{res}_w(d_\eta^{(l)}) = 0$. We will do this by showing that all of $H^1(D_w, B(F^{(l)}))$ vanishes.

More generally, let Φ/Φ_0 be an unramified, Galois extension of local fields. (In the case above we take $\Phi = F_w^{(l)}$ and $\Phi_0 = F_v$.) Let B be an abelian variety over Φ_0 with good reduction over $\mathcal{O}_{\Phi_0}$. We claim that

$$H^1(\mathrm{Gal}(\Phi/\Phi_0), B(\Phi)) = 0.$$

This is essentially a consequence of Lang's theorem; we begin by noting that by properness

$$B(\Phi) = B(\mathcal{O}_\Phi) = \varprojlim B(\mathcal{O}_\Phi/\mathfrak{m}^n)$$

where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}_\Phi$. Thus we must show that

$$H^1(\mathrm{Gal}(\Phi/\Phi_0), B(\mathcal{O}_\Phi/\mathfrak{m}^n)) = 0$$

for all n. For $n = 1$ this is precisely Lang's theorem; for $n > 1$, one uses the Greenberg functor to express $B(\mathcal{O}_\Phi/\mathfrak{m}^n)$ as the k-valued points of an n-dimensional smooth, connected algebraic group. Lang's theorem again completes the proof.

The above argument works for $v \neq 11, l$. For $v = 11$, B has bad reduction, so one must use the Neron model of B and a more refined analysis in order to apply Lang's theorem. The key is that the Neron model is just the product of the multiplicative group and a cyclic group of order 5; since 5 is prime to 11, this group does not enter in to the calculations, and Lang's theorem applies directly to $\mathbb{G}_\mathrm{m}$; we omit the details. □

1.4. Singular Depth of the Kolyvagin-Flach Classes. We next must compute the singular depth of $\kappa_\eta^{(l)}$ at $v = l$. Recall the defining diagram

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & H^1(\mathfrak{g}^{(l)}, B(F^{(l)}))[p] & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & B(F)/pB(F) & \longrightarrow & H^1(G_F, B[p]) & \longrightarrow & H^1(G_F, B)[p] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} & & \\
0 & \longrightarrow & (B(F^{(l)})/pB(F^{(l)}))^{\mathfrak{g}^{(l)}} & \longrightarrow & H^1(G_{F^{(l)}}, B[p])^{\mathfrak{g}^{(l)}} & \longrightarrow & H^1(G_{F^{(l)}}, B)[p]^{\mathfrak{g}^{(l)}} & &
\end{array}$$

(Recall that we are assuming $F^{(1)} = F$.) We have

$$d_\eta^{(l)} \in H^1(\mathfrak{g}^{(l)}, B(F^{(l)}))[p]$$

and

$$\kappa_\eta^{(l)} = c_\eta^{(l)} \in H^1(G_F, B)[p] = H^1_s(G_F, B[p]).$$

Let $\tilde{d}_\eta^{(l)}$ be the image of $d_\eta^{(l)}$ under the map

$$H^1(\mathfrak{g}^{(l)}, B(F^{(l)})) \to H^1(\mathfrak{g}^{(l)}, B(F_l^{(l)})).$$

(Note that $F^{(l)}/F$ is totally ramified at F, so $\mathfrak{g}^{(l)}$ is the decomposition group of l.)

The residue field of $F_{0,l}$ is $k_0 = \mathbb{F}_l$, while those of F_l and $F_l^{(l)}$ are $k = \mathbb{F}_{l^2}$. Consider the map

$$B(F_l^{(l)}) \to B(k).$$

The kernel is pro-l, so, since $\tilde{d}_\eta^{(l)}$ maps to an element of order p in the cohomology, we find that $\tilde{d}_\eta^{(l)} = 0$ if and only if $\tilde{\tilde{d}}_\eta^{(l)} = 0$, where $\tilde{\tilde{d}}_\eta^{(l)}$ is the image of $\tilde{d}_\eta^{(l)}$ under

$$H^1(\mathfrak{g}^{(l)}, B(F_l^{(l)})) \to H^1(\mathfrak{g}^{(l)}, B(k)).$$

Since $\mathfrak{g}^{(l)}$ acts trivially on k, we have that

$$H^1(\mathfrak{g}^{(l)}, B(k)) = \mathrm{Hom}(\mathfrak{g}^{(l)}, B(k)).$$

Now, however, our earlier notational simplifications come back to haunt us. Really we must consider

$$\mathrm{Hom}(\mathfrak{g}^{(l)}, B(k)) \otimes I^{(l)}/(I^{(l)})^2 = \mathrm{Hom}(\mathfrak{g}^{(l)}, B(k) \otimes I^{(l)}/(I^{(l)})^2)$$

and ask what

$$\tilde{\tilde{d}}_\eta^{(l)} : \mathfrak{g}^{(l)} \to B(k) \otimes I^{(l)}/(I^{(l)})^2$$

is.

LEMMA 1.3. *For all $g \in \mathfrak{g}^{(l)}$,*

$$\tilde{\tilde{d}}_\eta^{(l)}(g) = \pm \left(\frac{(l+1)\,\mathrm{Fr}_l - a_l}{p} \right) P \otimes (1 - g).$$

CHAPTER 22

Lecture 22

1. Completion of the Proofs

1.1. Bounding of the Shafarevich-Tate Group. We continue with the notation of the previous lectures. We assume the following lemmas for this section; we will prove Lemma 1.1 later in the lecture. (Recall that the cohomology class $\tilde{\tilde{d}}_\eta^{(l)}$ lies in $H^1(\mathfrak{g}^{(l)}, B(k))$, where k is the residue field of $F_l^{(1)}$ (and of $F_l^{(l)}$ and F).

LEMMA 1.1. *For all $g \in \mathfrak{g}^{(l)}$,*

$$\tilde{\tilde{d}}_\eta^{(l)}(g) = \pm \left(\frac{(l+1)\,\mathrm{Fr}_l - a_l}{p} \right) P \otimes (1-g).$$

LEMMA 1.2.

$$\kappa_\eta^{(l)} \in H^1_s(G_F, B[p])^+.$$

We now prove the main theorem of the course. Recall that $P \in B(F)$ is the basic Heegner point.

THEOREM 1.3. *If $P \in pB(F_l)$, then $\operatorname{Supp} \kappa_\eta^{(l)} = \emptyset$. If $P \notin pB(F_l)$, then $\operatorname{Supp} \kappa_\eta^{(l)} = \{l\}$, and $\kappa_\eta^{(l)}$ has singular depth 1 at l.*

PROOF. Recall from Lecture 21 that we had reduced this to determining the behavior of any representative crossed homomorphism of

$$\tilde{\tilde{d}}_\eta^{(l)} \in H^1(\mathfrak{g}^{(l)}, B(k)).$$

In fact, since $\mathfrak{g}^{(l)}$ acts trivially on $B(k)$, the homomorphism

$$\tilde{\tilde{d}}_\eta^{(l)} : \mathfrak{g}^{(l)} \to B(k)$$

is well-defined, and we must determine when it vanishes.

This can be done easily from Lemma 1.1 and Lemma 1.1 of Lecture 21. Specifically, Fr_l acts on P by -1, so

$$\tilde{\tilde{d}}_\eta^{(l)}(g) = \pm \left(\frac{l+1+a_l}{p} \right) P \otimes 1 - g.$$

But since $P \in B(k)_p^-$ and $B(k)_p^-$ is cyclic of order $p^{\mathrm{ord}_p(l+1+a_l)}$, $\tilde{\tilde{d}}_\eta^{(l)}$ vanishes if and only if $\tilde{P}$ is divisible by p in $B(k)_p^-$. Our analysis at the end of Lecture 21 shows that this happens if and only if $\tilde{P}$ is divisible by p in $B(F_l^{(1)})$, which completes the proof. □

[0]Last modified September 4, 2003

COROLLARY 1.4. *If P is of infinite order in $B(F)$, then*

$$Ш(J_0(11)/\mathbb{Q})_p = 0$$

for all but finitely many p.

PROOF. If P is of infinite order in $B(F)$, then P lies in $pB(F)$ for only finitely many p. For any p outside of this set and distinct from 2, 5 and 11, Theorem 1.3 and our Kolyagin-Flach theorems apply to yield the vanishing of $Ш(J_0(11)/\mathbb{Q})_p$. □

In fact, P is of infinite order and is a generator of $B(F)$, as can be shown by various (non-elementary) methods. In particular, this means that Corollary 1.4 applies for all $p \neq 2, 5, 11$. A more refined analysis can show that $Ш(J_0(11)/\mathbb{Q})_p = 0$ for these p as well, so that

$$Ш(J_0(11)/\mathbb{Q}) = 0.$$

1.2. Explicit Determination of Cocycles 1. In preparation for the proof of Lemma 3 we consider the following situation: let H be a subgroup of a group G with quotient $G/H = \Gamma$. Let M be a G-module such that $M^H = 0$. Then the inflation-restriction sequence yields an isomorphism

$$H^1(G, M) \xrightarrow{\cong} H^1(H, M)^\Gamma.$$

We wish to give an explicit inverse map, on the level of cocycles.

So let $c : H \to M$ be a crossed homomorphism representing a class in $H^1(H, M)$. Suppose further that the cohomology class of c is invariant under the action of G, which can be given explicitly by

$$c^g(h) = g^{-1}c(ghg^{-1}).$$

Thus for each $g \in G$, there is an element $b(g) \in M$ such that

$$(c^g - c)(h) = (h - 1)b(g)$$

for all $h \in H$. In fact, $b(g)$ is unique since $M^H = 0$. We now define a cocycle

$$C : G \to M$$

by $C(g) = b(g^{-1})$. It is not difficult to check that $C(g)$ is a crossed homomorphism and its class in $H^1(G, M)$ is independent of the choice of crossed homomorphism c. Furthermore, C restricts to c on H, so that C is the desired extension of c.

1.3. Explicit Determination of Cocycles 2. We abstract the situation of Lemma 1.1 somewhat before giving the proof. Let p be a fixed prime number and let B be an abelian variety defined over a number field K. Let L/K be a finite extension such that $B(L)$ has no non-trivial p-torsion. Set $G = G_K$, $H = G_L$ and $\Gamma = G/H$. Suppose that we are given $Q \in B(L)$ such that the image of Q lies in $(B(L)/pB(L))^\Gamma$. We wish to determine a crossed homomorphism

$$\kappa_Q : \Gamma \to B(L)$$

to which Q maps in the following commutative diagram.

$$\begin{array}{ccccccc} & & & & & & 0 \\ & & & & & & \downarrow \\ & & & & & & H^1(\Gamma, B(L)) \\ & & & & & & \downarrow \\ & & & & H^1(G, B[p]) & \longrightarrow & H^1(G, B) \\ & & & & \downarrow & & \downarrow \\ 0 & \longrightarrow & (B(L)/pB(L))^\Gamma & \longrightarrow & H^1(H, B[p])^\Gamma & \longrightarrow & H^1(H, B) \end{array}$$

Now, since Q is Γ-invariant in $B(L)/pB(L)$, for every $\gamma \in \Gamma$ there exists $R(\gamma) \in B(L)$ such that

$$\gamma Q - Q = pR(\gamma).$$

Furthermore, $R(\gamma)$ is unique, since $B(L)$ has no p-torsion. We claim that the crossed homomorphism

$$\gamma \mapsto -R(\gamma)$$

represents the class κ_Q in $H^1(\Gamma, B(L))$ corresponding to Q.

To see this, recall first that the Kummer map

$$B(L)/pB(L) \to H^1(H, B[p])$$

sends Q to the cocycle

$$h \mapsto (h-1)S \in B[p]$$

where $S \in B(\overline{\mathbb{Q}})$ is such that $pS = Q$. The analysis of the previous section tells us how to pull this cocycle back to $H^1(G, B[p])$; in our new notation, we find the cocycle

$$g \mapsto (g-1)S - R(g).$$

This maps next to $H^1(G, B)$. Here, however, $(g-1)S$ is trivial, so we are left with the cocycle

$$g \mapsto -R(g).$$

This restricts to

$$\gamma \mapsto -R(\gamma)$$

in $H^1(\Gamma, B(L))$, as claimed.

1.4. Proof of Lemma 1.1. Let us now apply the above analysis to the specific situation of Lemma 1.1. We have a diagram

$$\begin{array}{ccccc} & & & & 0 \\ & & & & \downarrow \\ & & & & H^1(\mathfrak{g}^{(l)}, B(F^{(l)})) \longrightarrow H^1(\mathfrak{g}^{(l)}, B(k)) \\ & & & & \downarrow \\ & & H^1(F^{(1)}, B[p]) & \longrightarrow & H^1(F^{(1)}, B) \\ & & \downarrow & & \\ 0 & (B(F^{(l)})/pB(F^{(l)}))^{\mathfrak{g}^{(l)}} & \longrightarrow & H^1(F^{(l)}, B[p])^{\mathfrak{g}^{(l)}} & \end{array}$$

(which one should really view as tensored with $I^{(l)}/(I^{(l)})^2$) and we wish to determine the cocycle of

$$H^1(\mathfrak{g}^{(l)}, B(k))$$

corresponding to

$$P_\eta^{(l)} = \sum_{\gamma \in \mathfrak{g}^{(l)}} \gamma x^{(l)} \otimes \gamma \in (B(F^{(l)})/pB(F^{(l)}))^{\mathfrak{g}^{(l)}} \otimes I^{(l)}/(I^{(l)})^2.$$

Note that since

$$\sum_{\gamma \in \mathfrak{g}^{(l)}} \gamma x^{(l)} \otimes 1 \in (B(F^{(l)})/pB(F^{(l)}))^{\mathfrak{g}^{(l)}} \otimes (I^{(l)})^2,$$

we can rewrite $P_\eta^{(l)}$ as

$$P_\eta^{(l)} = \sum_{\gamma \in \mathfrak{g}^{(l)}} \gamma x^{(l)} \otimes (\gamma - 1).$$

Let us begin by rewriting $P_\eta^{(l)}$. We fix a generator γ_0 of $\mathfrak{g}^{(l)}$. We write any $\gamma \in \mathfrak{g}^{(l)}$ as $\gamma_0^{\log \gamma}$, where $0 \leq \log \gamma < l + 1 = |\mathfrak{g}^{(l)}|$. Then an easy calculation shows that

$$\gamma - 1 = (\gamma_0 - 1) \sum_{j=0}^{\log \gamma - 1} (\gamma_0^j - 1)$$

in the group ring $\mathbb{Z}[\mathfrak{g}^{(l)}]$. Furthermore, since $\gamma_0 - 1 \in I^{(l)}$, one easily computes from this that

$$\gamma - 1 \equiv \log \gamma (\gamma_0 - 1) \pmod{(I^{(l)})^2}.$$

Thus we can rewrite $P_\eta^{(l)}$ as

$$P_\eta^{(l)} = \sum_{\gamma \in \mathfrak{g}^{(l)}} \log \gamma \cdot \gamma x^{(l)} \otimes (\gamma_0 - 1).$$

Now, note that in $\mathbb{Z}[\mathfrak{g}^{(l)}]$, we have the identity

$$(\gamma_0 - 1) \sum_{\gamma \in \mathfrak{g}^{(l)}} \log \gamma \cdot \gamma = l + 1 - \sum_{\gamma \in \mathfrak{g}^{(l)}} \gamma.$$

We now compute

$$(\gamma_0 - 1)P_\eta^{(l)} = \left((\gamma_0 - 1) \sum_{\gamma \in \mathfrak{g}^{(l)}} \log \gamma \cdot \gamma \right) x^{(l)} \otimes (\gamma_0 - 1)$$
$$= \left(1 + l - \sum_{\gamma \in \mathfrak{g}^{(l)}} \gamma \right) x^{(l)} \otimes (\gamma_0 - 1).$$

Our expression for $\gamma - 1$ in terms of $\gamma_0 - 1$ shows that this extends to

$$(\gamma - 1)P_\eta^{(l)} = \left(1 + l - \sum_{\gamma \in \mathfrak{g}^{(l)}} \gamma \right) x^{(l)} \otimes (\gamma - 1)$$

for all $\gamma \in \mathfrak{g}^{(l)}$.

We can use this expression to determine $R(\gamma)$, using the notation of the previous section. Using the fact that l is good for p and that

$$\sum_{\gamma \in \mathfrak{g}^{(l)}} \gamma x^{(l)} = a_l x^{(1)},$$

we find that

$$R(\gamma) = \left(\frac{1+l}{p} x^{(l)} - \frac{a_l}{p} x^{(1)} \right) \otimes (\gamma - 1).$$

The analysis of the previous section shows that the cocycle

$$d_\eta^{(l)} \in H^1(\mathfrak{g}^{(l)}, B(F^{(l)}))$$

is given by

$$d_\eta^{(l)}(\gamma) = -R(\gamma).$$

To complete the proof of Lemma 1.1 we must consider this formula over the residue field k. Here we have the reductions $\tilde{x}^{(l)}$ and $\tilde{x}^{(1)}$ in $B(k)$, since k is the residue field of both $F_l^{(l)}$ and $F_l^{(1)}$. The following lemma, which comes from a careful analysis of complex multiplication over finite fields, completes the proof of Lemma 1.1.

LEMMA 1.5.

$$\tilde{x}^{(l)} = \mathrm{Fr}\, \tilde{x}^{(1)}$$

where Fr *is the generator of* $\mathrm{Gal}(k/\mathbb{F}_l)$.

Bibliography

[AW] Micahel Atiyah and C.T.C. Wall, *Cohomology of groups* in *Algebraic number fields*, Ian Cassels and A. Frohlich (ed.), pp. 94–115.

[BFH] D. Bump, S. Friedberg and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, *Inventiones mathematicae*, vol. 102 (1990), pp. 543–618.

[Car] Roger Carter, *Finite groups of Lie type*, John Wiley and Sons, New York, 1985.

[Cas] Ian Cassels, *Global fields* in *Algebraic number fields*, Ian Cassels and A. Frohlich (ed.), pp. 42–84.

[CF] Ian Cassels and A. Frohlich (ed.), *Algebraic number fields*, Academic Press, London, 1967.

[Co] Brian Conrad, personal correspondence, March 4, 1998.

[Co2] Brian Conrad, personal correspondence, March 5, 1998.

[CS] Gary Cornell and Joseph Silverman (ed.), *Arithmetic geometry*, Springer-Verlag, New York, 1986.

[CSS] Gary Cornell, Joseph Silverman and Glenn Stevens (ed.), *Modular forms and Fermat's last theorem*, Springer-Verlag, New York, 1997.

[Cox] David Cox, *Primes of the form* $x^2 + ny^2$, John Wiley and Sons, New York, 1989.

[DI] Fred Diamond and John Im, *Modular forms and modular curves* in *Seminar on Fermat's last theorem*, V. Kumar Murty (ed.), pp. 39–113.

[FD] Benson Farb and R. Keith Dennis, *Noncommutative algebra*, Springer-Verlag, New York, 1993.

[Fr] A. Frohlich, *Local fields* in *Algebraic number fields*, Ian Cassels and A. Frohlich (ed.), pp. 1–41.

[GZ] Benedict Gross and Donald Zagier, *Heegner points and derivatives of L-series*, *Inventiones mathematicae*, vol. 84 (1986), pp. 225–320.

[Ha] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977.

[Ko] Victor Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E/\mathbb{Q})$ *for a class of Weil curves*, *Math. of the USSR Izvestiya*, vol. 32 (1989), pp. 523–542.

[La-Al] Serge Lang, *Algebra*, Addison-Wesley.

[La-ANT] Serge Lang, *Algebraic number theory*, Springer-Verlag, New York, 1986.

[La-EF] Serge Lang, *Elliptic functions*, Springer-Verlag, New York, 1987.

[La-MF] Serge Lang, *Introduction to modular forms*, Springer-Verlag, Heidelberg, Germany, 1995.

[Ma] Hideyuki Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986.

[Maz] Barry Mazur, *An introduction to the deformation theory of Galois representations* in *Modular forms and Fermat's last theorem*, Gary Cornell, Joseph Silverman and Glenn Stevens (ed.), pp. 243-311.

[Mi-AV] J.S. Milne, *Abelian Varieties* in *Arithmetic Geometry*, Gary Cornell and Joseph Silverman (ed.), pp. 103–150.

[Mi-ADT] J.S. Milne, *Arithmetic duality theorems*, Academic Press, Boston, 1986.

[Mi-EC] J.S. Milne, *Étale cohomology*, Princeton University Press, Princeton, New Jersey, 1980.

[Mi-JV] J.S. Milne, *Jacobian varieties* in *Arithmetic Geometry*, Gary Cornell and Joseph Silverman (ed.), pp. 167–212.

[Mu] David Mumford, *Abelian Varieties*, Oxford University Press, Oxford, 1970.

[MM] M.R. Murty and V.K. Murty, *Mean values of derivatives of modular L-series*, *Annals of Mathematics*, vol. 133 (1991), pp. 447–475.

[Mur] V. Kumar Murty (ed), *Seminar on Fermat's last theorem*, American Mathematical Society Press, Providence, 1995.

[PR] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Academic Press, Boston, 1994.

[Pi] Richard Pierce, *Associative algebras*, Springer-Verlag, New York, 1982.

[Roh] David Rohrlich.

[Ro] Michael Rosen, *Abelian varieties over* $\mathbb{C}$ in *Arithmetic Geometry*, Gary Cornell and Joseph Silverman (ed.), pp. 79–101.

[Ru-TS] Karl Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, *Inventiones mathematicae*, vol. 89 (1987), pp. 527–560.

[Ru-ES] Karl Rubin, *Euler systems and Iwasawa theory.*

[Se-CA] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973.

[Se-GC] Jean-Pierre Serre, *Galois cohomology*, Springer-Verlag, New York, 1997.

[Se-LF] Jean-Pierre Serre, *Local fields*, Springer-Verlag, New York, 1979.

[Se-EC] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, *Inventiones mathematicae*, vol. 15 (1972), pp. 259–331.

[ST] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, *Annals of Mathematics*, vol. 68 (1968), pp. 492–517.

[Sh] Stephen Shatz, *Group schemes, formal groups and p-divisible groups* in *Arithmetic geometry*, Gary Cornell and Joseph Silverman (ed.), pp. 29–78.

[Shi] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, New Jersey, 1971.

[Si-AEC] Joseph Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[Si-H] Joseph Silverman, *The theory of height functions* in *Arithmetic geometry*, Gary Cornell and Joseph Silverman (ed.), pp. 151–166.

[Si-2] Joseph Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1993.

[Ta] John Tate, *Global class field theory* in *Algebraic number fields*, J.W.S Cassels and A. Frohlich (ed.), pp. 162–203.

[Ti] Jacques Tilouine, *Hecke algebras and the Gorenstein property* in *Modular forms and Fermat's last theorem*, Gary Cornell, Joseph Silverman and Glenn Stevens (ed.), pp. 327–342.

[Wei] Charles Weibel, *An introduction to homological algebra*, Cambridge University Press, Cambridge, 1994.

[Wes-Ide] Tom Weston, *The idelic approach to number theory.*

[Wes-IR] Tom Weston, *The inflation-restriction sequence: an introduction to spectral sequences.*