Galois Representations

Joel Bellaiche, Math 203b (Spring 2009)

Contents

1 Introduction

1.1 Overview

Three fields of study that are now thought to be related in quite fundamental ways are algebraic number theory, representations of real and p-adic Lie groups, and algebraic geometry over number fields (note here that algebraic geometry over $\mathbb{C}$ looks like algebraic geometry over number fields since any [finite] collection of equations has a finite number of coefficients so lives in some finite extension of $\mathbb{Q}$).

In particular, the topics of Galois representations (which are finite dimensional representations of Galois groups of number fields), automorphic forms, and motives are thought to have strong relationships with one onother.

A motive defines Galois representations through étale cohomology, and this is expected to be "bijective" in the sense that these representations should capture all of the interesting information about the motive (Tate, Mazur).

The correspondence between Galois representations and automorphic forms is the subject of the Langlands program.

The correspondence between motives and automorphic forms is due to Langlands and Mazur.

The work remaining to flesh out and understand these correspondences is huge - more than 50-100 years of work.

We will not discuss automorphic forms or motives much in this class, concentrating instead on Galois representations. Galois representations are fundamental objects in algebraic number theory itself; many of the interesting statement in ANT can be reformulated in terms of Galois representations.

1.2 Galois groups of algebraic closures

We start by recalling the analysis of Galois groups of number fields, local field (the completions of number fields), and finite fields (the residue fields).

Definition 1. Let K be a field. Its algebraic closure $\bar{K}$ is unique up to K-isomorphism, so we may define

$$G_K \cong \mathrm{Gal}(\bar{K}/K)$$

Note that if $\bar{K}, \bar{K}'$ are two algebraic closures, and $\sigma : \bar{K} \to \bar{K}'$ a K-isomorphism between them, this gives an isomorphism

$$\mathrm{Gal}(\bar{K}/K) \cong \mathrm{Gal}(\bar{K}'/K) : \tau \mapsto \sigma\tau\sigma^{-1}$$

This is not a canonical isomorphism, so that G_K is only defined up to conjugacy class [in the group of isomorphisms of algebraic closures of K].

Definition 2. The *Krull topology* on G_K is defined by letting the system of neighborhoods around 1 be given by $\{\mathrm{Gal}(\bar{K}/L)\}$ as L runs over all finite extensions of K in $\bar{K}$ (for a fixed algebraic closure). By translation, we define the system of neighborhoods around an arbitrary $g \in G_K$.

This topology makes G_K into a topological group. Composition and inverse are clearly continuous since any two elements belong to some $\mathrm{Gal}(\bar{K}/L)$ and they are continuous within that group.

If we give $\mathrm{Gal}(L/K)$ the discrete topology, then

$$G_K = \varprojlim_{L \text{ finite Galois}/K} \mathrm{Gal}(L/K)$$

where L is inside some fixed algebraic closure is a topological isomorphism[1]. Since each $\mathrm{Gal}(L/K)$ is compact and totally disconnected (it is discrete), so is G_K; thus G_K is a profinite group. Note that the Krull topology on G_K is the same as the profinite topology. An open subgroup of G_K is of the form $\mathrm{Gal}(\bar{K}/L)$ for L finite over K; a closed subgroup of G_K is $\mathrm{Gal}(\bar{K}/L)$ where L/K is not necessarily finite. (Recall that every open subgroup is also closed).

First assume $K = \mathbb{F}_q$ is a finite field. Then any finite extension L/K is Galois and isomorphic to $\mathbb{F}_{q^n}$ with Galois group $\mathbb{Z}/n\mathbb{Z}$. There is a canonical isomorphism

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(L/K) : 1 \mapsto \mathrm{Frob}$$

where $\mathrm{Frob}(x) = x^q$. Then

$$G_K = \varprojlim \mathrm{Gal}(L/K) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \prod_{l \text{ prime}} \mathbb{Z}_l =_{df} \hat{\mathbb{Z}}$$

Also, $\langle \mathrm{Frob} \rangle$ is dense in $\hat{\mathbb{Z}}$.

Next, recall that local fields consist of $\mathbb{R}, \mathbb{C}$, finite extensions of $\mathbb{Q}_p$, and finite extensions of $\mathbb{F}_p((T))$. We will be working in characteristic zero only, so we will consider only the first three. Clearly $G_{\mathbb{C}} = \{1\}$ and $G_{\mathbb{R}} = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$, where σ is complex conjugation.

If $K/\mathbb{Q}_p$ is finite with ring of integers $\mathcal{O}_K$ (recall that the ring of integers can be defined as the valuation ring of the valuation on K), then $\mathcal{O}_K$ is a DVR with unique maximal ideal $\mathfrak{m}_K$ and finite residue field $F_K = \mathcal{O}_K/\mathfrak{m}_K$. In addition, if L/K is finite, it too is a local ring with ring of algebraic integers $\mathcal{O}_L$ and maximal ideal $\mathfrak{m}_L$. We then have that

$$\mathfrak{m}_K \mathcal{O}_L = \mathfrak{m}_L^e, \quad e \geq 1$$

e is the *ramification index* of L/K; if $e = 1$ we say that L is *unramified* over K.

In general, there exists a maximal unramified extension L^{nr} of K inside of L; if L/K is Galois, so is L^{nr}, so there is an exact sequence

$$1 \to I_L \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L^{\mathrm{nr}}/K) \to 1$$

I_L is called the *inertia group of* L/K. Note that $\mathrm{Gal}(L^{\mathrm{nr}}/K) \cong \mathrm{Gal}(F_{L^{\mathrm{nr}}}/F_K)$; since it is true that there is a Galois extension of each degree, upon taking limits, we get

$$1 \to I \to G_K \to \mathrm{Gal}(\bar{K}^{\mathrm{nr}}/K) = G_{F_K} \cong \hat{Z} \to 1$$

The structure of G_K is fairly well-known in this case. Serre (Local Fields) proves that G_K is solvable; it is also known that G_K is topologically finitely generated (i.e. there is a finite family that generates a dense subgroup).

Finally, suppose K is a number field. Recall that a *place* of K is an equivalence class of nontrivial absolute values $|\cdot|$ on K. The places of K are either *finite*, corresponding to the prime ideals of K, or infinite, corresponding to embeddings $K \hookrightarrow \mathbb{C}$ modulo complex conjugation. A valuation

[1] To see this, use the universal property of inverse limits. Suppose A is a topological group with compatible maps $A \to \mathrm{Gal}(L/K)$ for L/K finite Galois. Then each element of A acts on every such L/K. But every element of $\bar{K}$ is in some finite extension, so we know how a acts on it. This gives the required map $A \to G_K$.

corresponding to a finite place $\mathfrak{p}$ is $2^{-v_{\mathfrak{p}}(\cdot)}$; a valuation corresponding to an infinite place σ is simply $|\sigma(\cdot)|_{\mathbb{C}}$.

Now if v is a place, and K_v the completion of K for an absolute value of v, then K is a local field - $\mathbb{R}$ or $\mathbb{C}$ if v is infinite, and a finite extension of $\mathbb{Q}_p$ is v is finite.

If L/K is finite, and v a place of K, then there are a finite number of places w of L extending v (written $w \mid v$), and in fact

$$L \otimes_K K_v = \prod_{w|v} L_w$$

If L/K is Galois, the Galois group acts transitively on the places of L extending v; we define

$$D_w = \{g \in \mathrm{Gal}(L/K) \ \mid \ gw = w\}$$

called the *decomposition group* of w; $D_w = \mathrm{Gal}(L_w/K_v)$ (see, e.g. notes from 203a). If $w, w' \mid v$ then D_w and $D_{w'}$ are conjugate subgroups of $\mathrm{Gal}(L/K)$.

Fix a place v of K. For each L algebraic over K, choose a compatible sequence of $w \mid v$ (note that any finite extension of K_v is L_w for some w), use the injection $D_w \hookrightarrow \mathrm{Gal}(L/K)$ and take limits to get

$$i_v : G_{K_v} \hookrightarrow G_K$$

This map is not well-defined since we chose particular w's, but it is well-defined up to conjugacy. If v is a finite place, we get an exact sequence

$$0 \to I_v \to G_{K_v} \to \langle \mathrm{Frob}_v \rangle \to 0$$

by taking the limit of the exact sequences associated with the decomposition groups.

We can study G_K by studying the representations of G_K and how they restrict to G_{K_v}.

Definition 3. Let K be a number field, S a finite set of finite places of K. Then $G_{K,S}$ is the quotient of G_K by the smallest closed normal subgroup of G_K containing all inertia groups I_v for v finite, $v \notin S$. Note that normality of the subgroup both ensures that the quotient is a group and makes irrelevant the fact that the map $G_{K,v} \to G_K$ is only defined up to conjugacy class.

An alternative definition for $G_{K,S}$ is that it is the Galois group of the maximal extension of K unramified outside of S, written $K^{\mathrm{nr},S}$.

Not much is known about the groups $G_{K,S}$. For example, it is conjectured that $G_{K,S}$ is topologically of finite type[2].

If v is a finite place of K, then we have a composite map

$$\iota_v : G_{K_v} \xrightarrow{i_v} G_K \twoheadrightarrow G_{K,S}$$

Clearly for $v \notin S$, we have $\iota_v(I_v) = 1$ and thus $\iota_v : \langle \mathrm{Frob}_v \rangle \to G_{K,S}$ is well-defined up to conjugacy class. The image of Frob_v under this map is also called Frob_v.

If $v \in S$, we still get a map $\iota_v : G_{K_v} \to G_{K,S}$; it seems reasonable to believe that this map is injective, but this is an open question.

Theorem 4. *The conjugacy classes of the* Frob_v *for* $v \notin S$ *are dense in* $G_{K,S}$.

[2] Note that G_K (and thus $G_{K,S}$) is countably infinitely generated. For fix an algebraic closure $\bar{K}$ of K; then K has a finite number of extensions of a given degree, so a countable number of finite extensions, contained in $\bar{K}$. Thus G_K is a countable limit of finite groups, so countable.

Proof. This is an almost immediate consequence of the Cebotarev density theorem. The open normal subgroups of finite index form by definition a basis for the topology of $G_{K,S}$ at the identity. If $g \in G_{K,S}$, then a basis of neighborhoods of g is the set of gU for U a finite index open normal subgroup, so it suffices to show that each of these contains a conjugate of some $\mathrm{Frob}_v, v \notin S$. For each U, we can define K_U to be the extension of K that is fixed by U; this is Galois since U is normal, and

$$G_{K,S}/U = \mathrm{Gal}(K_U/K)$$

Given $gU \in \mathrm{Gal}(K_U/K)$, the Cebotarev density theorem says that there is some $v \notin S$ such that $\mathrm{Frob}_v \in \mathrm{Gal}(K_U/K)$ is conjugate to gU. But Frob is functorial, so in $G_{K,S}$, some conjugate of Frob_v is in gU. □

2 Galois representations

2.1 Introduction

Definition 5. A Galois representation of G_K, where K is any field, over a topological field L, is a finite-dimensional L-vector space V together with a continuous morphism $\rho : G_K \to GL_L(V)$.

If $(\rho_1, V_1), (\rho_2, V_2)$ are two representations, a morphism between them is an L-linear map $f : V_1 \to V_2$ such that for every $g \in G_K$,

$$f \circ \rho_1(g)(v) = \rho_2(g)(f(v))$$

Definition 6. A *subrepresentation* of (ρ, V) is a subspace $W \subset V$ such that for all $g \in G$, $\rho(g)(W) \subset W$. A subrepresentation W is *proper* if $W \neq \{0\}, W \neq V$. A representation is *irreducible* if it has no proper subrepresentations. A *complement* for a subrepresentation $W \subset V$ is another subrepresentation W' of V such that $W \oplus W' = V$. A representation is *indecomposable* if it cannot be written $V = W \oplus W'$ where W is a proper subrepresentation. Finally a representation is *semisimple* if it is a direct sum of irreducible representations, i.e. if every subrepresentation has a complement.

If (ρ, V) is a representation with dimension n, we can choose a basis of V over L and get a representation $\rho : G_K \to GL_n(L)$.

Now let K be a number field.

Definition 7. Let (ρ, V) be a Galois representation of K. Let v be a finite place of K. Then ρ is *unramified at* v if $\rho(I_v) = 1$; that is, if $I_v \subset \ker \rho$. (Note again that I_v is defined only up to conjugacy, but $\ker \rho$ is normal, so all conjugates of any element $\sigma \in I_v$ are also in $\ker \rho$ if σ is).

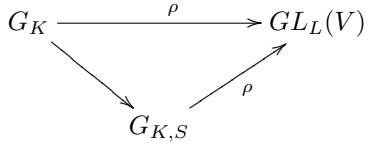
Equivalently, ρ is unramified at v if $K' = \bar{K}^{\ker \rho}$ is unramified over K at v, since ρ is unramified at v if and only if $I_v \subset \ker \rho$ if and only if $\bar{K}^{I_v} \supset \bar{K}^{\ker \rho}$. But $\bar{K}^{I_v}/K$ is unramified at v.

Definition 8. (ρ, V) is *unramified outside of* S if it is unramified at each place $v \notin S$. (ρ, V) is *unramified almost everywhere* if there is a finite set S of finite places of K such that ρ is unramified outside of S.

Proposition 9. *If ρ has finite image, then ρ is unramified almost everywhere (that is, ρ is unramified outside of a finite set of primes).*

Proof. Since ρ has finite image, it factors through a finite quotient of G_K, which is a finite group that is the Galois group of a finite Galois extension K'/K. ρ is ramified at v iff $\rho(I_v) \neq 1$, which happens iff v ramifies in K'. Thus ρ is ramified precisely where K'/K is ramified. □

Proposition 10. *If S is a finite set of primes and ρ is unramified outside of S, then ρ factors through $G_{K,S}$:*



Proof. The kernel of the map $G_K \to G_{K,S}$ is the smallest normal subgroup containing all I_v for $v \notin S$, and this subgroup is in the kernel of ρ. □

We call the induced map $G_{K_S} \to GL_L(V)$ ρ as well.

If ρ is unramified outside of S and $v \notin S$, then $\rho(\mathrm{Frob}_v)$ is an element of $GL_L(V)$ well-defined up to conjugacy class. This means that $\operatorname{tr}\rho(\mathrm{Frob}_v)$, $\det\rho(\mathrm{Frob}_v)$, and $\chi_{\rho(\mathrm{Frob}_v)}$ (the characteristic polynomial of $\rho(\mathrm{Frob}_v)$) are all well-defined.

Theorem 11. *If* $\operatorname{char} L = 0$*, then a semisimple Galois representation unramified outside of* S *is completely determined up to isomorphism by the data of* $\operatorname{tr}\rho(\mathrm{Frob}_v)$ *for* $v \notin S$*.*

The proof uses the following standard fact about representations of groups: A semisimple representation of a group G over a field L of characteristic zero is determined by its *character*, which is the map $G \to L : g \to \operatorname{tr}\rho(g)$. Both hypotheses are required. Thus, if L does not have characteristic zero, consider the representation consisting of $p+1$ copies of the trivial representation; this has character identical to that for the trivial representation. If V is not semisimple, choose a proper subrepresentation $W \subset V$ that is not a direct summand. Then as vector spaces, $V = W \oplus V/W$; the matrix of V consists of the matrix of W in the upper left, zeros in the lower left, the matrix of V/W in the lower right, and some arbitrary nonzero entries in the upper right. The matrix of $W \oplus V/W$ as a representation is identical except that it has zeros in the upper right. Thus the trace of these two representations is the same, but the representations themselves are not.

Proof. tr and ρ are both continuous, so $\operatorname{tr}\rho$ is as well. Since Frob_v for $v \notin S$ is dense in G_K the values of $\operatorname{tr}\rho(g)$ are determined for all $g \in G$ and thus the representation is. □

2.2 Artin representations

Suppose we take $L = \mathbb{C}$ in a Galois representation . Such a Galois representation is called an *Artin representation.* It turns out that these representations are not general enough, primarily because the topologies on $\mathbb{C}$ and on K are quite different. In fact

Theorem 12. *Every Artin Galois representation has finite image.*

Corollary 13. *Every Artin Galois representation* ρ *1) is semisimple, 2) is unramified almost everywhere, and 3) factors through some* $G_{K,S}$ *for* S *finite, and if* $v \notin S$*, then* $\rho(\mathrm{Frob}_v)$ *is well-defined up to conjugacy and has eigenvalues that are all roots of unity. Thus* $\operatorname{tr}(\rho(\mathrm{Frob}_v))$ *is a cyclotomic integer.*

Proof. Since ρ has finite image, it factors through a finite quotient of G_K, so it is semisimple by standard finite group representation theory. By Proposition **??**, ρ is unramified except at a finite number of primes. Since ρ is unramified almost everywhere, by Proposition **??** it factors through $G_{K,S}$ for S finite containing the set of primes at which ρ is ramified. The rest follows from finite group representation theory. □

We start the proof of the theorem above with the following lemma, which holds actually for all Lie groups. Note that it does not hold for, e.g., $\mathbb{Z}_p$, since $\mathbb{Z}/p^n\mathbb{Z}$ are arbitrarily small.

Lemma 14. $GL_n(\mathbb{C})$ *has no arbitrarily small subgroups except for* $\{I\}$*; that is, there is a neighborhood* U *of* $\{1\}$ *that contains no nontrivial subgroup.*

Proof. Consider the map $\exp : M_n(\mathbb{C}) \to GL_n(\mathbb{C})$. This is not a group homomorphism, but it is a diffeomorphism from a neighborhood W of $0 \in M_n(\mathbb{C})$ to an open neighborhood V of $I \in GL_n(\mathbb{C})$. We may assume that $W = B(0,r)$ for some $r > 0$ in some norm. Take $W' = B(0, r/2)$, and

$U = \exp(W')$. Claim U is the U asserted by the lemma. Suppose not, and that $G \subset U$ is a nontrivial subgroup. Choose $I \neq g \in G$; then $g = \exp(x), x \in W'$, and $0 < \|x\| < r/2$. Thus there is some $n \in \mathbb{Z}$ such that $r/2 \leq \|nx\| < r$. Then $\exp(nx) = x^n \in G$ (this is obvious from the power series for exp). But $x^n \notin U$ since $nx \notin W'$. □

Proof. (of theorem regarding Artin representations) Suppose $\rho : G_K \to GL_n(\mathbb{C})$ is an Artin representation, and choose U as in the theorem. Then $\rho^{-1}(U)$ is a neighborhood of $1 \in G_K$, so it contains some open subgroup H of G_K. Thus $\rho(H) \subset U$ so that $H \in \ker \rho$. But G_K is compact and H has finite index since it is an open subgroup of a compact space. Thus $\rho(G)$ is finite. (Alternatively, a basis of open sets consists of *normal* open subgroups, and then ρ factors through G/H). □

Example 15. Let $K = \mathbb{Q}$, L a quadratic extension; then $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. Define an Artin representation ϵ_L by the following composition:

$$G_{\mathbb{Q}} \xrightarrow{restriction} \mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\} \subset \mathbb{C}^* = GL_1(\mathbb{C})$$

ϵ_L is continuous since the kernel of the restriction map is open, and ϵ_L is ramified at places where $L/\mathbb{Q}$ is ramified, since $\ker \epsilon_L = \mathrm{Gal}(\bar{\mathbb{Q}}/L)$ (this follows from the definition: ϵ_L is ramified at v if and only if $\bar{\mathbb{Q}}^{\ker \epsilon_L}/K$ is ramified at v; but $\bar{\mathbb{Q}}^{\ker \epsilon_L} = \bar{\mathbb{Q}}^{\mathrm{Gal}(\bar{\mathbb{Q}}/L)} = L$.

If p is a prime unramified in L, then

$$\epsilon_L = \begin{cases} 1 & \text{when } p \text{ splits in } L \\ -1 & \text{when } p \text{ is inert in } L \end{cases}$$

This follows from the fact that this formula holds for the image of $\mathrm{Frob}_p \in \mathrm{Gal}(L/K)$, which is a standard result from the theory of quadratic extensions[3] If you embed $L \subset \mathbb{Q}(\zeta_n)$, you can regard ϵ_L as a Dirichlet character of $\mathbb{Z}/n\mathbb{Z}$.

Example 16. Let $P(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ be irreducible, and L its decomposition field in some fixed algebraic closure of $\mathbb{Q}$. Assume that $[L : \mathbb{Q}] = 6$, so that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. S_3 acts on $\mathbb{C}^2$: take the obvious action of S_3 on $\mathbb{C}^3$ and take the subrepresentation on the plane $V = \{x_1 + x_2 + x_3 = 0\}$. This gives a two-dimensional Artin representation

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \cong S_3 \to GL(V)$$

that is unramified at primes unramified in L.

As an exercise, fill in the blanks:

$$\mathrm{tr}(\rho(\mathrm{Frob}_p)) = \begin{cases} ? & ? \\ ? & ? \\ ? & ? \end{cases}$$

where the conditions are some arithmetic property of $P(x)$ relative to p.

All Artin representations are like this - they have finite image, so factor through some finite group and thus arise from a representation of $\mathrm{Gal}(L/K)$ for some finite extension L of K.

[3] Writing $L = K(\sqrt{d})$, note that $\mathrm{Frob}_{\mathfrak{P}}$ is determined by its value on $\sqrt{d}$, and has the property that $\mathrm{Frob}_{\mathfrak{P}}(a) \equiv a^p \mod \mathfrak{P}$. So $\mathrm{Frob}_{\mathfrak{P}}(\sqrt{d}) \equiv d^{p/2} \mod \mathfrak{P}$ and thus $\mathrm{Frob}_{\mathfrak{P}}(\sqrt{d})/\sqrt{d} \equiv d^{(p-1)/2} \mod \mathfrak{p}$ and hence $\mod p$, since it happens to be in $\mathbb{Q}$, so it is exactly the Legendre symbol.

2.3 The l-adic cyclotomic character

2.3.1 Definitions

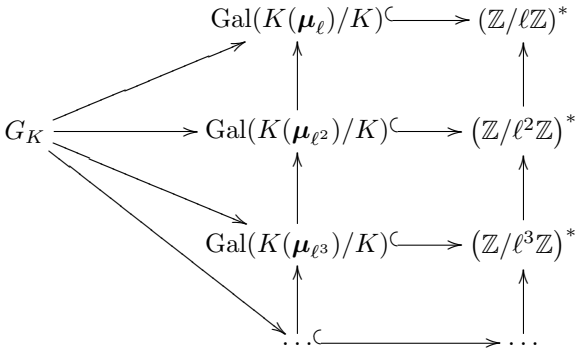
We now look at more general representations, ℓ-adic representations, which are Galois representations $\rho : G_K \to GL_L(V)$ where L is a finite extension of $\mathbb{Q}_p$ and V is a finite dimensional vector space over L.

Let K be a number field, ℓ a prime. We will define the ℓ-adic cyclotomic character $\omega_\ell : G_K \to \mathbb{Q}_\ell^* = GL_1(\mathbb{Q}_\ell)$.

Let $n \geq 1$ be an integer, and $K(\boldsymbol{\mu}_{\ell^n}) \subset \bar{K}$ the cyclotomic field (i.e. adjoin all $\ell^{n\text{th}}$ roots of unity to K from $\bar{K}$. This is Galois over K, and there is a natural homomorphism

$$\omega_{\ell,n} : \mathrm{Gal}(K(\boldsymbol{\mu}_{\ell^n})/K) \hookrightarrow (\mathbb{Z}/\ell^n\mathbb{Z})^*$$

that is defined as follows. It suffices to define $\omega_{\ell,n}$ on a primitive $\ell^{n\text{th}}$ root of unity; for any such, and for $\sigma \in \mathrm{Gal}(K(\boldsymbol{\mu}_{\ell^n})/K)$, define $\omega_{\ell,n}(\sigma)$ by $\sigma(\zeta) = \zeta^{\omega_{\ell,n}(\sigma)}$; $\sigma(\zeta)$ is also a primitive root of unity. The map is obviously injective. We thus get a system of maps



Let $K_\infty = \varinjlim_n K(\boldsymbol{\mu}_{\ell^n})$; write $\Gamma = \mathrm{Gal}(K_\infty/K)$. It is easy to see that $\Gamma = \varprojlim \mathrm{Gal}(K(\boldsymbol{\mu}_{\ell^n})/K)$, so taking inverse limits we get a map

$$\omega_\ell : G_K \to \Gamma \to \mathbb{Z}_\ell^* \subset \mathbb{Q}_\ell^*$$

This the ℓ-adic cyclotomic character. Note that the embeddings $\mathrm{Gal}(K(\boldsymbol{\mu}_{\ell^k})/K) \hookrightarrow \left(\mathbb{Z}/\ell^k\mathbb{Z}\right)^*$ are in fact independent of the choice of primitive root of unity above, so the cyclotomic character can be seen as a canonical embedding of Γ into $\mathbb{Z}_\ell^*$.

In what follows, we will freely write $\omega_{l,n}$ for the map either from $\mathrm{Gal}(K(\boldsymbol{\mu}_{\ell^n})/K)$ or from G_K.

Theorem 17. *ω_ℓ is continuous and is unramified at all places of K not dividing ℓ. Further, if v is a finite place of K not dividing ℓ, then $\omega_\ell(\mathrm{Frob}_v)$ is well-defined (not just up to conjugacy, since $\mathbb{Q}_\ell^*$ is abelian), and is equal to the size of the residue field of v.*

Proof. That ω_ℓ is continuous follows from the fact that each $\omega_{l,n}$ from G_K is continuous since the kernel is an open Galois subgroup.

The field $K(\boldsymbol{\mu}_{\ell^n})$ is unramified over K at all places not dividing ℓ, so this is true for $\omega_{\ell,n}$. Thus ω_ℓ is trivial on all $I_{\ell,n}$ and thus on I.

A sketch for the third statement in the case where $K = \mathbb{Q}$ is as follows: The size of the residue field of p in $\mathbb{Q}_\ell^*$, for $p \neq \ell$, is p, so the statement is simply that $\omega_\ell(\mathrm{Frob}_p) = p$. But this is true for each $\omega_{\ell,n}$, so it is true in the limit. □

In particular, note that $\omega_\ell(\mathrm{Frob}_p)$ is rational in $\mathbb{Q}_p^*$; this attribute of a Galois representation is called "rationality of representation".

Corollary 18. *If $v \nmid \ell$, then $\omega_\ell(\mathrm{Frob}_v) = \mathrm{N}(v) =_{df} \|\mathcal{O}_{K_v}/\mathfrak{m}_v\|$.*

Note that $\mathrm{N}(v) \in \mathbb{Z}$ and is defined for almost all v, and if $v \nmid \ell, \ell'$, then $\omega_\ell(\mathrm{Frob}_v) = \omega_{\ell'}(\mathrm{Frob}_v)$. Thus $\omega_\ell(\mathrm{Frob}_v)$ does not depend on ℓ and we have a compatible system of Galois representations.

Theorem 19. *If K'/K is a finite extension, then $\omega_\ell^K|_{G_{K'}} = \omega_\ell^{K'}$.*

Proof. ω_ℓ is defined by the action of G_K on the ℓ^n roots of unity, and that action is identical over K' since K, K' are contained in the same algebraic closure of K. □

Theorem 20. *$\omega_\ell(G_K)$ is an open subgroup of finite index in $\mathbb{Z}_\ell^*$.*

Proof. It is in $\mathbb{Z}_\ell^*$ by construction. Now, $\omega_{\ell,n}(G_\mathbb{Q})$ is surjective since each map is an isomorphism, so in the limit $\omega_\ell(G_\mathbb{Q})$ is surjective. G_K is compact in $G_\mathbb{Q}$, so that $\omega_\ell(G_K)$ is closed. By the previous theorem, since $K/\mathbb{Q}$ is finite, $\omega_\ell(G_K)$ is of finite index in $\mathbb{Z}_\ell^*$ and thus open. □

2.3.2 Summary of CFT

Recall that we have a commutative diagram, for any place v of K,

$$\begin{array}{ccc} \mathbb{A}_K^*/K^*(K_\infty^*)^0 & \xrightarrow[Art]{\cong} & G_K^{ab} \\ \uparrow & & \uparrow \\ K_v^* & \xrightarrow{Art_v} & G_{K_v}^{ab} \end{array}$$

where K^* is the image of K in the adèles under the diagonal embedding and $(K_\infty^*)^0$ is the connected component of the identity in the product of the completions at the archimedean places; i.e. it is $(\mathbb{C}^*)^s(\mathbb{R}_+)^r$ so that each real place contributes $\mathbb{Z}/2\mathbb{Z}$ to the result. The map along the top row is called the *Artin map* and is an isomorphism; the map along the left-hand side embeds K_v^* into the component corresponding to the place $v$and the map on the right-hand side arises from the fact that we have a map $G_{K_v} \hookrightarrow G_K$ defined up to conjugacy class, so that in the abelianizations, the map is well-defined.

The bottom map is called the *local Artin map*. If v is nonarchimedean (finite), then Art_v is injective with dense image, while if v is archimedean, then $\ker Art_v = (K_v^*)^0$ and $\mathrm{im}\, Art_v = G_{K_v}^{ab}$ (which is either trivial or congruent to $\mathbb{Z}/2\mathbb{Z}$).

Additionally, if v is a finite place, we can add a third row to the diagram:

$$\begin{array}{ccc} \mathbb{A}_K^*/K^*(K_\infty^*)^0 & \xrightarrow[Art]{\cong} & G_K^{ab} \\ \uparrow & & \uparrow \\ K_v^* & \xrightarrow{Art_v} & G_{K_v}^{ab} = \mathrm{Gal}(K_v^{ab}/K_v) \\ \uparrow & & \uparrow \\ \mathcal{O}_{K_v}^* & \xrightarrow[\cong]{Art_v} & I(K_v^{ab}/K_v) \end{array}$$

where the right-hand map is actually an inclusion. Thus the inertia group of the abelianization is the elements of norm 1. We also see that if v is a finite place, then

$$Art_v(\pi_v) = \mathrm{Frob}_v$$

if π_v is a uniformizer; this map is well-defined since both π_v and Frob_v are well-defined up to elements of $\mathcal{O}_{K_v}^*$ and the inertia group respectively, and those groups are isomorphic through Art_v.

Since $\omega_\ell : G_L \to \mathbb{Q}_\ell^*$, which is an abelian group, the map factors through G_K^{ab}, the abelianization of G_K; we call the factor map $\omega_\ell : G_K^{ab} \to \mathbb{Q}_\ell^*$ as well.

2.3.3 Computation of the l-adic cyclotomic character on the rationals

We will use the adelic representation of G_K^{ab} to describe ω_ℓ in the case $K = \mathbb{Q}$. Define $\tilde{\omega_\ell} = \omega_\ell \circ Art$; describing $\tilde{\omega_\ell}$ means describing its action on each embedded subgroup $\mathbb{Q}_p^*$ as well as $\mathbb{R}^*$.

Note that for each prime p, the map

$$\mathbb{Q}_p^* \hookrightarrow \mathbb{A}_\mathbb{Q}^* \to \mathbb{A}_\mathbb{Q}^*/\mathbb{Q}^*\mathbb{R}_+^*$$

is actually injective since if $x \in \mathbb{Q}_p^* \cap \mathbb{Q}^*\mathbb{R}_+^*$ then x maps to $(1, \dots, 1, x, 1, \dots) \in \mathbb{A}_\mathbb{Q}^*$. But the embedding of $\mathbb{Q}^*\mathbb{R}_+^*$ into $\mathbb{A}_\mathbb{Q}^*$ is diagonal, so if this is in the kernel, we must have $x = 1$.

If $p \neq \ell$ is a prime, we wish to compute $\tilde{\omega_\ell}|_{\mathbb{Q}_p^*}$. Recall that $\mathbb{Q}_p^* \cong \mathbb{Z}_p^* \times p^\mathbb{Z}$, and that the inertia group of $G_{\mathbb{Q}_p}^{ab}$ corresponds to $\mathcal{O}_{\mathbb{Q}_p}^* = \mathbb{Z}_p^*$. Since ω_ℓ is unramified at p, it is trivial on the inertia group and thus $\tilde{\omega_\ell}$ is trivial on $\mathbb{Z}_p^*$. It remains to say what it does to p. But $\tilde{\omega_\ell}(p) = \omega_\ell(\mathrm{Frob}_p) = p$.

Consider next the case of an infinite (real) prime. $\tilde{\omega_\ell}|_{\mathbb{R}^*}$ is trivial on $\mathbb{R}_+^*$, and $\mathbb{R}^* = \mathbb{R}_+^* \times \{\pm 1\}$. Thus is suffices to compte $\tilde{\omega_\ell}(-1)$. But this is just ω_ℓ applied to complex conjugation in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, so is either ± 1. Since the ℓ^n roots of unity are not real, complex conjugation is not the identity, so we have $\tilde{\omega_\ell}(-1) = -1$.

Finally, we compute $\tilde{\omega_\ell}|_{\mathbb{Q}_\ell^*}$. Here ω_ℓ is not trivial on $\mathcal{O}_\ell^*$, and we can't really apply the CFT diagram. But we can use the embedding of $\mathbb{Q}^*$ into the adèles together with the fact that $\tilde{\omega_\ell}$ is trivial on $\mathbb{Q}^*$. For $x \in \mathbb{Q}^*$, write

$$x = \epsilon \cdot \ell^{n_\ell} \cdot \prod_{p \neq \ell} p^{n_p}, \quad \epsilon = \pm 1$$

x embeds as $(x, x, \dots) \in \mathbb{A}_\mathbb{Q}^*$, so

$$\begin{aligned} 1 = \tilde{\omega_\ell}(x) &= \prod_{v \text{ a place of } \mathbb{Q}} \tilde{\omega_\ell}|_{\mathbb{Q}_v^*}(x) \\ &= \tilde{\omega_\ell}|_{\mathbb{Q}_\ell^*}(x) \cdot \tilde{\omega_\ell}|_{\mathbb{R}^*}(x) \cdot \prod_{p \neq \ell} \tilde{\omega_\ell}|_{\mathbb{Q}_p^*}(x) \\ &= \tilde{\omega_\ell}|_{\mathbb{Q}_\ell^*}(x) \cdot \epsilon \cdot \prod_{p \neq \ell} p^{n_p} \end{aligned}$$

Here $\tilde{\omega_\ell}|_{\mathbb{Q}_p^*}(x) = p^{n_p}$ since all other factors of x end up in $\mathbb{Z}_p^*$ inside $\mathbb{Q}_p^*$, and $\tilde{\omega_\ell}$ maps all of those to 1. Thus we get for $x \in \mathbb{Q}$

$$\tilde{\omega_\ell}|_{\mathbb{Q}_\ell^*}(x) = \frac{\ell^{n_\ell}}{x}$$

Finally, since $\mathbb{Q}^*$ is dense in $\mathbb{Q}_\ell^*$, we have for $x \in \mathbb{Q}_\ell^*$

$$\tilde{\omega_l}|_{\mathbb{Q}_\ell^*}(x) = \frac{\ell^{v_\ell(x)}}{x}$$

In particular, on $\mathbb{Z}_\ell^*$, $\tilde{\omega_\ell}(x) = \frac{1}{x}$.

2.4 The Tate module of an elliptic curve

Let K be a field and E/K an elliptic curve defined over K. Let l be a prime not equal to the characteristic of K. Then for $n \geq 1$ we have the groups

$$E(\bar{K})[\ell^n] = \ker[\ell^n] : E(\bar{K}) \to E(\bar{K})$$

This group is isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. Also, $G_K = \mathrm{Gal}(\bar{K}/K)$ acts on $E(\bar{K})[\ell^n]$ by transforming the coordinates of any point in this group; the image under this action is again in $E(\bar{K})[\ell^n]$ since the elliptic curve is defined over K so that the Galois group leaves the equation of E fixed.

We get a sequence of maps $[\ell] : E(\bar{K})[\ell^{n+1}] \to E(\bar{K})[\ell^n]$ that is simply the projection map

$$\left(\mathbb{Z}/\ell^{n+1}\mathbb{Z}\right)^2 \to (\mathbb{Z}/\ell^n\mathbb{Z})^2$$

Definition 21. The *Tate module* of E is $T_\ell(E) = \varprojlim E(\bar{K})[l^n]$

It is clear from the above that $T_\ell(E) \cong \mathbb{Z}_\ell^2$, and that it too commutes with the G_K action since multiplication by ℓ is defined over K. Thus G_K acts continuously on $T_\ell(E)$.

Definition 22. $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

It is a fact that $V_\ell(E)$ is a continuous representation of G_K of dimension 2.

Proposition 23. *V_ℓ is a covariant functor from the category $Ell(K)$ of elliptic curves over K and morphisms to $Rep(G_K, \mathbb{Q}_\ell)$ of representations of G_K on $\mathbb{Q}_\ell$ where the morphisms are maps of vector spaces compatible with the group actions. In addition, V_ℓ maps isogenies to isomorphisms.*

A sketch of the proof is as follows. For the first part, a map $E \to E'$ gives maps $E(\bar{K})[\ell^n] \to E(\bar{K'})[\ell^n]$ that commute with the G_K action, so we get maps $T_\ell(E) \to T_\ell(E')$ and $V_\ell(E) \to V_\ell(E')$ that do as well. For the second part, assume $\phi : E \to E'$ is an isogeny with $\deg \phi = d$. Then we know that there is $\hat{\phi} : E' \to E$ with

$$[d] = \phi \circ \hat{\phi} = \hat{\phi} \circ \phi$$

Then

$$V_\ell([d]) = V_\ell(\phi) \circ V_\ell(\hat{\phi})$$
$$V_\ell([d]) = V_\ell(\hat{\phi}) \circ V_\ell(\phi)$$

and $V_\ell([d])$ is simply multiplication by d in the vector space $V_\ell(E)$ so is an isomorphism of $V_\ell(E)$. Thus the maps on the right are isomorphisms as well.

Note that $[n]$ is an isomorphism in $\mathbb{Q}_\ell$ even if $\ell \mid n$; this is not the case in $\mathbb{Z}_\ell$.

We thus have a map (actually a homomorphism of groups)

$$f : \mathrm{Hom}_K(E_1, E_2) \to \mathrm{Hom}_{G_K}(V_\ell(E_1), V_\ell(E_2))$$

that maps nonzero isogenies to isomorphisms. It follows that *if there is any nonzero isogeny between two elliptic curves E_1, E_2, then their Tate modules are isomorphic as G_K representations.*

Theorem 24. $\mathrm{Hom}_K(E_1, E_2) \hookrightarrow \mathrm{Hom}_{G_K}(V_\ell(E_1), V_\ell(E_2))$*, and injectivity is preserved on tensoring:* $\mathrm{Hom}_K(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Q} \hookrightarrow \mathrm{Hom}_{G_K}(V_\ell(E_1), V_\ell(E_2))$.

See Silverman for a discussion of this issue.

In general, this map is not surjective. For example, if $K = \bar{K}$, then G_K is small so there are lots of G_K homomorphisms.

We want to analyze the Tate module over number fields; in order to do this, we first look at the finite field and local field cases.

If K is a finite field, say $K = \mathbb{F}_q$, $q = p^n, \ell \neq p$, then $V_\ell(E)$ is a $G_K \cong \hat{\mathbb{Z}}$ module. We have the Frobenius endomorphism $\phi \in \mathrm{End}_K(E) : (x, y) \mapsto (x^q, y^q)$.We can also define $\phi_\ell \in GL_{\mathbb{Q}_\ell}(V_\ell(E)) \cong GL_2(\mathbb{Q}_\ell)$ by

$$\phi_\ell = V_\ell(E)(\mathrm{Frob})$$

that is, the image of the Frobenius of $\bar{K}/K$ (a generator of $\hat{\mathbb{Z}}$) under the representation map.

Theorem 25. *1.* $\#E(K) = \deg(1 - \phi)$

2. $\det \phi_\ell = \deg \phi = q = \#K$

3. $\mathrm{tr}\, \phi_\ell = 1 + \det \phi_\ell - \det(1 - \phi_\ell) = 1 + \deg \phi - \deg(1 - \phi)$

4. $\#E(K) = 1 + q - \mathrm{tr}(\phi_\ell)$

5. The eigenvalues of ϕ_ℓ are algebraic integers that are either real and equal, or complex and conjugate. If we denote them α, β, we have $|\alpha| = |\beta| = q^{1/2}$.

Proof. Much of this is in Silverman §V.2. The first equality in (3) is true of any 2×2 matrix. □

Corollary 26. *(Hasse, Weil conjecture)*

$$|\#E(K) - q - 1| \leq 2\sqrt{q}$$

Proof. The left-hand side is $|\mathrm{tr}(\phi_\ell)| = |\alpha + \beta| \leq 2\sqrt{q}$. □

Corollary 27. *Two isogenous elliptic curves over K have the same number of points in K.*

Proof. If they are isogenous, then their Tate modules are isomorphic, so ϕ_ℓ is conjugate in the two modules so have the same trace. By part (4) of Theorem **??**, this means they have the same number of points in K. □

Theorem 28. *(Tate) If K is a finite field, then*

$$\mathrm{Hom}_K(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{Hom}_{G_K}(V_\ell(E_1), V_\ell(E_2))$$

Now suppose K is a local field with ring of integers $\mathcal{O}$, maximal ideal $\mathfrak{m}$, and residue field k.

Definition 29. E/K has *good reduction* if and only if a minimal Weierstrass equation for E has $\Delta \in \mathcal{O}^*$.

If E/K has good reduction, we can reduce the minimal equation modulo $\mathfrak{m}$ to get an equation $\tilde{E}/k$ that has nonzero discriminant and thus is nonsingular over k.

Theorem 30. *(Neron-Ogg-Shafarevich) E/K has good reduction if and only if $V_\ell(E)$ is unramified. In addition, if E/K has good reduction, then $V_\ell(E) \cong V_\ell(\tilde{E})$ via the reduction map, and the reduction map commutes with the Galois actions. That is, we have the following diagram:*

$$\begin{array}{ccccccccc} & & & & V_\ell(E) & \xrightarrow{\cong} & V_\ell(\tilde{E}) & & \\ & & & & \circlearrowleft & & \circlearrowleft & & \\ 1 & \longrightarrow & I_K & \longrightarrow & G_K & \longrightarrow & G_k & \longrightarrow & 1 \end{array}$$

Note that the commutativity of the diagram proves one direction of the if and only if, since if E/K has good reduction, clearly the image of I_K acts trivially on $V_\ell(\tilde{E})$; since the actions are compatible, I_K acts trivially on $V_\ell(E)$ and $V_\ell(E)$ is unramified.

Corollary 31. *If E, E' are isogenous over K then either both have good reduction or neither does.*

This follows easily from the theorem together with the fact that isogenous curves have isomorphic Tate modules.

Note that if E/K has good reduction, then $\det V_\ell(E)(\text{Frob}) = q$ (Frob is well-defined in G_K because I_K acts trivially since $V_\ell(E)$ is unramified.). Also

$$1 + q - \operatorname{tr} V_\ell(E)(\text{Frob}) = \#\tilde{E}(k)$$

This follows from the commutative diagram above plus the corresponding equality for finite fields. We can lift Frob from G_k, and the actions are compatible.

Now let K be a number field, E/K an elliptic curve, and $V_\ell(E)$ the Tate module with the action of G_K.

Theorem 32. *If v is a finite place of K, $v \nmid \ell$, then E has good reduction at v if and only if $V_\ell(E)$ is unramified at v.*

To see why this is so, observe first that for E/K, $K' \supset K$ a finite extension, we have $V_\ell(E/K') = V_\ell(E)|_{G_{K'}}$ by the definition of the action - if you look at ℓ^n torsion, the action of G_K and $G_{K'}$ on that torsion is identical. One can make the same argument for the embedding $G_{K_v} \hookrightarrow G_K$ via the decomposition group.

Don't understand this.

Corollary 33. *$V_\ell(E)$ is unramified at every place where E has good reduction and that does not divide ℓ, so that $V_\ell(E)$ is unramified almost everywhere.*

Corollary 34. *If $E/K, E'/K$ are isogenous, then they have the same set of primes of bad reduction.*

Proof. Note that $V_\ell(E) \cong V_\ell(E')$. The theorem then implies that for primes not dividing ℓ, the curves have good reduction at the same set of primes. But by choosing a different ℓ', we can then cover all primes. □

Theorem 35. *Let $v \nmid l$ be a finite place of E, and assume E has good reduction at v. Let k_v be the residue field at v. Then*

$$\det(V_\ell(E)(\text{Frob}_v)) = N(v) = \#k_v$$
$$1 + \#k_v - \operatorname{tr}(V_\ell(E)(\text{Frob}_v)) = \#\tilde{E}_v(k_v)$$

In particular, both the determinant and the trace of $V_\ell(E)(\text{Frob}_v)$ are rational integers for every finite place v. This theorem shows that the Tate module contains a lot of information about the elliptic curves, since it counts points on the curve modulo different primes.

Corollary 36. $\det V_\ell(E) = \omega_\ell$ *and* $V_\ell(E)^* = V_\ell(E) \otimes \omega_\ell^{-1}$.

Proof. The first of these follows since $\omega_\ell(\mathrm{Frob}_v) = N(v)$, so the representations agree on Frob_v for almost all places so are the same. The second follows since for any 2-dimensional representation $\rho : G \to GL(V)$ we have $\rho^* = \rho \otimes (\det \rho)^{-1}$ [4]. □

Theorem 37. *(Serre) Let K be a number field with $\mathrm{End}_K(E) = \mathbb{Z}$ (note that we do not assume that $\mathrm{End}_{\bar{K}}(E) = \mathbb{Z}$; the condition assumed is much weaker). Then $V_\ell(E)$ is irreducible.*

This theorem says that we have an irreducible two-dimensional representation of G_K, which allows us to get information about the nonabelian part of G_K; CFT talks only about the abelianization.

We start by proving a lemma:

Lemma 38. *Assume* $\mathrm{char}\, K = 0$*, E/K an elliptic curve with $\mathrm{End}_K(E) \cong \mathbb{Z}$. If $E' \xrightarrow{f} E, E'' \xrightarrow{g} E$ are K-isogenies with cyclic kernels $\mathbb{Z}/n'\mathbb{Z}, \mathbb{Z}/n''\mathbb{Z}$ where $n' \neq n''$, then E' is not isomorphic to E'' over K.*

Proof. Assume $E' \xrightarrow{h} E''$ is an isomorphism, and consider the composite map

$$E \xrightarrow{\hat{f}} E' \xrightarrow{h} E'' \xrightarrow{g} E$$

This map is $[a]$ for some a by the assumption on $\mathrm{End}_K(E)$ and thus $n'n'' = a^2$. Now obviously $\ker E(\bar{K})[a] \subset (\mathbb{Z}/a\mathbb{Z})^2$, but by the above, $\ker E(\bar{K})[a]$ is an extension of $\mathbb{Z}/n'\mathbb{Z}$ by $\mathbb{Z}/n''\mathbb{Z}$, so by elementary abelian group theory, we get $a = n' = n''$[5]. □

Proof. (of Serre's theorem) Assume $V_\ell(E)$ is reducible. Then there is a one-dimensional line $D \subset V_\ell(E)$ that is stable under G_K. Define $D_0 = D \cap T_\ell(E)$; since $T_\ell(E)$ is a rank 2 lattice, isomorphic to $\mathbb{Z}_\ell^2$, we have that D_0 is a $\mathbb{Z}_\ell$ submodule of rank 1, thus isomorphic to $\mathbb{Z}_\ell \subset T_\ell(E)$, and that it is stable under the G_K action. (Note that $D_0 \neq T_\ell(E)$ since D is proper, and note that it is free since $\mathbb{Z}_\ell^2$ is free). Now, claim the image of D_0 in

$$T_\ell(E)/\ell^n T_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^n\mathbb{Z} = E[\ell^n]$$

is $\mathbb{Z}/\ell^n\mathbb{Z}$ and is stable under G_K. (The final equality in the above formula holds because the tensor product reduces to just the points with l^n torsion or less). To see this, consider the short exact sequence

$$0 \to D_0 \to T_\ell(E) \to D_1 \to 0$$

In general, in an exact sequence like this, D_1 is not isomorphic to $\mathbb{Z}_\ell$ (e.g. $D_0 = \ell\mathbb{Z}_\ell$). But in this case it is since $T_\ell(E)/D_0$ injects into $V_\ell(E)$ so is torsion-free. Then tensor with $\mathbb{Z}/\ell^n\mathbb{Z}$ to get

Why is this an injection?

$$\cdots \to \mathrm{Tor}(D_1, \mathbb{Z}/\ell^n\mathbb{Z}) \to D_0 \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^n\mathbb{Z} \to T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^n\mathbb{Z} \to D_1 \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^n\mathbb{Z} \to 0$$

Since $D_1 \cong \mathbb{Z}_\ell$, it is torsion-free and the resulting sequence is short exact.

Why does this show the claim?

Now define $E_n = E/\operatorname{im} D_0$; this curve is defined over K , so we get an isogeny $E \to E_n$ with kernel

Why defined over K?

[4] Recall that the dual of ρ is defined by $\rho^*(g) = (\rho(g^{-1}))^T = (\rho(g)^{-1})^T$. Thus if $\rho(g) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $\rho^*(g) = (\det \rho(g))^{-1} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$. But that matrix is similar to $\rho(g)$ since

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

[5] For since $\mathbb{Z}/n'\mathbb{Z}$ injects into $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$, the image must have an element of order exactly n', so that $n' \mid a$ and $n' \leq a$. Similarly, the quotient has an element of order n'', so that $a \geq n''$. But $n'n'' = a^2$, and the result follows.

$\mathbb{Z}/l^n\mathbb{Z}$ and thus a dual isogeny $E_n \to E$ with the same kernel, for every n. By the above lemma (and since $\mathrm{End}_K(E) \cong \mathbb{Z}$), the E_n are not pairwise isomorphic over K. The result then follows by contradiction using

Theorem 39. *(Shafarevich) Let K be a number field, S a fixed finite set of finite places of K. Then there are only a finite number of K-isomorphism classes of elliptic curves over K with good reduction outside of S (Silverman, AEC, Ch. IX, /textsection 6).*

Corollary 40. *If K is a number field and E/K an elliptic curve, then there are only finitely many elliptic curves E'/K isogenous to E, up to K-isomorphism.*

□

The corollary clearly follows from Shafarevich's theorem: any curve isogenous to E has an isomorphic Tate module and thus has bad reduction at exactly the places where E does, so by the theorem there are only a finite number of such, up to K-isomorphism.

Here is a sketch of the proof of Shafarevich's theorem. First enlarge S such that $\mathcal{O}_{K,S}$, the set of elements of K that are integers outside of S (i.e. whose valuation is ≥ 0 except at S), is a PID (see, for example, www.math.uga.edu/˜mbaker/Sunits.pdf). If we prove the result for this S, clearly we are done. Now, an elliptic curve E/K with good reduction outside S has minimal equation $y^2 = 4x^3 + ax + b$ for $a, b \in \mathcal{O}_{K,S}$ and Δ invertible in $\mathcal{O}_{K,S}$. Since Δ is well-defined up to twelfth powers, we have

$$\Delta \in \mathcal{O}_{K,S}^* / \left(\mathcal{O}_{K,S}^*\right)^{12}$$

and this group is finite since $\mathcal{O}_{K,S}$ is finitely generated (Dirichlet's unit theorem). So we may assume that Δ is fixed. $\Delta = 4a^3 - 27b^2$, and we are reduced to the problem of discovering how many solutions this Diophantine equation has in $\mathcal{O}_{K,S}$, which is a question about integral points on an elliptic curve. This question is answered by Siegel's theorem (Silverman, AEC, Ch. IX, §3), which says there are only a finite number.

It turns out that the same statement holds for abelian varieties. The proof above does not carry through, however, since we do not have nice equations for these varieties.

In fact a stronger statement than Serre's theorem is true. We say that $V_\ell(E)$ is *absolutely irreducible* if it remains irreducible when extended to an algebraic closure, i.e. if $V_\ell(E) \otimes \bar{\mathbb{Q}}_\ell$ is irreducible. For example, $SO(2, \mathbb{R}) \cong S^1$ acts on $\mathbb{R}^2$ as an irreducible representation over $\mathbb{R}$, but this becomes reducible over $\mathbb{C}$ (since it has eigenvalues in $\mathbb{C}$). The theorem then becomes:

Theorem 41. *If $\mathrm{End}_K(E) \ncong \mathbb{Z}$, then $V_\ell(E)$ is not absolutely irreducible.*

(See Problem Set 1, Ex. 5.3, Problem Set 2, Ex. 2.4).

3 Étale cohomology

3.1 Basic Properties

References: SGA4 and SGA5 (about 2000 pages), Milne's Étale Cohomology (about 350 pp), and SGA 4 1/2 (Deligne, first paper, about 40 pp).

Let K be a field with $\ell \neq \operatorname{char} K$. Grothendieck constructed contravariant functors for $i = 0, 1, 2, \ldots$

$$\text{Algebraic Varieties}/K \to \text{Finite-dimensional representations of } G_K \text{ on } \mathbb{Q}_\ell$$

that map $X \mapsto H^i(X, \mathbb{Q}_\ell)$, and map a morphism $f : X \to Y$ defined over K to its pullback $f^* : H^i(Y, \mathbb{Q}_\ell) \to H^i(X, \mathbb{Q}_\ell)$.

Basic properties:

1. $H^i(X, \mathbb{Q}_\ell) = 0$ for $i > 2 \dim X$.
2. If K'/K is an extension, then $H^i(X, \mathbb{Q}_\ell) \cong H^i(X_{K'}, \mathbb{Q}_\ell)$ as $\mathbb{Q}_\ell$ vector spaces (i.e. they have the same dimension); this isomorphism is functorial. If further K'/K is algebraic, then $G_{K'} \hookrightarrow G_K$ and $H^i(X_{K'}, \mathbb{Q}_\ell) = H^i(X, \mathbb{Q}_\ell)|_{G'_K}$ as $G_{K'}$ representations, and this correspondence is functorial as well. Note that the larger K gets the less information we get out of the cohomology groups since G_K gets smaller.
3. There is a cup product

   $$H^i(X, \mathbb{Q}_\ell) \times H^j(X, \mathbb{Q}_\ell) \to H^{i+j}(X, \mathbb{Q}_\ell)$$

   that is a bilinear morphism of Galois representations and is functorial in X. In addition, for $a + b - i$ we have

   $$H^a(X, \mathbb{Q}_\ell) \otimes H^b(Y, \mathbb{Q}_\ell) \to H^i(X \times Y, \mathbb{Q}_\ell)$$

   This map comes about from considering the projections $X \times Y \to X, Y$ which gives pullback maps

   $$H^a(X, \mathbb{Q}_\ell) \to H^a(X \times Y, \mathbb{Q}_\ell)$$
   $$H^b(Y, \mathbb{Q}_\ell) \to H^b(X \times Y, \mathbb{Q}_\ell)$$

   and thus a bilinear map

   $$H^a(X, \mathbb{Q}_\ell) \times H^b(Y, \mathbb{Q}_\ell) \to H^a(X \times Y, \mathbb{Q}_\ell) \times H^b(X \times Y, \mathbb{Q}_\ell)$$

   which, by universality of $\otimes$ together with the cup product above, gives the required map. One also has the *Künneth formula*

   $$\sum_{a+b=i} H^a(X, \mathbb{Q}_\ell) \otimes H^b(Y, \mathbb{Q}_\ell) \cong H^i(X \times Y, \mathbb{Q}_\ell)$$

4. There is a version of Poincaré duality. If X is proper (projective) and smooth (regular everywhere) over K, then
   - $H^{2 \dim X}(X, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$ has dimension 1 and G_K acts by $\omega_l^{-\dim X}$ (note that we defined the cyclotomic character only for number fields, but it is possible to extend this definition).

- If $i + j = 2 \dim X$, then

$$H^i(X, \mathbb{Q}_\ell) \times H^j(X, \mathbb{Q}_\ell) \to H^{2 \dim X}(X, \mathbb{Q}_\ell)$$

  is nondegenerate, and thus H^i and H^j are dual as $\mathbb{Q}_\ell$ vector spaces and as Galois representations, so
- $H^i(X, \mathbb{Q}_\ell) \cong H^j(X, \mathbb{Q}_\ell)^* \otimes_{\mathbb{Q}_\ell} \omega_l$ canonically if $i+j = 2 \dim X$. As a special case, $H^0 \cong \mathbb{Q}_\ell$ with the trivial action.

5. If $K = \mathbb{C}$, then $H^i(X, \mathbb{Q}_\ell) = H^i(X(\mathbb{C}), \mathbb{Q}_\ell)$ where the right-hand side is, say, singular cohomology. This explains why (over $\mathbb{C}$, anyway) $H^i = 0$ for $i > 2 \dim X$. Note that combining this with point (2), we see that in characteristic zero we can compute the dimensions of $H^i(X, \mathbb{Q}_\ell)$ by computing cohomology over $\mathbb{C}$.

6. If A is a complete DVR with maximal ideal $\mathfrak{m} = (\pi)$. Let K be the fraction field of A and $k = A/\mathfrak{m}$. These rings provide a link between characteristic zero and characteristic p fields. Thus $\operatorname{Spec} A = \{\mathfrak{m}, (0)\}$; $\mathfrak{m}$ is closed, while the closure of (0) is the whole space. (0) is called a *generic* point because it generates $\operatorname{Spec} A$. If X is a proper, smooth scheme over $\operatorname{Spec} A$, write X_k for the fiber over $\mathfrak{m}$ and X_K for the fiber over (0). Then it can be shown that X_k (resp. X_K) is a proper and smooth variety over k (resp. K).

Theorem 42. *(Grothendieck) We have a commutative diagram*

$$\begin{array}{ccccccccc} & & & & H^i(X_K, \mathbb{Q}_\ell) & \xrightarrow{\cong} & H^i(X_k, \mathbb{Q}_\ell) & & \\ & & & & \circlearrowleft & & \circlearrowleft & & \\ 1 & \longrightarrow & I_K & \longrightarrow & G_K & \longrightarrow & G_k & \longrightarrow & 1 \end{array}$$

The argument is more difficult, but similar to that used for the corresponding theorem for the Tate modules. (Note that the map $G_K \to G_k$ arises from the fact that K is complete so that any place v of K has a unique extension to a place w of $L \supset K$).

Example 43. Let $E/\mathbb{Q}_p$ be an elliptic curve with good reduction at p and assume $p \neq l$. For example, $y^2 z = x^3 + axz^2 + bz^3$ for $a, b \in \mathbb{Z}_p$ with $\Delta \in \mathbb{Z}_p^*$. This equation defines a proper and smooth scheme $\mathbb{E}$ over $\operatorname{Spec} \mathbb{Z}_p$ since $a, b \in \mathbb{Z}_p$, and we get $\mathbb{E}_{\mathbb{Q}_p} = E, \mathbb{E}_{\mathbb{F}_p} = \tilde{E}$. Thus we can investigate $H^i(E)$ by investigating $H^i(\tilde{E})$.

Definition 44. Let V/K be an algebraic variety, proper and smooth, and K a nonarchimedean local field with ring of integers A. V has *good reduction* if there is a scheme X over $\operatorname{Spec} A$ proper and smooth such that $X_K \cong V$.

Theorem 45. *X/K has good reduction if and only if $H^i(X, \mathbb{Q}_\ell)$ is unramified.*

Proof. This is a diagram trace from the Grothendieck theorem above. □ how does this work?

Theorem 46. *Let E/K be an elliptic curve; then*

1. $\dim H^0(E, \mathbb{Q}_\ell) = \dim H^2(E, \mathbb{Q}_\ell) = 1, \dim H^1(E, \mathbb{Q}_\ell) = 2$.
2. *If $f, g : E' \to E$ are isogenies, we may define $f^*, g^* : H^1(E, \mathbb{Q}_\ell) \to H^1(E', \mathbb{Q}_\ell)$. Then $(f + g)^* = f^* + g^*$. (Note that addition on the left is addition on the elliptic curve, while addition on the right is addition in the vector space).*

Proof. (1): The statement is clear for H^0 and H^2 from the above basic properties. For H^1, assume first that $K = \mathbb{C}$. Then

$$\dim H^1(E, \mathbb{Q}_\ell) = \dim H^1(E(\mathbb{C}), \mathbb{Q}_\ell) = \dim H_1(E(\mathbb{C}), \mathbb{Q}_\ell) = \\ \dim H_1(E(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Q}_\ell = \dim(\pi_1(E(\mathbb{C})^{\mathrm{ab}}) \otimes \mathbb{Q}_\ell = 2$$

The final equality follows since $\pi_1(E(\mathbb{C}))^{\mathrm{ab}} \cong \mathbb{Z}^2$ since $E/\mathbb{C}$ is a torus.

Next assume there is some field morphism $\sigma : K \to \mathbb{C}$ (which is then an embedding). Then by property (2), $H^1(E_K, \mathbb{Q}_\ell) \cong H^1(E_{\mathbb{C}}, \mathbb{Q}_\ell)$ which has dimension 2.

Next assume $\operatorname{char} K = 0$ is an arbitrary field; then $E/K : y^2 = x^3 + ax + b$ for $a, b \in K$. Write $K_0 = \mathbb{Q}(a, b)$; then E is defined over K_0 and (again by property 2) $H^1(E_0, \mathbb{Q}_\ell) = H^1(E, \mathbb{Q}_\ell)$. But K_0 is embeddable into $\mathbb{C}$ regardless of whether a, b are algebraic or transcendental over $\mathbb{C}$.

Finally, let $\operatorname{char} K = p$; call it k in what follows, and call E $\tilde{E}$ as well.. Assume k is finite with characteristic $\neq 2, 3$ for simplicity. (In general, what follows can be done for any perfect k, and for the general case, one can embed any field into its perfect closure). Thus $k = \mathbb{F}_q$ for $q = p^n$. Let K be the unique unramified extension of degree n of $\mathbb{Q}_p$ with ring of integers A and maximal ideal $\mathfrak{m}$; then $A/\mathfrak{m} = \mathbb{F}_q \cong k$. Then $\tilde{E}/k : y^2 = x^3 + \bar{a}x + \bar{b}$ for $\bar{a}, \bar{b} \in k$. Choose $a, b \in K$ such that $\bar{a} \cong a \mod \mathfrak{m}, \bar{b} \cong b \mod \mathfrak{m}$, and define $E/K : y^2 = x^3 + ax + b$. Then E has good reduction, and $\tilde{E}$ is its reduction. But then $H^1(E, \mathbb{Q}_\ell) = H^1(\tilde{E}, \mathbb{Q}_\ell)$ by Grothendieck's theorem and we are done by the previous cases.

(This argument is useful in other settings as well: for example, the Cayley-Hamilton theorem may be proved relatively easily over $\mathbb{C}$; an argument similar to that above can be used to prove it for an arbitrary field.)

(2): (Sketch) Define $m : E \times E \to E$ to be multiplication; then

$$m^* : H^1(E, \mathbb{Q}_\ell) \to H^1(E \times E, \mathbb{Q}_\ell) = H^1(E, \mathbb{Q}_\ell) \otimes H^0(E, \mathbb{Q}_\ell) + H^0(E, \mathbb{Q}_\ell) \otimes H^1(E, \mathbb{Q}_\ell) \\ = H^1(E, \mathbb{Q}_\ell) + H^1(E, \mathbb{Q}_\ell)$$

is the diagonal map and $f + g = m \circ (f, g)$. We can then prove equality again by starting over $\mathbb{C}$. $\square$

Remark 47. All "interesting" Galois representations come from étale cohomology. We can't get all Galois representations in this way because there are only countably many varieties/schemes over $\mathbb{Q}$ and, by a homework exercise, uncountably many Galois representations (even of dimension one).

3.2 Lefshetz Fixed Point Theorem from Differential Geometry

Let X be a compact, orientable manifold, $f : X \to X$ be $\mathcal{C}^\infty$ and $\dim X = n$.

Definition 48. A *fixed point* for f is $x \in X$ such that $f(x) = x$. A fixed point for f is **non-critical** if $df_x - Id : T_x X \to T_x X$ is invertible. In this case, define $m_x := \operatorname{sgn}(\det(df_x - Id))$; this tells us whether f preserves or reverses orientation near x.

Theorem 49 (Lefshetz Fixed Point or Trace Formula)**.** *Assume that f has only non-critical fixed points. Then*

$$\sum_{f(x)=x} m_x = \sum_{i=0}^{n} (-1)^i tr(f^*(H^i(X, \mathbb{C})))$$

where the you can use your favourite topologically defined cohomology: de Rham, singular...

Note that:

- The LHS is a geometric condition, while the RHS is a cohomological condition.
- The left hand side is a finite sum since non-critical fixed points are isolated and X is compact.
- There is a more general formula when f simply has isolated fixed points (critical or non).
- For a proof see Milnor's Topology from a Differential Viewpoint.

Not clear why the LHS is a finite sum: "if an accumulation point, then in fact $df_x \sim Id$"

Example 50. $X = S^2$ and let $f : X \to X$ be homotopic to the identity. Then f has a fixed point. Proof: if f has no fixed point then the left hand side, being an empty sum, is 0. So since $f^* = id^*$,

$$0 = \sum_{i=0}^{2} (-1)^i \operatorname{tr}(id^* H^i(S^2, \mathbb{C})) = \chi(S^2) = 2$$

a contradiction. A corollary is the hairy ball theorem: any vector field on S^2 has a zero (because you can integrate it, and the map obtained is homotopic to the identity).

Theorem 51 (Lefshetz-Grothendieck Fixed Point or Trace Formula, EGA4)**.** *X/K proper and smooth and K algebraically closed (but this is not a real assumption since this is a geometric statement) and $f : X \to X$ a K-morphism. Assume that all fixed points of f in $X(K)$ are non-critical (same definition as before, reinterpreted in the algebraic setting). Then*

$$\#\textit{fixed points of } f = \sum_{i=0}^{2n} (-1)^i \operatorname{tr}(f^*(H^i(X, \mathbb{Q}_\ell)))$$

for $\ell \neq \operatorname{char} K$ and the H^i is étale cohomology.

(We dropped the sign because varieties are all canonically oriented; the sign is 1 because it's the real determinant of a complex matrix, which is always positive.)

This is a very powerful theorem and is used in odd ways:

Example 52. Let $X/\mathbb{F}_q$. Then we have a Frobenius map, $F : \bar{X} \to \bar{X}$ given (in affine charts) by $(a_0, \ldots, a_n) \mapsto (a_0^q, \ldots, a_n^q)$. Don't worry, these glue together well. Then the fixed points of F^n on $\bar{X}(\bar{\mathbb{F}}_q)$ are $X(\mathbb{F}_{q^n})$. Also, F has only non-critical fixed points because F^* is zero on the tangent space. Therefore

$$\#X(\mathbb{F}_{q^n}) = \sum_{i=0}^{2n} (-1)^i \operatorname{tr}(F^{n*} H^i(X, \mathbb{Q}_\ell))$$

Note the following subtlety: the above is the geometric Frobenius. There is also an arithmetic Frobenius which is what we've talked about before: $\mathrm{Frob} \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. These are not the same; in fact, they're not even really comparable objects. However:

Lemma 53. *The action of F^* on $H^i(\bar{X}, \mathbb{Q}_\ell)$ is the action of Frob^{-1} on $H^i(X, \mathbb{Q}_\ell)$ and these two H^i are equal as vector spaces.*

3.3 The Weil Conjecture

Theorem 54 (Weil Conjecture, Deligne '73)**.** *$X/\mathbb{F}_q$ proper and smooth. Then 1) the eigenvalues of F^* acting on $H^i(X, \mathbb{Q}_\ell)$ are algebraic numbers α such that for every embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}$, $|\alpha|_{\mathbb{C}} = q^{i/2}$ and 2) these eigenvalues are independent of ℓ.*

Note:

- That the eigenvalues are algebraic is really saying something; a priori we only know that they're in $\mathbb{Q}_\ell$.
- Also, the fact that they're independent of ℓ doesn't even make sense without the fact that they're algebraic; elements of $\mathbb{Q}_\ell$ and $\mathbb{Q}_p$ aren't comparable if $\ell \neq p$. Independence can be easily derived from statement 1).
- The history: Hasse proved this for elliptic curves, Weil proved this for curves of genus g and made the general conjecture. Then Serre and Grothendieck worked on this, laying foundational work. Then Deligne proved it for general varieties (or schemes i guess).
- The condition on α is pretty darn restrictive.

Corollary 55. *Let $X/\mathbb{F}_q$ proper and smooth, geometrically connected, of dimension d. Then*

$$\#X(\mathbb{F}_{q^n}) = q^{nd} + O(q^{nd-n/2})$$

Proof.

$$\#X(\mathbb{F}_{q^n}) = \sum_{i=0}^{2d}(-1)^i \operatorname{tr}(F^{n*}H^i) = \operatorname{tr}(F^{n*}H^{2d}) + \sum_{i=0}^{2d-1}(-1)^i \operatorname{tr}(F^{n*}H^i)$$

and by the Lefshetz Formula

$$\operatorname{tr}(F^{n*}H^{2d}) = \operatorname{tr}(\mathrm{Frob}^{-n}\, H^{2d} = \omega_\ell^{-d}(\mathrm{Frob}^{-n}) = \omega_\ell^d(\mathrm{Frob}^n) = q^{nd}$$

For the other part of the sum we have, from Deligne,

$$\operatorname{tr}(F^{n*}H^i) = \sum_{j=1}^{\dim H^i} \alpha_{i,j}^n \qquad \text{so} \qquad \left|\operatorname{tr}(F^{n*}H^i)\right| \leq (\dim H^i)q^{ni/2}$$

and the largest i is $2d-1$. Taking the sum we have what we want. □

Example 56. What is the étale cohomology of $\mathbb{P}^d(\mathbb{F}_q)$?
Answer

$$\#\mathbb{P}^d(\mathbb{F}_{q^n}) = \frac{q^{n(d+1)}-1}{q^n-1} = q^{nd} + q^{n(d-1)} + \cdots + q^n + 1 = \sum_{i=0}^{2d}(-1)^i tr(F^{n*}H^i) = \sum_{i=0}^{2d}(-1)^i \sum_{j=1}^{\dim H^i} \alpha_{i,j}^n$$

This is partial, and will be completed as an exercise. But we're basically done by the uniqueness of representations of numbers in base q. So we get the (already known) result:

$$\dim H^i(\mathbb{P}^d(\mathbb{F}_{q^n})) = \begin{cases} 1 & i \text{ even} \\ 0 & i \text{ odd} \end{cases}$$

Let $X/\mathbb{F}_q$ be a proper and smooth variety. Then $F^* : H^i(\bar{X}, \mathbb{Q}_\ell) \to H^i(\bar{X}, \mathbb{Q}_\ell)$ has eigenvalues $\alpha_{i,j}$ with $j = 1, \ldots, \dim H^i$ that are algebraic numbers, independent of ℓ and $|\sigma(\alpha_{i,j})|_{\mathbb{C}} = q^{i/2}$ where σ is any embedding of $\mathbb{Q}(\alpha_{i,j})$ into $\mathbb{C}$. It is not known that F^* is semisimple (this is a conjecture still) ie, that we have the right number of eigenvalues; here we count the eigenvalues with multiplicities.

Corollary 57. *(Deligne) Under the same hypotheses, the characteristic polynomial of F^* acting on $H^i(\bar{X}, \mathbb{Q}_\ell)$ is in $\mathbb{Z}[x]$ and is independent of ℓ and has roots with $|\cdot| = q^{i/2}$.*

Proof omitted, ('because it's elementary'), but he urges us to read the first few pages of Deligne's paper: La Conjecture de Weil, IHES '73. (see numdam.org) The argument uses the ζ function of a variety over $\mathbb{Q}$.

Conjecture 58. F^* is semisimple (diagonalizable over $\bar{\mathbb{Q}}_\ell$) on $H^i(\bar{X}, \mathbb{Q}_\ell)$. (known for abelian varieties and thus for elliptic curves.)

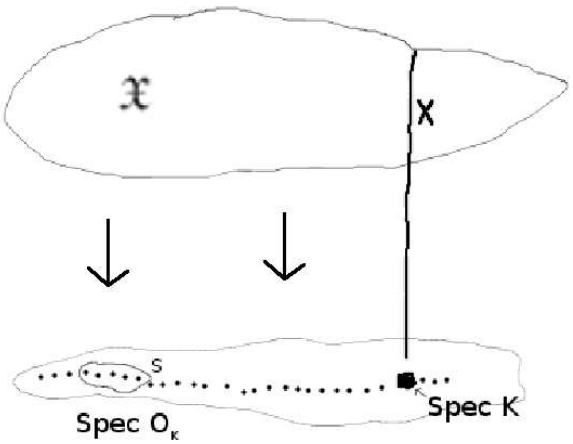
Now let X/K be proper and smooth variety over a number field. Notation: $\mathcal{O}_K$ ring of integers. If v is a place, K_v is the completion. If $v < \infty$, $\mathcal{O}_v \subset K_v$. $\mathfrak{m}_v \subset \mathcal{O}_v$. and $F_v := \mathcal{O}_v/\mathfrak{m}_v = F_{q_v}$ where $q_v = \#\mathcal{O}_v/\mathfrak{m}_v$.

Theorem 59. *The representation $H^i(X, \mathbb{Q}_\ell)$ of G_K is unramified outside a finite set of places S of K. If v is finite and not in S, then the characteristic polynomial of* Frob_v *acting on $H^i(X, \mathbb{Q}_\ell)$ is in $\mathbb{Q}[x]$, is independent of ℓ and has roots of absolute value $q_v^{-i/2}$.*

Proof. Since X is proper (projective) over K there exists a scheme $\mathfrak{X}$ proper over $\operatorname{Spec} \mathcal{O}_K$ and

$$\mathfrak{X} \times_{\operatorname{Spec} \mathcal{O}_K} \operatorname{Spec} K = X$$

(X is projective if it sits inside $\mathbb{P}^d_K$ and X is defined by some equations $P_0, \ldots, P_r = 0$ with $P_i \in K[x_0, \ldots, x_d]$ and clearing denominators we can get $P_i \in \mathcal{O}_K[x_0, ..., x_d]$) We don't say that this 'model' is unique – (there are many such models, but at least there is one. $\mathfrak{X}$ is smooth over $\operatorname{Spec} \mathcal{O}_K \setminus S$ where S is a finite set of points in $\operatorname{Spec} \mathcal{O}_K$.



To see this, note that smoothness is an open property, so $\mathcal{X}$ is smooth over an open set $\operatorname{Spec} \mathcal{O}_K$, and thus from the topology of $\operatorname{Spec} \mathcal{O}_K$, it has a finite set of non-smoothness; we can remove these by adding them to S.

Now let v be a prime of K not in S.

$\mathfrak{X} \otimes_{\operatorname{Spec} \mathcal{O}_K} \operatorname{Spec} \mathcal{O}_v =: \mathfrak{X}_v$ proper and smooth over $\operatorname{Spec} \mathcal{O}_v$ (two points).

Recall: $H^i(X \times K_v, \mathbb{Q}_\ell) \cong H^i(X \times \operatorname{Spec} F_v, \mathbb{Q}_\ell)$ and you have compatible actions of $Gal(\bar{K}_v/K_v)$ on the left, and $Gal(\bar{F}_v/F_v)$ on the right (and the kernel is I_v) and Frob_v a lift of Frob in $Gal(F_v)$ (since I_v acts trivially).

Frob_v acts on $H^i(X \times K_v, \mathbb{Q}_\ell) = H^i(X, \mathbb{Q}_\ell)$ and Frob acts on $H^i(X \times \operatorname{Spec} F_v, \mathbb{Q}_\ell)$ as $(F^*)^{-1}$. □

Conjecture 60. $H^i(X, \mathbb{Q}_\ell)$ is absolutely semisimple as a representation of G_K. (follows from Hodge conjecture) (could be semisimple, but not semisimple over $\bar{\mathbb{Q}}_\ell$)

Definition 61. Let ρ be a representation of G_K over L finite over $\mathbb{Q}_\ell$. We say that ρ is *algebraic over a number field* $L_0 \subset L$ if: ρ is unramified almost everywhere and $\rho(\mathrm{Frob}_v)$ has characteristic polynomial in L_0 for almost all v.

A *q-Weil number of weight i*, where $q = p^k$, $i \in \mathbb{Z}$, is an algebraic number α such that $|\sigma(\alpha)| = q^{i/2}$ for all $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$.

If ρ is a representation of G_K that is algebraic over some number field, then we say that ρ is of *weight i* if $\rho(\mathrm{Frob}_v)$ has eigenvalues that are q_v-Weil numbers of weight $-i$ for almost all v.

Remark 62. • A priori there is no reason for a representation to have a weight.
• So the theorem just says that $H^i(X, \mathbb{Q}_\ell)$ is algebraic over $\mathbb{Q}$ of weight i.

Example 63. ω_ℓ, the cyclotomic character. It is algebraic over $\mathbb{Q}$, of weight -2. (four possible conventions: could be $1, -1, 2, -2$)

Definition 64. A representation ρ of G_K over $\mathbb{Q}_\ell$ is **geometric** if there exists a $k \in \mathbb{Z}$, such that $\rho \otimes \omega_\ell^k$ is a subquotient of some $H^i(X, \mathbb{Q}_\ell)$ for some X proper and smooth variety over K.

The point of the rest of this class is to figure out when we can say a representation is geometric. If we didn't allow the 'twist' by ω_ℓ we could say that a necessary condition is positive weight, but it's much better to allow the twist so that we get a category which is stable under the operations of taking duals and tensor products.

Cyclotomic character is not positive weight (so not 'geometric' with the naïve notion of geometric (without the twist)): but it's the dual of a (naïve) geometric: $H^2(\mathbb{P}^1, \mathbb{Q}_\ell)$ has G_K acting by ω_ℓ^{-1}.

Exercise: dual and tensor product of geometric representations are geometric.

Theorem 65. *E/K elliptic curve over number field. Then $V_\ell(E)$ is isomorphic to $H^1(E, \mathbb{Q}_\ell) \otimes \omega_\ell$ and to the dual of first cohomology: $H^1(E, \mathbb{Q}_\ell)^*$. (These two are isomorphic by Poincaré duality).*

Proof. It is enough to prove that Frob_v has the same trace on $V_\ell(E)$ as on $H^1(E, \mathbb{Q}_\ell)^*$ for almost all v. For almost all p, $\mathrm{tr}(\mathrm{Frob}_p|_{V_\ell(E)}) = \#\tilde{E}_p(\mathbb{F}_p) - 1 - p$ and $\mathrm{tr}(\mathrm{Frob}_p|_{H^1(E)^*}) = \mathrm{tr}(F^*|_{H^1(E)}) = \#\tilde{E}_p(\mathbb{F}_p) - 1 - p$ by Lefshetz fixed point thm. □

Trivial representation is geometric: take a point and the H^0 (or any connected variety).

So when are representations geometric?

Having a weight, being algebraic are necessary..but it's not even a conjecture that it's sufficient. (There are some other notions of 'algebraic' that replace our simple notion. I think he said that there's some conjecture about that being sufficient.)

Here's another condition: 'being in a family': should have other ℓ-adic representations 'related' to it (from other primes...)

Question: Suppose $H^i(X, \mathbb{Q}_\ell)$ is reducible. Is $H^i(X, \mathbb{Q}_{\ell'})$ reducible? This is not known.
Motivic philosophy: Yes. Because there's (ATC: here 'is' should be read as 'should be') an object $M^i(X)$ in some crazy category of motives $\mathfrak{M}$ so that we have $X \to M^i(X) \to H^i(X, \mathbb{Q}_\ell)$ the latter maps being 'realization functors' of which there should be one for each prime and **moreover** these realization functors are fully faithful.

The things standing in the way of the theory of motives are the 'hard Lefshetz conjecture' and the Hodge conjecture.

4 Hecke Characters

As usual, we let K be a number field, v a place of K, K_v the completion, $\mathcal{O}_v$ the ring of integers in K_v with (for v finite) maximal ideal $\mathfrak{m}_v$ and uniformizer π_v; we denote by k_v the residue field $\mathcal{O}_v/\mathfrak{m}_v$. For v finite, if $v \mid p$, then $|k_v| = q_v$ and $q_v = p^r$.

We also write $\mathbb{A}_K = \mathbb{A}_{K,f} \times \mathbb{A}_{K,\infty}$ and similarly $\mathbb{A}_K^* = \mathbb{A}_{K,f}^* \times \mathbb{A}_{K,\infty}^*$, where the subscript K, f means the finite places and K, ∞ the infinite places. Note that $\mathbb{A}_{K,\infty}^*$ is a product of copies of $\mathbb{R}^*$ and $\mathbb{C}^*$; as before we denote by $\mathbb{A}_{K,\infty}^{*,0}$ the component of the neutral element in $\mathbb{A}_{K,\infty}^*$; this is a product of copies of $\mathbb{R}_+^*$ and $\mathbb{C}^*$.

Class Field Theory tells us that

$$\mathbb{A}_K^*/K^*\mathbb{A}_{K,\infty}^{*,0} \xrightarrow[Art]{\cong} G_K^{\mathrm{ab}}$$

Definition 66. A *Hecke character* (or *grössencharacter*) of K is a continuous morphism $\chi : \mathbb{A}_K^* \to \mathbb{C}^*$ that is trivial on K^*.

Clearly an equivalent definition is that a Hecke character is a continuous morphism from $\mathbb{A}_K^*/K^* \to \mathbb{C}^*$.

If χ is a Hecke character and v a place of K, then $\chi_v = \chi\big|_{K_v^*}$ is a character of K_v^*; we may ask what such characters look like.

1. For v real, $\chi_v : \mathbb{R}^* \to \mathbb{C}^*$, then

   $$\chi_v(x) = \operatorname{sgn}(x)^\epsilon |x|^c, \quad c \in \mathbb{C}, \epsilon \in \{0, 1\}$$

   and two such characters are distinct if they differ in either c or ϵ. Why? $\mathbb{R}^* \cong \{\pm 1\} \times \mathbb{R}_+^*$ via $x \mapsto (\operatorname{sgn} x, |x|)$. Maps $\{\operatorname{sgn} x\} \to \mathbb{C}^*$ are clearly of the form $\operatorname{sgn}(x)^\epsilon$; the second part follows from

   Lemma 67. *A continuous morphism $\mathbb{R}_+^* \to \mathbb{C}^*$ is of the form $x \mapsto x^c$ for some $c \in \mathbb{C}$.*

   Proof. Exercise. Follows from the fact that $\mathbb{C}^* \cong \mathbb{R}_+^* \times S^1$. □

2. For v complex, $\chi_v : \mathbb{C}^* \to \mathbb{C}^*$; in this case,

   $$\chi_v(z) = z^n |z|^c, \quad n \in \mathbb{Z}, c \in \mathbb{C}$$

   This follows since $\mathbb{C}^* \cong \mathbb{R}_+^* \times S^1$ via $z \mapsto \left(|z|, \frac{z}{|z|}\right)$; a character of $\mathbb{R}_+^*$ is of the form $|z| \mapsto |z|^c$, and a character of S^1 must have image in S^1 since the image of S^1 is a compact subgroup, so it must be of the form $z \mapsto z^n$.

3. If v is a finite place, the form of $\chi_v : K_v^* \to \mathbb{C}^*$ is left as an exercise.

Definition 68. For v finite, χ_v is *unramified* if $\chi_v(\mathcal{O}_v^*) = 1$, which is equivalent to $\chi_v = |\cdot|^c$ for some $c \in \mathbb{C}$.

These two definitions are equivalent since $|\cdot| \cong \mathbb{R}_+^*$; use the previous result.

Lemma 69. *If $\chi : \mathbb{A}_K^* \to \mathbb{C}^*$ is any character (not necessarily a Hecke character), then χ_v is unramified for almost all v.*

Proof. $\chi|_{\mathbb{A}_f^*}$ is continuous, and $\mathbb{A}_f^*$ has a basis of neighborhoods of 1 consisting of subgroups of the form

$$U = \prod_v U_v, \quad U_v \subset \mathcal{O}_v^*, U_v = \mathcal{O}_v^* \text{ for almost all } v$$

(this follows directly from the topology on the idèles). But we know that $\mathbb{C}^*$ has no arbitrarily small subgroups, so choose a neighborhood V of 1 containing no nontrivial subgroup; then $\chi^{-1}(1)$ contains some U and thus χ is trivial on that U. But this means that χ_v is trivial on $\mathcal{O}_v^*$ for almost all v. □

It follows that the product $\prod_v \chi_v(x_v)$ makes sense for $x \in \mathbb{A}_K^*$, so we recover $\chi(x)$ from the $\chi_v(x_v)$.

So arbitrary continuous characters look like products of characters on the completions. The Hecke property, however (i.e. triviality on K^*), is a global condition, and is arithmetically interesting.

Example 70. Characters of Artin type
Let $\psi : G_K \to \mathbb{C}^*$ be a continuous character. This must factor through G_K^{ab}, so we get a character

$$\chi = \psi \circ \text{Art} : \mathbb{A}_K^* \to G_K^{\text{ab}} \to \mathbb{C}^*$$

χ is then trivial on K^* since $G_K^{\text{ab}} \cong \mathbb{A}_K^*/K^*\mathbb{A}_{K,\infty}^{*,0}$, so that χ is a Hecke character. χ is also trivial on $\mathbb{A}_{K,\infty}^{*,0}$. Such a Hecke character is said to be of *Artin type*.

Lemma 71. *Let χ be a Hecke character. TFAE:*

1. *χ is of Artin type.*
2. *χ has finite image.*
3. $\chi_v = \begin{cases} (\operatorname{sgn} x)^\epsilon & v \text{ real}, \epsilon \in \{0,1\} \\ 1 & v \text{ complex} \end{cases}$

Proof. (1) ⇒ (2) is obvious since if χ is of Artin type, it is an Artin representation and thus has finite image. (2) ⇒ (3) is also clear, since χ_v has finite image for all v; from the form of representations of $\mathbb{R}^*$ above we see that $c = 0$; from the form of representations of $\mathbb{C}^*$ we see that $n, c = 0$.

(3) ⇒ (1): Since χ_v is trivial on $\mathbb{R}_+^*$ and $\mathbb{C}^*$, it is trivial on $\mathbb{A}_{K,\infty}^{*,0}$, and trivial on K^* since it is a Hecke character, thus it is a character of G_K^{ab} and is of Artin type. □

Example 72. The Idelic Norm
We define a norm on $\mathbb{A}_K^*$ by

$$|\cdot| = \prod_v |\cdot|_v$$

where $|\cdot|_v$ is the *normalized absolute value* on K_v^*:

- If $K_v^* = \mathbb{Q}_p^*$, define $|p|_p = p^{-1}$.
- If K_v is a finite extension of $\mathbb{Q}_p$, define $|\cdot|_v = \left|N_{K/\mathbb{Q}_p}(\cdot)\right|_p$.
- If $K_v = \mathbb{R}$, define $|\cdot|_{\mathbb{R}}$ to be the usual real absolute value.
- If $K_v = \mathbb{C}$, define $|\cdot|_{\mathbb{C}} = \left|N_{\mathbb{C}/\mathbb{R}}(\cdot)\right|_{\mathbb{R}}$, i.e. $|x|_{\mathbb{C}} = x\bar{x}$. Note that this is not really an absolute value, but that fact doesn't matter and we will ignore it. It is, however, a character $\mathbb{C}^* \to \mathbb{C}^*$.

Note that $|\cdot| : \mathbb{A}_K^* \to \mathbb{C}^*$ is trivial on K^* by the product formula, so this is a Hecke character with values in $\mathbb{R}_+^*$; more generally, for $c \in \mathbb{C}$, $|\cdot|^c$ is a Hecke character with values in $\mathbb{C}^*$.

Example 73. The Hecke character associated to an Elliptic curve
Let E/K be an elliptic curve with K an imaginary quadratic extension of $\mathbb{Q}$, and assume E has complex multiplication by K. Then the main theorem of complex multiplication (see Silverman's Advanced Topics) is

Theorem 74. *There is a unique Hecke character $\chi_E : \mathbb{A}_K^* \to \mathbb{C}^*$ such that*

$$\chi_E(\pi_v) = \mathrm{Frob}_{\tilde{E}_v} \in K^* \subset \mathbb{C}^*$$

for every finite place v at which E has good reduction (note that this is almost all v), and such that

$$\chi_E(\infty) : \mathbb{C}^* \to \mathbb{C}^* : z \mapsto z$$

The proof is difficult; a very brief outline is as follows. $\mathrm{Frob}_{\tilde{E}_v}$ is an endomorphism of $\tilde{E}_v$ commuting with the action of K in $\mathrm{End}_{k_v}(\tilde{E}_v) \otimes \mathbb{Q}$, so lies in the centralizer of K. But K is its own centralizer, so that $\mathrm{Frob} \in K^*$.

4.1 Algebraic Hecke Characters

Definition 75. (A. Weil) A Hecke character is called *algebraic* if

$$\chi_v(x) = \begin{cases} \mathrm{sgn}(x)^{\epsilon_v} |x|^{n_v}, \quad \epsilon_v \in \{0,1\}, n_v \in \mathbb{Z} & v \text{ real} \\ x^{a_v} \bar{x}^{b_v}, \quad a_v, b_v \in \mathbb{Z} & v \text{ complex} \end{cases}$$

For example, a Hecke character of Artin type is algebraic since $n_v = 0, a_v, b_v = 0$ for all v. The idelic norm is algebraic, and $|\cdot|^c$ is algebraic if and only if $c \in \mathbb{Z}$. Finally, χ_E is algebraic.

Note by the way that if v is real then $K_v^* \cong \mathbb{R}^*$ canonically, while if v is complex, the isomorphism is not canonical, and the characters χ_v associated with the conjugate embeddings are themselves conjugate.

Theorem 76. *If χ is algebraic, then there is $w \in \mathbb{Z}$ such that for every infinite place v,*

$$w = \begin{cases} 2n_v & v \textit{ real} \\ a_v + b_v & v \textit{ complex} \end{cases}$$

Thus all the n_v are equal for all real places, and there is a strong relation among the n_v, a_v, and b_v.

The proof uses the following lemma:

Lemma 77. *If χ is any character, then there is a subgroup $\Gamma \subset \mathcal{O}_K^*$ of finite index such that for $x \in \Gamma$, $\chi_f(x_f) = 1$ (we write χ_f for $\chi|_{\mathbb{A}_f^*}$).*

Proof. We have $\mathcal{O}_K^* \subset \prod_{v \text{ finite}} \mathcal{O}_v^* \subset \mathbb{A}_f^*$. As before, we know that $\chi|_{\mathbb{A}_f^*}$ is trivial on some $U = \prod_v U_v \subset \prod_v \mathcal{O}_v^*$ (where the product is over all finite places). But $\prod_v \mathcal{O}_v^*$ is compact and U is open, so U is of finite index. Let $\Gamma = U \cap \mathcal{O}_K^*$; this is then of finite index and $\chi_f(x_f)$ is trivial for $x \in \Gamma$. $\square$

Proof. (of theorem) It suffices to prove the result for elements of Γ, since the n_v, a_v, b_v depend only on v, not on $x \in \mathbb{A}_K^*$. Now, since $\Gamma \subset K^*$, we have $\chi(\Gamma) = 1$, and $\chi_f(x_f) = 1$ by construction of Γ, so that for $x \in \Gamma$,

$$1 = \chi(x) = \chi_f(x_f) \cdot \prod_{v|\infty} \chi_v(x_v) = \prod_{v|\infty} \chi_v(x_v) = \prod_{v \text{ real}} \mathrm{sgn}(x_v)^{\epsilon_v} |x_v|^{n_v} \cdot \prod_{v \text{ complex}} x_v^{a_v} \bar{x}_v^{b_v}$$

so that, taking logs,

$$0 = \sum_{v \text{ real}} n_v \log|x_v| + \sum_{v \text{ complex}} (a_v + b_v) \log|x_v|$$

for all $x \in \Gamma$.

Now, the Dirichlet Unit Theorem says that the log map

$$L : \mathcal{O}_K^* \to \mathbb{R}^{r+s} : x \mapsto (\log|x_v|)_v \text{ for } v \mid \infty$$

has image $L(\mathcal{O}_K^*)$ in the hyperplane $\sum_{v \text{ real}} y_v + 2\sum_{v \text{ complex}} y_v = 0$, so $L(\Gamma)$ has image in that hyperplane as well. Thus the form

$$\sum_{v \text{ real}} n_v \log|x_v| + \sum_{v \text{ complex}} (a_v + b_v) \log|x_v|$$

is trivial on $\ker(L|_\Gamma)$, so that it must be proportional to

$$\sum_{v \text{ real}} \log|x_v| + 2 \sum_{v \text{ complex}} \log|x_v|$$

and the result follows. □

Corollary 78. *If K is totally real and χ is an algebraic Hecke character, then $\chi = \alpha|\cdot|^n$ where α is a Hecke character of Artin type, $n \in \mathbb{Z}$, and $|\cdot|$ is the idelic norm.*

Proof. All the n_v are equal (to n). But then since K is totally real, there are no complex embeddings, so by Lemma **??**, $\chi|\cdot|^{-n}$ is Artin and we are done. □

Comment in class: Totally real fields have lots of units (the maximum rank, from DUT, of an extension of given degree); this corresponds to a small number of Hecke characters.

Corollary 79. *Let K be a number field and χ an algebraic Hecke character, w as in the theorem. Then $\chi\bar{\chi} = |\cdot|^w$.*

Proof. Let n'_v, a'_v, b'_v be associated to the character $\chi\bar{\chi}$. Clearly $n'_v = 2n_v = w$ for v real, while for v complex, $a'_v = b'_v = a_v + b_v = w$. Then $\chi\bar{\chi}|\cdot|^{-w}$ is of Artin type and takes values in $\mathbb{R}_+^*$ since $\chi\bar{\chi}$ and $|\cdot|$ do. But values of an Artin character are roots of unity, so $\chi\bar{\chi}|\cdot|^{-w} = 1$. □

Theorem 80. *Let χ be an algebraic Hecke character. Then there is a number field $L \subset \mathbb{C}$ with $\chi(\mathbb{A}_{K,f}^*) \subset L$. (Note: this really means a number field L and an embedding $L \subset \mathbb{C}$).*

This is a pretty surprising result, since $\mathbb{A}_{K,f}^*$ is a pretty big ring and there's a priori no reason to suppose that this would hold.

Proof. The idea of the proof is to note that K^* is almost dense in $\mathbb{A}_{K,f}^*$ and to compute the image of an element of K^* in $\mathbb{A}_{K,f}^*$, which is the inverse of the image of that element in $\mathbb{A}_{K,\infty}^*$.

If U is any open compact subgroup of $\mathbb{A}_{K,f}^*$ (i.e. a subgroup equal to $\mathcal{O}_v^*$ for almost all finite v), then since $\mathbb{A}_K^*/\mathbb{A}_{K,\infty}^* = \mathbb{A}_{K,f}^*$, we have

$$\mathbb{A}_K^*/K^*\mathbb{A}_{K,\infty}^*U = \mathbb{A}_{K,f}^*/K^*U$$

Any such U has finite index in $\prod_v \mathcal{O}_v^*$, so this quotient is finite, say of order m.

Now if we choose U to be a subgroup of $\mathbb{A}_{K,f}^*$ on which χ_f is trivial (as before, since $\mathbb{C}$ has no arbitrarily small nontrivial subgroups), then for any $x \in \mathbb{A}_{K,f}^*$ we may write

$$x = yrut, \quad y \in K^*, r \in \mathbb{A}_{K,\infty}^*, u \in U, t \text{ of finite order } \mid m$$

Then $\chi(y) = \chi(u) = 1$.

At the infinite places, $\chi_\infty(x) = 1, \chi_\infty(r) = r, \chi_\infty(u) = 1$ (since $x \in \mathbb{A}^*_{K,f}, r \in \mathbb{A}^*_{K,\infty}, \chi$ trivial on U, and $\chi_\infty(t)$ is again of finite order dividing m.

So if v is any infinite place, we have

$$r_v = y_v^{-1} t_v$$

where $r_v \in \mathbb{C}$, y_v^{-1} is in the normal closure of K (since any embedding of K is contained in its normal closure), and t_v is a root of unity in $\mathbb{Q}(\zeta_m)$. Let L be the compositum of the normal closure of K and $\mathbb{Q}(\zeta_m)$. Thus $r_v \in L$ for infinite places L.

Finally, $\chi(x) = \chi(r)\chi(t) = \chi_\infty(r)\chi(t) \in L$ since $\chi_\infty(r) = \prod_{v \text{ real}} \pm r_v^{n_v} \prod_{v \text{ complex}} r_v^{a_v} \bar{r}_v^{b_v}$. □

Now, if χ is a Hecke character of Artin type we have seen above that χ defines an Artin representation $G_K \to \mathbb{C}^*$ (or $G_K^{\text{ab}} \to \mathbb{C}^*$. Can we use other algebraic Hecke characters to define degree 1 representations of G_K^{ab}?

Theorem 81. *Let χ be an algebraic Hecke character. Assume $L \subset \mathbb{C}$ is a number field containing $\chi(\mathbb{A}^*_{K,f})$ and the normal closure of K. Let λ be a finite place of L with $\lambda \mid \ell$ for ℓ a rational prime. Then there is a unique continuous $\chi^\lambda : G_K \to L^*_\lambda$ unramified at every place v not dividing ℓ where χ is unramified, and such that $\chi^\lambda(\text{Frob}_v) \in L^*$ and $\chi^\lambda(\text{Frob}_v) = \chi(\pi_v)$.*

Note that $\chi(\pi_v)$ is in L by the way we have defined L together with the previous theorem, so that it makes sense to compare $\chi^\lambda(\text{Frob}_v)$ and $\chi(\pi_v)$.

For dimension 1 representations, Frob_v is the trace, and we have seen that the trace is an important invariant of any representation.

Definition 82. χ^λ is called the *λ-adic realization* of χ.

Proof. (of theorem): Uniqueness is clear, since χ^λ is determined by its image on each of the Frob_v's. Why is χ^λ determined as stated?

The idea of the existence proof is to transform χ to make trivial at the infinite places while keeping it trivial on K^*. Recall that

$$\chi_\infty(x) = \prod_{v \text{ real}} |x_v|^{n_v} \operatorname{sgn}(x_v)^{\epsilon_v} \prod_{v \text{ complex}} x_v^{a_v} \bar{x_v}^{b_v}$$

Define

$$\tau_\infty : \mathbb{A}^*_{K,\infty} \to \mathbb{C}^* : x \mapsto \prod_{v \text{ real}} x_v^{n_v} \prod_{v \text{ complex}} x_v^{a_v} \bar{x_v}^{b_v}$$

Note that $\chi_\infty = \tau_\infty$ on $\mathbb{A}^{*,0}_{K,\infty}$.

We will now need the following lemma, which is proved after the proof of the theorem:

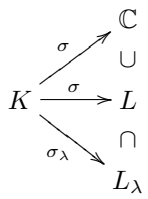
Lemma 83. *In this situation, there is an algebraic Hecke character $\tau_\lambda : (K \otimes \mathbb{Q}_\ell)^* = \prod_{v|\ell} K_v^* \to L^*_\lambda$ such that for $x \in K^*$, we have $\tau_\infty(x) = \tau_\lambda(x) \in L^*$ (again note that the comparison makes sense since $\tau_\infty(x)$ is in the normal closure of K, which is contained in L.*

Assuming the lemma, note that $\chi\tau_\infty^{-1}$ is trivial on $\mathbb{A}^{*,0}_{K,\infty}$ and takes values in L; then $\chi\tau_\infty^{-1}\tau_\lambda : \mathbb{A}^*_K \to L^*_\lambda$ is trivial both on K^* (since χ is and since by the lemma $\tau_\infty^{-1}\tau_\lambda$ is) and on $\mathbb{A}^{*,0}_{K,\infty}$ (since τ_λ is), so that

$$\chi^\lambda = (\chi\tau_\infty^{-1}\tau_\lambda) \circ Art^{-1} : G_K^{\text{ab}} \to L^*_\lambda$$

But $\chi^\lambda(\pi_v) = \chi(\pi_v)$ for $v \nmid \ell$, and the Artin map takes $\text{Frob}_v \mapsto \pi_v$. Finally, $\chi^\lambda = \chi$ for finite places not dividing ℓ. □

Proof. (of lemma): We have the following diagram:



For $x \in K^*$, claim

$$\tau_\infty(x) = \prod_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} \sigma(x)^{n_\sigma}, \quad n_\sigma \in \mathbb{Z}$$

For real embeddings, this is clear. Complex embeddings come in conjugate pairs; for these, if $\sigma(x) = x_v$, define $n_\sigma = a_v, n_{\bar{\sigma}} = b_v$.

We then define

$$\tau_\lambda : (K \otimes \mathbb{Q}_\ell)^* \to L_\lambda^*$$

by $\tau_\lambda = \prod_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} \sigma_\lambda^{n_\sigma}$ (note that σ_λ defines a morphism from $K \otimes \mathbb{Q}_\ell$ since L_λ is a $\mathbb{Q}_\ell$-algebra).

Then for $x \in K^*$, we have $\tau_\lambda(x) = \tau_\infty(x)$ since for $x \in K^*$, $\sigma_\lambda(x) = \sigma(x)$. □

What exactly is the action of τ_λ on x?

Corollary 84. *χ^λ is of weight $-w$.*

Proof. Start with $\chi\bar{\chi} = |\cdot|^w$. Then

$$\chi^\lambda(\mathrm{Frob}_v)\overline{\chi^\lambda(\mathrm{Frob}_v)} = \chi(\pi_v)\overline{\chi(\pi_v)} = |\pi_v|^w = q_v^{-w}$$ □

The proof of the theorem also shows that if $v \nmid \ell$ is a finite place of K then $\chi^\lambda|_{D_v} \circ Art_v = \chi_v$, even if χ is ramified. Note first that if $v \nmid \ell$ then χ is unramified at v if and only if χ^λ is unramified at v. If χ is unramified at v, then χ_v is trivial on $\mathcal{O}_v^*$, which maps surjectively to inertia, so that χ^λ is unramified at v. Now, $\chi^\lambda|_{D_v}$ $(I_v) = \chi^\lambda(I_v)$ is finite since χ on $\mathbb{A}_{K,f}^*$ is trivial on some finite index subgroup U of $\prod_{v \text{ finite}} \mathcal{O}_v^*$ so that χ_v is trivial on a finite index subgroup of $\mathcal{O}_v^*$.

This proof makes no sense to me and may be completely wrong.

Definition 85. A character $\eta : K_v^* \to L_\lambda^*$ is *locally algebraic* if $\eta(x) = \prod_{\sigma \in \mathrm{Hom}(K_v, L_\lambda)} \sigma(x)^{n_\sigma}$ for some $n_\sigma \in \mathbb{Z}$ for every x in some open subgroup of $\mathcal{O}_v^*$. Note that this definition has content only in the case where $v \mid \ell, \lambda \mid \ell$. A character $\tilde{\eta} : D_v \to L_\lambda^*$ is locally algebraic if $\tilde{\eta} \circ Art_v$ is locally algebraic.

Corollary 86. *If $v \mid \ell$, $\chi^\lambda|_{D_v}$ is locally algebraic.*

Proof. From the theorem, we have $\chi^\lambda \circ Art_K = \chi\tau_\infty^{-1}\tau_\lambda$, and τ_λ is nontrivial on places dividing ℓ. Now, on K_v^*, $v \mid \ell$ τ_∞^{-1} is trivial, and χ is trivial on some finite index subgroup of $\mathcal{O}_v^*$. Additionally, $\tau_\lambda(x)$ is of the required form since it is an algebraic Hecke character. □

Theorem 87. *Let K be a number field, L an ℓ-adic field, and $\tau : G_K \to L^*$ a continuous character of G_K. Assume τ is locally algebraic at all places $v \mid \ell$. Then up to finite extensions of L, τ is the λ-adic realization of an algebraic Hecke character.*

This means that the only condition for an ℓ-adic character to be a realization is that it be locally algebraic.

Proof. This is the same as the proofs of Theorems **??** and **??**. In the proof of Theorem **??**, since τ is locally algebraic, you can split it up into τ_∞ and τ_λ and run the argument backwards. Then show that $\mathrm{im}(\mathrm{Frob}_v)$ is in a number field. □

Theorem 88. *If $\tau : G_K \to L^*$ is as in the previous theorem, then the following are equivalent:*

1. *τ is geometric*
2. *τ is locally algebraic at all $v \mid \ell$*
3. *τ is the λ-adic realizaion of an algebraic Hecke character*

Note that we only define geometric characters over $\mathbb{Q}_\ell$, but a vector space over L is also a vector space over $\mathbb{Q}_\ell$.

Proof. (3) $\Rightarrow$ (2) is Theorem **??**.
(2) $\Rightarrow$ (3) is Theorem **??**.
(3) $\Rightarrow$ (1) is in the Exercises.
(1) $\Rightarrow$ (2) is Fontaine theory, which we will cover later, and is due primarily to Faltings. □

Example 89. Let $|\cdot|$ be the idelic norm. In this case $|\cdot|^\lambda = \omega_\ell^{-1}$ since their images on Frob_v are the same. Note that $\omega_\ell^{-1} : G_K \to \mathbb{Q}_\ell^*$ while $|\cdot|^\lambda : G_K \to L_\lambda^*$. However in this case we can take $L = \mathbb{Q}$ for the Hecke character (that is, the image of $|\cdot|^\lambda$ actually lies in $\mathbb{Q}_\ell^*$).

Example 90. Let E/K be an elliptic curve for K a quadratic imaginary field, and assume that E has CM by $\mathcal{O}_K$. Then CM theory shows that there is a map $E \mapsto \chi_E$ where χ_E is an algebraic Hecke character, and $\chi_E(\pi_v) = \mathrm{Frob}_v \in K^* \subset \mathbb{C}^*$; this is the geometric Frobenius. Again in this case we can take $L = K$. If λ is a place of L, then $\chi_E^\lambda : G_K \to L_\lambda^* = K_\lambda^*$. Then $V_\ell(E)$ is a G_K-module of dimension 2, so $V_\ell(E)$ is acted on by $\mathcal{O}_K$ where the action is given by CM (this is because $V_\ell(E)$ is the limit of ℓ^n-torsion). But $V_\ell(E)$ is a $\mathbb{Q}_\ell$-vector space, so it is acted on by $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, and the action of G_K commutes with this $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ structure since the isogeny is defined over K.

If ℓ is inert in K, then $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = K_\ell$ is a field, $V_\ell(E)$ has degree 1 over K_ℓ, and $G_K \hookrightarrow V_\ell(E)$ is a character $G_K \to K_\ell$; this is χ_E^ℓ.

If ℓ splits in $K = L$, say $\ell = \lambda\bar{\lambda}$, then $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = L_\lambda L_{\bar{\lambda}} \cong \mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Then $V_\ell(E)$ splits as a G_K module as $V_\ell(E) = V_\lambda(E) \oplus V_{\bar{\lambda}}(E)$; these are both of dimension 1 and G_K acts on each. (To see this, take the nilpotents in $K \otimes \mathbb{Q}_\ell$; these commute with the G_K action.) We thus get a character $G_K \to L_\lambda^*$; this is χ_E^λ.

5 Galois Representations of Local Fields, p-adic case - Fontaine Theory

We now consider the case where $p = \ell$ (the so-called p-adic theory). Thus assume that both K and L are finite extensions of $\mathbb{Q}_p$, and that $\rho : G_K \to GL_n(L)$ is a continuous representation.

Note that the critical observation in the proof of the monodromy theorem was that $\operatorname{im}\rho$ was finite since a map from a p-adic to an ℓ-adic group was trivial for $p \neq \ell$. This step obviously fails here, and in fact the result is false - not every representation is semi-stable. But it turns out that the semi-stable representations are the geometric representations (for a somewhat different definition of semi-stable), and thus these are still the interesting objects of study.

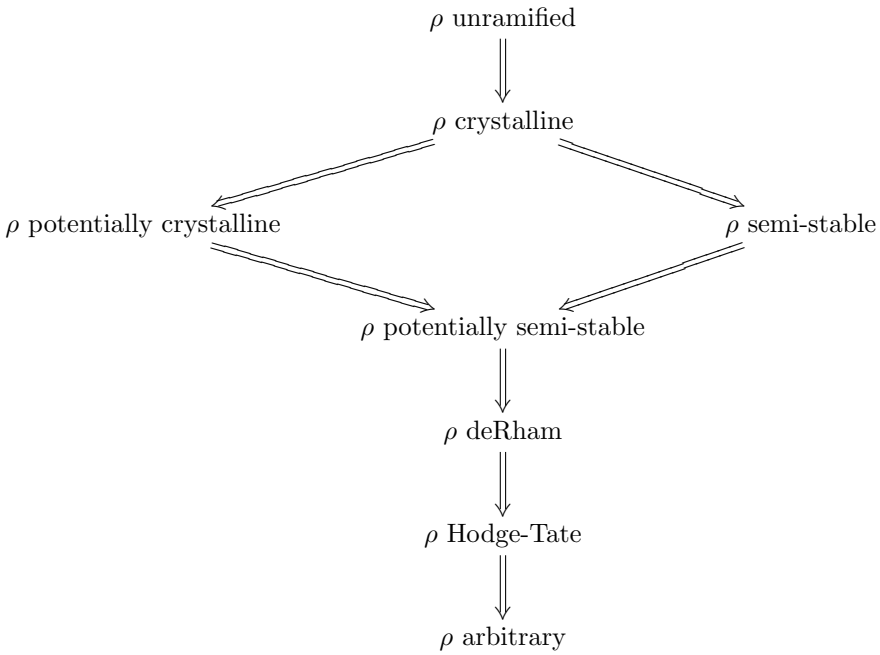
5.1 Overview

The condition that ρ be unramified is very strong in this case. For $p \neq \ell$, it was somewhat weaker since we already knew that wild inertia was trivial. For $p = \ell$, that is not the case. So it turns out that unramified is too strong a condition. For example, look at $\omega_\ell : G_K \to \mathbb{Q}_\ell^*$. If K is ℓ-adic, recall that $\omega_\ell : \mathcal{O}_K^* \to \mathbb{Q}_l^* : x \mapsto x^{-1}$, so that ω_ℓ is ramified since inertia is not trivial.

A property called *crystalline* takes the place of unramified. It is much weaker than unramified, but has the right degree of generality for the p-adic theory. In addition, we get a notion of potentially crystalline, similar to potentially unramified.

A notion of semi-stability exists as well, although the definition is different than in the ℓ-adic case.

The following set of implications is easy to see once the definitions are made; this is similar to the picture in the ℓ-adic case:



Two long-standing conjectures of Fontaine, since proved, are:

Conjecture 91. (proved by Berger): ρ is deRham if and only if ρ is potentially semi-stable.

This is the p-adic analogue of Grothendieck's monodromy theorem.

Conjecture 92. (proved by Faltings)

- If X is a proper and smooth variety over K, then $H^i(X, \mathbb{Q}_p)$ with its G_K action is deRham.
- If X has good reduction, then $H^i(X, \mathbb{Q}_p)$ is crystalline.

Note that in the ℓ-adic theory, if X has good reduction, then $H^i(X, \mathbb{Q}_\ell)$ is unramified. This argument does not work here, but we do get crystalline instead.

It follows that deRham representations are the ones that come from geometry. There are representations that are not deRham (unlike the analogous case in the ℓ-adic theory), but those are less interesting.

One approach to analyzing these representations might be to try to analyze the wild inertia. It turns out that this is just too complicated. Instead, Fontaine defined rings B_* that are also $\mathbb{Q}_p$-algebras with Galois actions such that if $\dim(B_* \otimes V)^{G_K} = \dim V$ (here $\overset{G}{K}$ means the G_K-invariant subspace), then V has the $*$ property, for $*$ in {crystalline, semi-stable, deRham, Hodge-Tate} (thus there are four different rings, $B_{\text{crys}}, B_{\text{ss}}, B_{\text{deRham}}, B_{\text{H-T}}$).

5.2 Fontaine's formalism

Let F be any field, G a group, and denote by $\text{Rep}_F(G)$ the category of finite-dimensional representations of G over F.

Definition 93. A (F, G)-*regular ring* B is an F-algebra B (i.e. a ring containing F) that is a commutative domain with unity, together with a G-action preserving the F-algebra structure (i.e. such that the G-action is trivial on F), such that

- $B^G = \text{Frac}(B)^G$, where $\cdot^G$ means the elements invariant under the G-action. Note that $\subset$ always holds. Here the G-action on $\text{Frac}(B)$ is the quotient of the actions on the numerator and denominator.
- For all $0 \neq b \in B$, if Fb is G-stable, then $b \in B^*$.

If B is (F, G)-regular, we will write $E = B^G = \text{Frac}(B)^G$. E is a field since $\text{Frac}(B)$ is, and $E \supset F$ since $B^G \supset F$. It may or may not be finite over F. Thus B is an E-algebra as well as a F-algebra.

Note that if B is a field, then the conditions in the definition always hold. Many of the B we will consider are in fact fields, although B_{crys} is not.

Fix a (F, G)-regular ring B. For $V \in \text{Rep}_F(G)$ set $D_B(V) = (V \otimes_F B)^G$ (here the action of G on $V \otimes_F B$ is given by $g(v \otimes b) = gv \otimes gb$, in contrast to the situation where B is simply an extension of F and the tensor product is extension of scalars). If B has a rich enough G-action, we can use the tensor product to detect properties of V.

Lemma 94. *D_B is a left-exact functor from $\text{Rep}_F(G)$ to Vec_E (the category of E-vector spaces).*

Proof. Since $B^G = E$, it is clear that $D_B(V)$ can be multiplied by elements of E and that the result is still G-invariant. Thus $D_B(V)$ is an E-vector space. D_B is functorial since if $V \to V'$ is a map of representations, then $V \otimes_F B \to V' \otimes_F B$ is compatible with the G-action. Finally, to see that the functor is left exact, if

$$0 \to V_1 \to V_2 \to V_3 \to 0$$

is an exact sequence in $\mathrm{Rep}_F(G)$, then since F is a field,

$$0 \to V_1 \otimes_F B \to V_2 \otimes_F B \to V_3 \otimes_F B \to 0$$

is exact as well. Now consider

$$0 \to (V_1 \otimes_F B)^G \to (V_2 \otimes_F B)^G \to (V_3 \otimes_F B)^G$$

and exactness is clear. □

We now define $\alpha_V : B \otimes_E D_B(V) \to B \otimes_F V$ by

$$B \otimes_E D_B(V) \hookrightarrow B \otimes_E (B \otimes_F V) \xrightarrow{\cong} (B \otimes_E B) \otimes_F V \xrightarrow{x \otimes y \mapsto xy} B \otimes_F V$$

Note that α_V is B-linear.

Proposition 95. *α_V is compatible with the G-action, where the G-action on $B \otimes_E D_B(V)$ is just the action on B (since G acts trivially on $D_B(V)$).*

Proof.

$$\begin{aligned}\alpha_V(g(b_1 \otimes \sum b_\alpha \otimes v_\alpha) &= \alpha_V(g(b_1) \otimes \sum b_\alpha \otimes v_\alpha) = \alpha_V(g(b_1) \otimes \sum g(b_\alpha) \otimes g(v_\alpha)) \\ &= \sum g(b_1)g(b_\alpha) \otimes g(v_\alpha) = \sum g(b_1 b_\alpha) \otimes g(v_\alpha) = g(b_1 \sum b_\alpha \otimes v_\alpha) \\ &= g(\alpha_V(b_1 \otimes \sum b_\alpha \otimes v_\alpha))\end{aligned}$$

□

Proposition 96. *α_V is an injection, and $\dim_E D_B(V) \leq \dim_F V$ (in particular, this shows that $\dim_E D_B(V)$ is finite). Moreover, if equality holds, then α_V is an isomorphism of B-modules.*

Definition 97. A representation V is *B-admissible* if $\dim_E D_B(V) = \dim_F V$.

Proof. First assume that B is a field, and let $(e_\alpha)_{\alpha \in I}$ be an E-basis for $D_B(V)$. Then since B is a vector space over E, we have also that $(1 \otimes_E e_\alpha)$ is a basis of $B \otimes_E D_B(V)$ over B[6]. We want to show that α_V sends this basis to a linearly independent set over B; then α_V is injective and thus $\dim_B B \otimes_F V \leq \dim_F V$.

Now, $\alpha_V(1 \otimes e_\alpha) = e_\alpha$ (just follow the definition; only the multiplication map in α_V actually does anything, and here it multiplies by 1). So assume that we have $b_\alpha \in B$ with $\sum b_\alpha \alpha_V(1 \otimes e_\alpha) = \sum b_\alpha e_\alpha = 0$ with the b_α not all zero, and almost all $b_\alpha = 0$. Assume further that we have chosen such a relation with the minimal number of nonzero b_α. Finally, we may assume wlog that $b_1 = 1$ (where $1 \in I$ is some index). Choose $g \in G$. Then

$$g\left(\sum b_\alpha e_\alpha\right) = \sum g(b_\alpha)g(e_\alpha) = \sum g(b_\alpha)e_\alpha = e_1 + \sum_{\substack{\alpha \in I \\ \alpha \neq 1}} g(b_\alpha)e_\alpha = 0$$

since the e_α are G-invariant. Subtract the two relations to see that

$$\sum_{\substack{\alpha \in I \\ \alpha \neq 1}} (b_\alpha - g(b_\alpha))e_\alpha = 0$$

[6] This is extension of scalars for free modules: if $R \subset S$ then $S \otimes_R R \cong S$, and tensor product distributes over direct sums, so $S \otimes_R R^n \cong S^n$

But this relation has fewer nonzero elements, so in fact they are all zero and $b_\alpha = g(b_\alpha)$ for all $g \in G$. Thus $b_\alpha \in B^G = E$. But then the b_α were all zero to start with, since the e_α form an E-basis.

If the dimensions are equal, then the two sides have the same B-dimension, so are isomorphic.

In the general case, where B is not necessarily a field, write $C = \mathrm{Frac}(B)$. Then we have a diagram

$$\begin{array}{ccc} \alpha_V : B \otimes_E D_B(V) & \longrightarrow & B \otimes_F V \\ \downarrow & & \downarrow \\ \alpha_V^C : C \otimes_E D_V(C) & \longrightarrow & C \otimes_F V \end{array}$$

since $E = B^G = C^G$, and α_V^C is injective so that α_V is as well. Now, both $B \otimes_E D_B(V)$ and $B \otimes_F V$ are free B-modules (extension of scalars again), so α_V being injective implies a $\leq$ relationship between their ranks.

If the dimensions are equal, then α_V is an injective map of free B-modules of the same rank. That does not necessarily make it an isomorphism, but consider $\det(\alpha_V) \in B - \{0\}$ defined by choosing bases. This is well-defined up to an element of B^*, and if $\det(\alpha_V) \in B^*$, then α_V is an isomorphism. Now, $F\det(\alpha_V)$ is G-stable since α_V is compatible with the G-action, so that $\det(\alpha_V)$ is invertible and thus in B^*. □

Not clear, some calculation was involved here?

Remark 98. If V is B-admissible, then $V \otimes_F B \cong B \otimes_E D_B(V) \cong B \otimes_E E^n \cong B^n$ as $B[G]$-modules (isomorphism as B-modules is clear, and all the isomorphisms are compatible with the G-action [in particular, the first one, α_V, is]). The converse is also true: if $V \otimes_F B \cong B^n$ as $B[G]$-modules, then V is B-admissible since we always have $B^n \cong B \otimes_E D_B(V)$. Thus a representation is B-admissible if its tensor product with B is a sum of trivial representations.

Definition 99. We write $\mathrm{Rep}_F^B G$ for the full subcategory of $\mathrm{Rep}_F G$ of B-admissible representations (*full* here means that we keep all the morphisms from the original category).

Note that the definitions of $D_B(V)$ and of B-admissibility depend only on the $F[G]$ action on B, not on the multiplicative structure of B. The multiplication on B was used to define α_V and to prove the proposition about the dimensions of $D_B(V)$ and V. In the case where B is a field, both $B \otimes_E D_B(V)$ and $B \otimes_F V$ are B-vector spaces with a G-action, so they are representations. However, they are not linear since G acts nontrivially on B: if $w \in B \otimes_F V$ and $b \in B$, we have $g(bw) = g(b)g(w) \neq bg(w)$ in general.

Definition 100. Let G be a group, B be a commutative ring with a G-action. A *semi-linear* representation of B over B is a free finite rank B-module W with a morphism $\rho : G \to \mathrm{Aut}_+(W)$ (the automorphisms of W as an additive group), not necessarily linear, such that

$$\rho(g)(bw) = g(b)\rho(g)(w)$$

Note that if the action of G on B is trivial, this is a linear representation.

If B is a field, a semi-linear representation W is a B-vector space and an additive group with G-action.

Definition 101. Let $(\rho_1, W_1), (\rho_2, W_2)$ be two semi-linear representations. A morphism $f : W_1 \to W_2$ is a morphism of semi-linear representations if f is B-linear and $f(\rho_1(gw)) = \rho_2(g)f(w)$ for all $g \in G, w \in W_1$.

With these definitions, the set of semi-linear representations of G over B forms a category.

The trivial semi-linear representation of dimension n is B^n, with

$$\rho(g)(b_1, \ldots, b_n) = (gb_1, \ldots, gb_n)$$

Clearly $B \otimes_F V$ is a semi-linear representation of dimension $\dim_F V$ since V is an F-vector space and the G-action is defined appropriately. $B \otimes_E D_B(V)$ is clearly a free B-module with a G-action and is also semi-linear:

$$\rho(g)(b_1(b \otimes v)) = g(b_1 b) \otimes g(v) = g(b_1 b) \otimes v = g(b_1)(gb \otimes v) = g(b_1)\rho(g)(b \otimes v)$$

since the G-action on $D_B(V)$ is trivial. Again since the G-action is trivial, $B \otimes_E D_B(V)$ is the trivial representation.

Now, α_V is clearly a morphism of semi-linear representations, and V is B-admissible if and only if α_V is an isomorphism of semi-linear representations if and only if $B \otimes_F V$ is the trivial semi-linear representation. This is a restatement, in the language of semi-linear representations, of Remark **??**.

Proposition 102.

1. *If V is B-admissible, then any subrepresentation of V and any quotient of V are also B-admissible.*
2. *If V_1, V_2 are B-admissible, then $V_1 \otimes_F V_2$ is B-admissible, and*
$$D_B(V_1 \otimes_F V_2) = D_B(V_1) \otimes_E D_B(V_2)$$
3. *If V is B-admissible, then so is $V^{\otimes n}$.*
4. *If V is B-admissible, then so are $\Omega^n V$ and $\Lambda^n V$, and $D_B(\Lambda^k V) = \Lambda^k D_B(V)$.* and $D_B(\Omega^k V) = \Omega^k D_B(V)$?
5. *If V is B-admissible, so is V^*.*

Proof.

1. Suppose V is B-admissible and that
$$0 \to V_1 \to V \to V_2 \to 0$$
is exact in $\mathrm{Rep}_F G$; then
$$0 \to D_B(V_1) \to D_B(V) \to D_B(V_2)$$
is also exact, so that $\dim_E D_B(V) \leq \dim_E D_B(V_1) + \dim_E D_B(V_2)$. But $\dim_E D_B(V) = \dim_F V$, so that
$$\dim_F V = \dim_E D_B(V) \leq \dim_E D_B(V_1) + \dim_E D_B(V_2) \leq \dim_F V_1 + \dim_F V_2$$
But equality holds here, so that $\dim_E D_B(V_i) \leq \dim_F V_i$ implies that both V_i are B-admissible.
2. Suppose that $\dim_F V_1 = m, \dim_F V_2 = n$. Then as $B[G]$-modules, $V_1 \otimes_F B \cong B^m, V_2 \otimes_F B \cong B^n$. Thus
$$(V_1 \otimes_F V_2) \otimes_F B \cong V_1 \otimes_F B^n = (V_1 \otimes_F B)^n \cong B^{mn}$$
as $B[G]$-modules, so that $V_1 \otimes_F V_2$ is B-admissible. This proves the first part of the statement.
3. This follows directly from the previous item.

4.

5. ???

The statements about Λ^k follow directly from (3) since $\Lambda^k V$ is a quotient of $V^{\otimes n}$?

□

Theorem 103. *Assume that B_1, B_2 are (F,G)-regular, and $f : B_1 \to B_2$ is an injective morphism of F-algebras compatible with the action of G such that f induces an isomorphism $B_1^G \to B_2^G$. Then if V is B_1-admissible, it is B_2-admissible.*

Proof. Since B_i^G is a field, $V \otimes_{B_i^G} \cdot$ is exact, so that $f_* : V \otimes B_1 \to V \otimes B_2$ is injective if f is injective (note that we used here the fact that $B_1^G = B_2^G$). Since f is compatible with the G-action, it carries $(V \otimes B_1)^G$ into $(V \otimes B_2)^G$; this map, too is injective if f is. Recall that we also have always $\dim_{B^G} D_B(V) \leq \dim_F V$. Then since f and thus f_* are injective, we have

$$\dim_F V = \dim_{B_1^G} D_{B_1}(V) = \dim_{B_2^G} f_*(D_{B_1}(V)) \leq \dim_{B_2^G} D_{B_2}(V) \leq \dim_F V$$

so that equality holds. □

Theorem 104. *Let F be a field of uncountable cardinality and I a countable index set. Assume that B is (F,G)-regular and B is the union of sub-F-algebras B_i for $i \in I$ such that $B^G = B_i^G$ for all i. Then if V is a representation of G over F, V is B-admissible if and only if V is B_i-admissible for some $i \in I$.*

Proof. $\Leftarrow$ follows directly from Theorem **??**. For $\Rightarrow$, note that

$$D_B(V) = (V \otimes B)^G = \bigcup_{i \in I} (V \otimes B_i)^G = \bigcup_{i \in I} D_{B_i}(V)$$

Then $D_B(V)$ is the denumerable union of vector spaces giving a vector space over a nondenumerable field, so $\dim D_B(V) = \dim D_{B_i}(V)$ for some $i \in I$ and thus V is B_i-admissible. □

5.3 Fontaine Rings

5.3.1 Introduction

We will apply this theory for $F = \mathbb{Q}_p$. Note that representations over L a finite extension of $\mathbb{Q}_p$ are also representations over $\mathbb{Q}_p$; it turns out that the information we lose in restricting our attention to $\mathbb{Q}_p$ is not important for the theory.

Thus let $F = \mathbb{Q}_p, G = G_K$ for K a p-adic field (i.e. $[K : \mathbb{Q}_p] < \infty$).

Example 105. Let $B = K'$ where K'/K is a finite Galois extension. Then G_K acts on K' through the quotient $\mathrm{Gal}(K'/K)$. B is a field, so is $(\mathbb{Q}_p, G_K)$-regular, and $E = B^G = K$. We have

Proposition 106. *Let (ρ, V) be a representation of G_K on $\mathbb{Q}_p$. Then (ρ, V) is K'-admissible if and only if ρ is trivial on $G_{K'}$ if and only if ρ factors through $\mathrm{Gal}(K'/K)$.*

Proof. The second if and only if is obvious. For the first, recall that if $\Gamma = \mathrm{Gal}(K'/K)$, the normal basis theorem says that $K' \cong K[\Gamma]$ as vector spaces over K, and from the exact sequence

$$1 \to G_{K'} \to G_K \to \mathrm{Gal}(K'/K) = \Gamma \to 1$$

it follows that G_K acts on Γ by permuting its elements, so that $K' \cong K[\Gamma]$ as G_K-representations. We thus have the following isomorphisms of G_K-representations:

$$(V \otimes K')^{G_K} \cong (V \otimes K[\Gamma])^{G_K} = \mathrm{Hom}_{G_K}(K[\Gamma]^*, V) = \mathrm{Hom}_{G_K}(K[\Gamma], V)$$

(the equality with Hom_{G_K} is a standard result from group cohomology, see e.g. Serre Local Fields).

But $K[\Gamma]$ is the regular representation of Γ, so is the sum of all irreducible representations of Γ. If V is one of those, then the formula above reduces to $\dim V$; otherwise, it is 0. Finally, (ρ, V) is K'-admissible if and only if $\dim D_{K'}(V) = \dim V$ if and only if $\dim(V \otimes K')^{G_K} = \dim V$ if and only if V is a representation of $\mathrm{Gal}(K'/K)$. □

Example 107. Let $B = \bar{K}$; then $B^{G_K} = K = E$.

Proposition 108. *(ρ, V) is $\bar{K}$-admissible if and only if ρ has finite image.*

Proof. There are a denumerable number of finite extensions of K contained in $\bar{K}$, and $\bar{K}$ is the union of these. Further, $\bar{K}^{G_K} = K'^{G_K} = K$ by Theorem **??**, so by Theorem **??**, V is $\bar{K}$-admissible if and only if V is K'-admissible for some K' finite over K if and only if (by Proposition **??**) ρ factors through $\mathrm{Gal}(K'/K)$ for some K' finite over K if and only if ρ has finite image. □

Thus the set of admissible representations for B as large as $\bar{\mathbb{Q}}_p$ is still too small – only representations with finite image are admissible. In order to get more admissible representations, we need to consider a larger ring than $\bar{\mathbb{Q}}_p$, which will be its completion $\mathbb{C}_p$.

5.3.2 Nonabelian Group Cohomology

Let G, A be groups (in the usual setting, A is an abelian group; we will not make that assumption. This will reduce the amount of information we can get from the cohomology). Assume A has a G-action; that is, a map $G \times A \to A$ such that for all $g, g' \in G, a, a' \in A$, the following conditions hold: $(gg')a = g(g'a)$, $ea = a$, $g(aa') = (ga)(ga')$, $ge = e$. In other words, a G-action is a morphism $\eta : G \to \mathrm{Aut}(A)$. (Such a morphism defines an action via $ga = \eta(g)(a)$).

Definition 109. $H^0(G, A) = A^G = \{a \in A \mid ga = a \,\forall\, g \in G\}$. This is obviously a subgroup of A.

Definition 110. A *crossed homomorphism* from G to A is a map $G \to A : g \mapsto a_g$ such that for all $s, t \in G$, $a_{st} = a_s \cdot s(a_t)$.

Remark 111. If the action of G on A is trivial (i.e. $ga = a$ for all $g \in G, a \in A$), then a crossed homomorphism is simply a homomorphism of groups.

Definition 112. Let (a_s), (a'_s) be two crossed homomorphisms from G to A. We say that (a_s) and (a'_s) are *cohomologous* (written $(a_s) \sim (a'_s)$) if there is some $a \in A$ such that

$$\forall\, s \in G, \quad a'_s = a^{-1} a_s s(a)$$

It is easy to see that $\sim$ is in fact an equivalence relation. Note also that if (a_s) is a crossed homomorphism and $a \in A$, then $a'_s = a^{-1} a_s s(a)$ is also a crossed homomorphism:

$$a'_s s(a'_t) = a^{-1} a_s s(a) s(a^{-1} a_t t(a)) = a^{-1} a_s s(a_t)(st)(a) = a^{-1} a_{st}(st)(a) = a'_{st}$$

Definition 113. $H^1(G, A)$ is the pointed set of equivalence classes of crossed homomorphisms from G to A modulo $\sim$. The distinguished point in $H^1(G, A)$ is the equivalence class of the crossed homomorphism $a_g = e$ for each $g \in G$.

Definition 114. If $f : (X, x) \to (Y, y)$ is a morphism of pointed sets, then $\ker f = f^{-1}(y)$.

Note that in the category of pointed sets, injectivity is definitely not the same as having trivial kernel. Both $\ker f$ and $\operatorname{im} f$ are pointed sets.

Theorem 115. *Let $0 \to A \to B \xrightarrow{p} C \to 0$ be an exact sequence in the category of groups with G-action (i.e. the maps are compatible with the G-action). Then there is a long exact sequence in cohomology*

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

Proof. δ is defined as follows. Choose $c \in C^G$. Since p is surjective, there is $b \in B$ such that $pb = c$. Define a crossed homomorphism from G to A by defining $a_s = b^{-1}s(b)$ for $g \in G$. Note that this crossed homomorphism in fact lands in A, not in B, since

$$p(a_s) = p(b^{-1})p(s(b)) = p(b)^{-1}s(p(b)) = c^{-1}s(c) = c^{-1}c = e$$

since $c \in C^G$. $s \mapsto a_s$ is a crossed homomorphism since

$$a_s s(a_t) = b^{-1}s(b)s(b^{-1}t(b)) = b^{-1}(st)(b) = a_{st}$$

and thus this defines an element of $H^1(G, A)$; this is $\delta(c)$.

We made a choice in the definition; namely, the choice of $b \in p^{-1}c$. Suppose we had chosen a different b, i.e. an element $ba \in B$ for $a \in A$ (this is the range of choices since we have an exact sequence of groups; further, since A is normal in B, we need not also worry about ab). Then we get

$$a'_s = (ba)^{-1}s(ba) = a^{-1}b^{-1}s(b)s(a) = a^{-1}a_s s(a)$$

and a, a' are cohomologous.

Exactness is either obvious or a diagram trace. □

Theorem 116. *(Hilbert's Theorem 90) Let K'/K be an algebraic Galois extension of fields. Then* $\mathrm{Gal}(K'/K)$ *acts on $M_n(K')$ coefficient by coefficient, and we have*

1. $H^1(\mathrm{Gal}(K'/K), GL_n(K'))$ *is trivial*
2. $H^1(\mathrm{Gal}(K'/K), M_n(K'))$ *is trivial where $M_n(K')$ is regarded as an additive group (this is the additive version of Theorem 90). In fact, since $M_n(K')$ is abelian, we can define higher cohomology groups, and $H^i(\mathrm{Gal}(K'/K), M_n(K'))$ is trivial for $i \geq 1$*
3. *For $n = 1$, $H^i(\mathrm{Gal}(K'/K), K'^*)$ is nontrivial for $i > 1$.*

Proof. (Sketch of 1 and 2)
(2): $M_n(K')$ is an induced module.
(1): Assume for simplicity that K'/K is finite, and let (a_s) be a crossed homomorphism from $G = \mathrm{Gal}(K'/K)$ to $\mathrm{GL}_n(K')$. For $c \in M_n(K')$, define

$$b = \sum_{s' \in G} a_{s'} s'(c)$$

Then for $s \in G$, we have

$$s(b) = \sum_{s' \in G} s(a_{s'})ss'(c) = \sum_{s' \in G} a_s^{-1}a_{ss'}ss'(c) = a_s^{-1} \sum_{s' \in G} a_{s'}s'(c) = a_s^{-1}b$$

Thus $s(b) = a_s^{-1}b$. If in fact $b \in GL_n(K')$, we are done, for $a_s = bs(b)^{-1}$ so that $a_s \sim e$. But you can always choose c so that b is in $GL_n(K')$ by linear independence of homomorphism. □

I assume this is an analog of linear independence of characters.

Remark 117. If G, A are topological groups and $G \times A \to A$ is a continuous action, then $H^1_{\text{cont}}(G, A)$ can be defined using continuous crossed homomorphisms, and the equivalence classes are closed.

There is a close relation between group cohomology and semi-linear representations. Let G be a group and B a ring with G-action. We can associate to each dimension n semi-linear representation V of G over B an element in $H^1(G, GL_n(B))$ as follows. Let $\mathcal{B}$ be a basis of V. For $s \in G$, we may consider $s\mathcal{B}$; this is still a basis. Thus

$$s\mathcal{B} = a_s^{-1}\mathcal{B}, \quad a_s \in GL_n(B)$$

and

$$a_{st}^{-1}\mathcal{B} = st(\mathcal{B}) = s(a_t^{-1}\mathcal{B}) = s(a_t^{-1})s\mathcal{B} = s(a_t^{-1})a_s^{-1}\mathcal{B}$$

using in the next-to-last step the fact that the representation is semi-linear. Thus $a_{st} = a_s s(a_t)$ so that a_s is a crossed homomorphism from G to $GL_n(B)$; we map V to the class of (a_s) in $H^1(G, GL_n(B))$. If we had picked a different basis $a\mathcal{B}, a \in GL_n(B)$, then $s(a\mathcal{B}) = a_s^{-1}s\mathcal{B}$ and we would get a cohomologous crossed homomorphism $a^{-1}a_s s(a)$. We thus get a morphism from B-semi-linear representations of dimension n modulo isomorphism to $H^1(G, GL_n(B))$.

Theorem 118. *This map is a bijection of pointed sets, where the distinguished point in the set of representations is the trivial semi-linear representation.*

Proof. (Sketch) Bijection is "easy". To see that the trivial representation maps to the distinguished element of cohomology, choose a basis invariant under the G-action. □

Note that if the G-action on B is trivial, then we are in fact talking about linear representations, and this theorem becomes the well-known fact that B-linear representations of G of dimension n, modulo isomorphism, are the same as maps $G \to GL_n(B)$.

Corollary 119. *Let K be an algebraic extension of $\mathbb{Q}_p$, let B be a $(\mathbb{Q}_p, G_K)$-regular ring, and L/K a Galois extension. Assume that $H^1(\mathrm{Gal}(L/K), GL_n(B^{G_L})) = 0$, and let (ρ, V) be a representation of G_K. Then if $V|_{G_L}$ is B-admissible, so is V.*

Proof. Saying that $V|_{G_L}$ is B-admissible means that $W = (V \otimes_{\mathbb{Q}_p} B)^{G_L}$ has dimension n over $A = B^{G_L}$. W has a natural G_K action in which G_L acts trivially; this induces an action of $\mathrm{Gal}(L/K)$ on W. This action is A-semi-linear since the G_K action is. By the theorem, since the cohomology vanishes, we see that $W = A^n$ as A-modules with semi-linear $\mathrm{Gal}(L/K)$-modules. But then as A-modules,

$$D_B(V) = (V \otimes_{\mathbb{Q}_p} B)^{G_K} = ((V \otimes_{\mathbb{Q}_p})^{G_L})^{\mathrm{Gal}(L/K)} = (A^n)^{\mathrm{Gal}(L/K)} = (B^{G_K})^n$$

and thus V is B-admissible. □

5.3.3 Representations over $\mathbb{C}_p$ and Sen Theory

$\bar{\mathbb{Q}}_p$ is algebraically closed, and has a unique absolute value extending $|\cdot|_p$ since every element of $\bar{\mathbb{Q}}_p$ is in some finite extension and there is a unique absolute value in that extension extending $|\cdot|_p$. However,

Proposition 120. *$\bar{\mathbb{Q}}_p$ is not complete.*

Proof. Let K_n be the compositum of all extensions of $\mathbb{Q}_p$ of degree $\leq n$. Then

$$\mathbb{Q}_p = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots$$

and $\bar{\mathbb{Q}}_p = \cup K_i$. Since there are only a finite number of extensions of $\mathbb{Q}_p$ of a given degree, we have $[K_n : \mathbb{Q}_p] < \infty$. Since K_n is finite dimensional, it is closed in $\bar{\mathbb{Q}}_p$ with empty interior. By the Baire category theorem, $\bar{\mathbb{Q}}_p$ cannot be complete. □

Definition 121. $\mathbb{C}_p$ is the completion of $\bar{\mathbb{Q}}_p$ for $|\cdot|_p$.

Proposition 122. *$\mathbb{C}_p$ is algebraically closed.*

Proof. Recall that a version of Krasner's lemma (actually a corollary) says the following: Let K be a field complete with respect to a nontrivial nonarchimedean absolute value, $P(x) \in K[x]$ a monic irreducible polynomial, α a root of $P(x)$ in some algebraic closure $\bar{K}$ of K. If $Q(x) \in K[x]$ is a monic polynomial of the same degree as $P(x)$ that is "sufficiently close" to $P(x)$, then there is a root β of $Q(x)$ in $\bar{K}$ such that $K(\alpha) = K(\beta)$.

So let α be algebraic over $\mathbb{C}_p$ and $P(x)$ its monic irreducible polynomial in $\mathbb{C}_p[x]$. Since $\bar{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$, we may choose $Q(x) \in \bar{\mathbb{Q}}_p[x]$ arbitrarily close to $P(x)$. Then there is a root $\beta \in \mathbb{C}_p$ such that $\mathbb{C}_p(\alpha) = \mathbb{C}_p(\beta) = \mathbb{C}$ so that $\alpha \in \mathbb{C}_p$. □

If $K/\mathbb{Q}_p$ is a finite extension, then G_K acts on $\bar{K} = \bar{\mathbb{Q}}_p$ continuously (if $x \in \bar{K}$, then $x, \sigma(x)$ are in some finite extension of K, so their absolute values are the same since they depend only on the norm of x). Thus it also acts on $\mathbb{C}_p$. This makes $\mathbb{C}_p$ into a $(\mathbb{Q}_p, G_K)$-regular ring, and we would like to know what $\mathbb{C}_p^{G_K}$ is.

Theorem 123. *(Tate) Let K be any algebraic extension of $\mathbb{Q}_p$, $\hat{K}$ the topological closure of K in $\mathbb{C}_p$.*[7] *Then $\mathbb{C}_p^{G_K} = \hat{K}$. In particular, if $K/\mathbb{Q}_p$ is finite, then K is closed so that $\mathbb{C}_p^{G_K} = K$.*

We will not prove this theorem. But clearly if K is any subfield of $\bar{\mathbb{Q}}_p$, $\mathbb{C}_p^{G_K} \supset K$. But $\mathbb{C}_p^{G_K}$ is closed; one can use this to show that it is equal to the topological closure of K in $\mathbb{C}_p$ by looking at elements approximately fixed by G_K and show those elements are almost in K.

This theorem says among other things that all elements on which G_K acts trivially are algebraic, something that is not a priori obvious.

Theorem 124. *(Sen, Serre-Tate) Let K be a finite extension of $\mathbb{Q}_p$, (ρ, V) a p-adic representation of G_K. Then (ρ, V) is $\mathbb{C}_p$-admissible if and only if $\rho(I_K)$ is finite.*

This theorem too is somewhat surprising, as it says that the admissible representations of the transcendental extension $\mathbb{C}_p$ are characterized by a purely algebraic condition. However, it shows that even $\mathbb{C}_p$ is not large enough.

The proof of Sen's theorem requires that we understand when a representation that is $\mathbb{C}_p$-admissible over an extension of $\mathbb{Q}_p$ is $\mathbb{C}_p$-admissible over a larger or smaller field. This is provided by the following proposition:

Proposition 125. *(Serre) Let K be a finite extension of $\mathbb{Q}_p$, K' any algebraic extension of K, (ρ, V) a p-adic representation of G_K of dimension n. Then*

[7] Note that $\hat{K}$ is also the completion of K with respect to the p-adic metric on K since both spaces are complete and contain K as a dense subset.

1. *If V is $\mathbb{C}_p$-admissible, then $V|_{G_{K'}}$ is $\mathbb{C}_p$-admissible (by this we mean that V, regarded as a representation of $G_{K'} \subset G_K$ is admissible, i.e. that $\dim_{\hat{K'}}(V \otimes \mathbb{C}_p)^{G_{K'}} = \dim_{\mathbb{Q}_p} V$).*
2. *If in addition the image of $|\cdot|_{K'}$ is discrete, then if $V|_{G_{K'}}$ is $\mathbb{C}_p$-admissible, V is also $\mathbb{C}_p$-admissible.*

Proof. V is $\mathbb{C}_p$-admissible if and only if $V \otimes_K \mathbb{C}_p \cong \mathbb{C}_p^n$ as G_K representations, which implies that $K' \otimes (V \otimes_K \mathbb{C}_p) = V \otimes_{K'} \mathbb{C}_p \cong \mathbb{C}_p^n$ as $G_{K'}$ representations. This proves (1).
To prove (2), we start with

Lemma 126. *Let K be a finite extension of $\mathbb{Q}_p$, and $K \subset K' \subset \bar{K}$. Extend the absolute value on K to K'. Then the absolute value on K' is discrete if and only if K' is a finite extension of an unramified extension of K.*

Proof. Recall that a ramified extension L/K of ramification index e is such that the image of $|\cdot|_L$ is the $1/e$ powers of the image of $|\cdot|_K$. Now, $\Leftarrow$ is clear since unramified extensions don't change the image of the absolute value. To see $\Rightarrow$, let K'' be the maximal unramified extension of K in K'. Then K'/K'' is totally ramified, and must be finite else the image of the absolute value will clearly not be discrete. □

Now, if K' is not Galois over K, replace K' by its Galois closure; by part (1), it suffices to prove (2) for this new K', since by Lemma **??**, the new K' also satisfies the discreteness condition. Letting K^{nr} be the maximal unramified extension of K contained in K', we have that K'/K^{nr} is finite Galois and K^{nr}/K is unramified. So we need only prove (2) in the two cases where K'/K is finite Galois and where K'/K is unramified.

Assume first that K'/K is finite Galois and that $V|_{G_{K'}}$ is $\mathbb{C}_p$-admissible. By Corollary **??**, it suffices to show that $H^1(\mathrm{Gal}(K'/K), GL_n(\mathbb{C}_p^{G_{K'}})) = 0$. Now, this is simply $H^1(\mathrm{Gal}(K'/K), GL_n(K'))$ since K' is closed, and this is zero by Hilbert's Theorem 90.

If K'/K is unramified and $V|_{G_{K'}}$ is $\mathbb{C}_p$-admissible, then we have $K' \subset \hat{K'}$, where the inclusion is perhaps proper. Again by Corollary **??**, it suffices to show that

$$H^1(\mathrm{Gal}(K'/K), GL_n(\mathbb{C}_p^{G_{K'}})) = H^1(Gal(K'/K), GL_n(\hat{K'})) = 0$$

Here we are actually considering the *continuous* cohomology. But this is the same as

$$H^1_{\mathrm{cont}}(\mathrm{Gal}(K'/K), GL_n(\mathcal{O}_{\hat{K'}}))$$

since we have seen before that a semi-linear representation of a compact group over a space has a stable lattice. But $GL_n(\mathcal{O}_{\hat{K'}}) = \varprojlim_r GL_n(\mathcal{O}_{\hat{K'}}/\mathfrak{m}^r)$ since $\mathcal{O}\hat{K'}$ is a DVR since $\hat{K'}$ is complete. Limits commute with cohomology, so

$$H^1_{\mathrm{cont}}(\mathrm{Gal}(K'/K), GL_n(\hat{K'})) = \varprojlim_r H^1_{\mathrm{cont}}(\mathrm{Gal}(K'/K), GL_n(\mathcal{O}_{\hat{K'}}/\mathfrak{m}^r))$$

To see that this is zero, consider the case $r = 2$. Let k' be the residue field of $\mathcal{O}_{\hat{K'}}$ (and of $\mathcal{O}_{K'}$), k the residue field of K. We have an exact sequence of groups

$$1 \to 1 + \mathfrak{m}M_n(k') \to GL_n(\mathcal{O}_{\hat{K'}}/\mathfrak{m}^2) \to GL_n(\mathcal{O}_{\hat{K'}}/\mathfrak{m}) \to 0$$

where the last map is simply reduction. Now, since K'/K is unramified, $\mathrm{Gal}(K'/K) = \mathrm{Gal}(k'/k)$, so from the long exact sequence in cohomology, it suffices to show that

$$H^1(\mathrm{Gal}(k'/k), GL_n(k')) = 0$$
$$H^1(\mathrm{Gal}(k'/k), 1 + \mathfrak{m}M_n(k')) = 0$$

Note that the statement of Hilbert 90 probably needs to be slightly different, then. Where have we seen this before How does stable lattice imply the result?

The first follows from Hilbert 90. For the second, $1+\mathfrak{m}M_n(k') \cong M_n(k')$ via the log map [note that $(1+pa)(1+pb) = 1+p(a+b)+p^2\dots$], so this cohomology is zero by the additive version of Hilbert 90.

It is clear that this argument generalizes to $r > 2$. □

Remark 127. The only fact we used about $\mathbb{C}_p$ in the K'/K finite case was the fact that $\mathbb{C}_p^{G_K} = K$, $\mathbb{C}_p^{G_{K'}} = K'$. So if B is any regular ring with $B^{G_{K'}} = K'$ for any finite K'/K, the same proof works. B is such a ring for B_{deRham}, but not for B_{crys}.

Remark 128. In the unramified case, note that $\text{Gal}(K'/K) = \text{Gal}(\hat{K}'/K)$, but it doesn't work to write $H^1(\text{Gal}(K'/K), GL_n(\hat{K}')) = H^1(\text{Gal}(\hat{K}'/K), GL_n(\hat{K}'))$ since Hilbert 90 does not apply to this non-algebraic extension.

Remark 129. Proposition **??** implies $\Leftarrow$ in Sen's Theorem (Theorem **??**): Since $\rho(I_K)$ is finite, we may choose a finite extension of K so that $\rho(I_K)$ is trivial; after an unramified extension, we may then assume that $\rho(G_K)$ is trivial. Then V is $\mathbb{C}_p$-admissible over this larger field by Proposition **??**. Apply the proposition.

How do we choose these extensions?

To prove the remainder of Sen's theorem, we will need to develop the so-called *Sen theory.* Thus let $[K : \mathbb{Q}_p]$ be a finite extension, V a G_K representation of dimension d. Define a field K_∞ by $K_\infty = \bigcup_n K_n$ where $K_n = K(\zeta_{p^n})$ for ζ_{p^n} some primitive p^n root of unity. Then K_∞ is Galois over K with Galois group $\Gamma = \text{Gal}(K_\infty/K)$, and $\bar{K}$ is Galois over K_∞ with Galois group H. Note that K_∞ is ramified over K. The outline of what is to follow is:

- We will define a K_∞ vector space $D_{\text{sen}}(V)$ that has a semi-linear action of Γ.
- This will allow us to define a K_∞-linear operator φ on $D_{\text{sen}}(V)$. We show that its characteristic polynomial is $\chi_\varphi(x) \in K[x]$.
- The roots of $\chi_\varphi(x)$ are called the Hodge-Tate-Sen weights of φ; there are d of them (in $\bar{K}$) counted with multiplicity.
- Finally, $\varphi = 0$ iff V is $\mathbb{C}_p$-admissible iff $\rho(I_K)$ is finite, thus proving the other direction of Sen's theorem.

Recall that $\omega_p : G_K \to \mathbb{Z}_p^*$. This map is surjective for $K = \mathbb{Q}_p$, and has image a finite index subgroup for $[K : \mathbb{Q}_p] < \infty$. ω_p is trivial on $\bar{K}/K_\infty$ since it was defined by an action on p^n roots of unity; in fact $H = \ker \omega_p$. Thus ω_p induces an injection $\Gamma \to \mathbb{Z}_p^*$ and thus Γ is the image of ω_p in $\mathbb{Z}_p^*$.

Proposition 130. *If V is a semi-linear representation of G_K, then $(V \otimes \mathbb{C}_p)^H$ has dimension d over $\hat{K}_\infty$. In other words, $V|_H$ is always $\mathbb{C}_p$-admissible.*

We will not prove this. However, this is equivalent to the statement that

$$H^1(H, GL_d(\mathbb{C}_p)) = H^1(H, GL_d(\mathbb{C}_p^H)) = 0$$

by Corollary **??**. The proof is longer and harder than the previous arguments. Essentially, an element of $\mathbb{C}_p$ is the limit of elements of $\bar{\mathbb{Q}}_p$; we find a sequence of elements that converge quickly to an element of $\mathbb{C}_p$ but whose algebraic degrees do not increase rapidly, and this suffices to prove the result.

Definition 131. If W is a finite-dimensional vector space over $\hat{K}_\infty$ with a Γ action, then W is clearly also a K-vector space. If $v \in W$, we say that v is Γ-finite over K if the K-linear span of γv for $\gamma \in \Gamma$ has finite dimension over K.

Example 132. Let $W = \hat{K}_\infty$ with the obvious Γ action. Then v is Γ-finite if and only if v is algebraic over K if and only if $v \in K_\infty$ (this uses the fact that the algebraic elements of $\hat{K}_\infty$ are just K_∞, a fact that follows from Theorem **??**).

Proposition 133. *In $(V \otimes \mathbb{C}_p)^H$, call $D_{\text{sen}}(V)$ the K-subspace generated by vectors that are Γ-finite over K. Then $D_{\text{sen}}(V)$ is a K_∞ vector space of dimension d and it has a semi-linear Γ action.*

Why a K_∞ vector space?

We will not prove this result either. As a consequence, we get

$$\begin{array}{ccccc} D_{\text{sen}}(V) & \subset & (V \otimes \mathbb{C}_p)^H & \subset & V \otimes \mathbb{C}_p \\ \circlearrowleft & & \circlearrowleft & & \circlearrowleft \\ \Gamma & & \Gamma & & G_K \end{array}$$

where the first is a K_∞ vector space of dimension d, the second a $\hat{K}_\infty$ vector space of dimension d, and the third a $\mathbb{C}_p$ vector space of dimension d. Thus we can recover $(V \otimes \mathbb{C}_p)^H$ by tensoring $D_{\text{sen}}(V)$ with $\hat{K}_\infty$.

Proposition 134. *There is a unique K_∞ operator φ on $D_{\text{sen}}(V)$ such that for all $v \in D_{\text{sen}}(V)$ there exists an open subgroup Γ_v of Γ such that for all $\gamma \in \Gamma_v$,*

$$\gamma \cdot v = \exp(\varphi \log_p(\omega_p(\gamma)))(v)$$

Further, there is a basis of $D_{\text{sen}}(V)$ over K_∞ in which the matrix of φ has coefficients in K.

Think by analogy about $\mathbb{R}$ acting on $\mathbb{R}^n$. The action is determined by the derivative at 0 using the exponential map. Here the group is written multiplicatively, hence the log.

Remark 135. If $\rho : \mathbb{Z}_p \to GL_n(L)$ is continuous (i.e. a one-parameter subgroup), then on an open subgroup of $\mathbb{Z}_p$, we have $\rho(t) = \exp(t\varphi)$ where $\varphi \in M_n(L)$. To see this, note that on a small enough subgroup of $\mathbb{Z}_p$, $\log \rho$ is defined, so we get a map $\mathbb{Z}_p \to M_n(L)$, i.e. n^2 maps $\mathbb{Z}_p \to L$.

Then what?

Remark 136. Γ acts semi-linearly on $D_{\text{sen}}(V)$. So for $\lambda \in K_\infty$, $w \in D_{\text{sen}}(V)$, we have $g(\lambda w) = g(\lambda)g(w)$. But $\lambda \in K'$ for some K'/K finite; if we take $g \in \text{Gal}(K_\infty/K')$, then $g(\lambda w) = \lambda g(w)$. Thus the Γ-action is not so far from a linear action.

Proof. Let $e_1, \ldots, e_d$ be a basis of $D_{\text{sen}}(V)$. There is some K'/K such that

$$D' = K'e_1 \oplus \cdots \oplus K'e_d$$

is Γ-stable, for since the e_1 are all Γ-finite, take K' to be a finite extension containing the span of the images of the e_i under Γ. Then Γ acts semi-linearly on D'. Let $\Gamma' = \text{Gal}(\bar{K}/K') \subset \Gamma$. Then Γ' acts linearly on K' since it acts trivially on scalars. Then by the first remark above, there is a K'-linear map $\varphi : D' \to D'$ such that for $g \in \Gamma', v \in D'$,

$$g(v) = \exp(\varphi \log(\omega_p(g)))(v)$$

To ensure this, enlarge K' if necessary to get the image of Γ' inside $1 + p\mathbb{Z}_p$.

Now, for $w \in D_{\text{sen}}(V)$, write $w = \lambda_1 e_1 + \cdots + \lambda_d e_d$ for $\lambda_i \in K_\infty$, and let Γ^* be an open subgroup fixing the λ_i. Then for $g \in \Gamma_w = \Gamma' \cap \Gamma^*$,

$$g(w) = \exp(\varphi \log(\omega_p(g)))w$$

since g fixes all the λ_i and all the $e_i \in D'$. This proves existence.

To see uniqueness, note that

$$gw - w = (\exp(\varphi \log(\omega_p(g))) - Id)w$$

Writing $t = \log \omega_p(g) \in \mathbb{Z}_p$ and dividing by t, we get

$$\frac{gw - w}{t} = \frac{\exp(\varphi t) - Id}{t}$$

and letting $g \to e$, the right-hand side becomes $\varphi(w)$. This proves uniqueness, since only one φ can be the limit of the left-hand side.

For the final statement, for $g' \in \Gamma$, we have

$$\varphi \circ g' = \lim \frac{gg'(w) - g'(w)}{\log t} = g' \circ \varphi$$

and thus ${g'}^{-1}\varphi g' = \varphi$. This means that if B is some basis of $D_{\text{sen}}(V)$, then

$$\text{Mat}_B \varphi = g'(\text{Mat}_{g'(B)}\varphi)$$

The result then follows from

Lemma 137. *Let L/K be Galois, $A \in M_n(L)$. If $g(A)$ is similar to A for all $g \in \text{Gal}(L/K)$, then A is similar to a matrix in $M_n(K)$.*

Proof. Since $g(A) \sim A$, $g(A)$ and A have the same minimal polynomial; since this holds for all $g \in \text{Gal}(L/K)$, the minimal polynomial is defined over K. □ Why does this imply that the matrix can be?

□

This entire construction works only because K_∞ is algebraic over K so that we can find an open subgroup on which the action is linear. This would not work, for example, in general over $\mathbb{C}_p$.

Definition 138. φ is called the *Sen operator*, and D_{sen} the *Sen space*. The eigenvalues of φ (i.e. the roots of its characteristic polynomial) are called the *Hodge-Tate-Sen weights of V*, and lie in $\bar{K}$. These are an important invariant of the representation.

Proposition 139. *$\varphi = 0$ if and only if V is $\mathbb{C}_p$-admissible.*

In fact, more is true: $\dim_{K_\infty} \ker \varphi = \dim_K (V \otimes \mathbb{C}_p)^G$.

Proof. If V is $\mathbb{C}_p$-admissible, then $A = (V \otimes \mathbb{C}_p)^{G_K}$ has dimension d over K. Now, Γ acts trivially on A, so that

$$A = (V \otimes \mathbb{C}_p)^{G_K} \subset D_{\text{sen}}(V) \subset B = (V \otimes \mathbb{C}_p)^H$$

By the definition of φ, if Γ acts trivially on a basis of $D_{\text{sen}}(V)$, then $\varphi = 0$. Now, it is true (although nontrivial) that a basis of A over K is a basis of B over K_∞. rest is gibberish

Now assume $\varphi = 0$. Then Γ acts finitely on $D_{\text{sen}}(V)$ since it acts through a finite quotient. Thus Γ acts continuously for the discrete topology on $D_{\text{sen}}(V)$ and thus by Hilbert 90, $D_{\text{sen}}(V)$ is the trivial semi-linear representation. Thus

$$\dim_K (V \otimes \mathbb{C}_p)^{G_K} = \dim_K D_{\text{sen}}(V)^\Gamma = d$$

□

Note however that $\mathbb{C}_p$-admissible is not equivalent to the statement that the Hodge-Tate-Sen weights are zero since φ could be nilpotent.

Proposition 140. *Let (ρ, V) be any representation, and let $G = \rho(I_K) \subset GL_d(\mathbb{Q}_p)$. ($GL_d(\mathbb{Q}_p)$ is a "p-adic Lie group"). G is compact since I_K is compact and thus is a closed subgroup of a Lie group, so is itself a Lie group. Let its Lie algebra be $\mathfrak{g}$. Thus*

$$\mathfrak{g} = \{M \in M_d(\mathbb{Q}_p) \mid \exp(tM) \in G \ \forall \text{ sufficiently small } t \in \mathbb{Z}_p\}$$

This is a subspace of $M_d(\mathbb{Q}_p)$, and $\dim G = \dim \mathfrak{g}$. Then $\mathfrak{g}$ is the smallest subspace of $M_d(\mathbb{Q}_p)$ such that $\varphi \in \mathrm{End}(V \otimes \mathbb{C}_p)$ lies in $\mathfrak{g} \otimes \mathbb{C}_p \subset M_d(\mathbb{C}_p) = \mathrm{End}(V \otimes \mathbb{C}_p)$.

We will not prove this.

Corollary 141. *If V is $\mathbb{C}_p$-admissible, then $\varphi = 0$, then $\mathfrak{g} = 0$ and thus $\rho(I_K)$ is finite.*

This finally proves the converse of Sen's theorem, that V being $\mathbb{C}_p$-admissible implies that $\rho(I_K)$ is finite.

Example 142.

$$\omega_p : \quad G_K \longrightarrow \mathbb{Z}_p^* \\ \quad \searrow \quad \nearrow \\ \quad \Gamma$$

Now, $\mathbb{Z}_p^* \cong \mathbb{Z}/p\mathbb{Z} \times (1 + p\mathbb{Z}_p)$. Assume that $\omega_p(G_K) \subset 1 + p\mathbb{Z}_p$ (i.e. that $K \supset \mathbb{Q}_p(\zeta_p)$, for then $\omega_p(G_K)$ is trivial in the "p" place; just look at the map $G_K \to \mathrm{Gal}(K(\boldsymbol{\mu}_p)/K) \to (\mathbb{Z}/p\mathbb{Z})^*$; here $K(\boldsymbol{\mu}_p) = K$). Then for $\lambda \in \mathbb{Z}_p$, define $\omega_p^\lambda(\cdot) = \exp(\lambda \log(\omega_p(\cdot)))$ (alternatively, use this definition for $\lambda \in \mathbb{Z}$ and extend by continuity). For $V = \mathbb{Q}_p$, G acts on it through ω_p^λ. $D_{\mathrm{sen}}(V) = K_\infty$, and the action of φ is λ. Then $V \otimes \mathbb{C}_p = \mathbb{C}_p$ with the ω_p^λ action and $(V \otimes \mathbb{C}_p)^H = K_\infty$ with the ω_p^λ action. Thus V has weight λ.

5.3.4 Hodge-Tate representations

Definition 143. For K a finite extension of $\mathbb{Q}_p$, define $B_{\mathrm{HT}} = \mathbb{C}_p[t, t^{-1}]$ where G_K acts on t^n via ω_p^n. That is, for $g \in G_K$,

$$g\left(\sum_{i=n}^{m} a_i t^i\right) = \sum_{i=n}^{m} g(a_i)\omega_p(g)^i t^i$$

Thus as a G_K-module, $B_{\mathrm{HT}} = \oplus_{i \in \mathbb{Z}} \mathbb{C}_p(i)$, where $\mathbb{C}_p(i)$ is $\mathbb{C}_p$ with the semi-linear action of ω_p^i. Hence $\mathbb{C}_p$ with the trivial action is a subgroup of B_{HT}.

Proposition 144. *B_{HT} is $(\mathbb{Q}_p, G_K)$-regular, and $B_{\mathrm{HT}}^{G_K} = K$.*

Proof. We prove the second part first. Invariance under the G_K action depends only on the module structure of B, not its ring structure, so we start with $B_{\mathrm{HT}}^{G_K} = \oplus_{i \in \mathbb{Z}} \mathbb{C}_p(i)^{G_K}$. For $i = 0$, Tate's theorem implies that $\mathbb{C}_p^{G_K} = K$. For $i \neq 0$, note that $\mathbb{C}_p(n) = \mathbb{C}_p \otimes \omega_p^n$, so that $\mathbb{C}_p(i)^{G_K} = D_{\mathbb{C}_p}(\omega_p^n)$. Thus $\mathbb{C}_p(i)^{G_K}$ has dimension 0 or 1. If it has dimension 1, we conclude that ω_p^n is $\mathbb{C}_p$-admissible. But the image of I_K under ω_p^n is not finite for $n \neq 0$. Thus the dimension is zero.

why is $\mathbb{C}_p(n)$ this tensor product?

Why is $\omega_p^n(I_K)$ not finite for $n \neq 0$?

To prove the first part, note first that $\mathrm{Frac}(B_{\mathrm{HT}}) = \mathbb{C}_p(t)$ as a ring, so that $\mathrm{Frac}(B_{\mathrm{HT}})^{G_K} = \mathbb{C}_p(t)^{G_K} \subset \mathbb{C}_p((T))^{G_K}$ (where we extend the action of G_K on $\mathbb{C}_p(t)$). This action is compatible with

the G_K action on $\mathrm{Frac}(B_{\mathrm{HT}})$ since it is obviously compatible on polynomials and thus on rational functions. As before, only $i = 0$ contributes, so this is again $K = B_{\mathrm{HT}}^{G_K}$.

Finally, suppose $L \subset B_{\mathrm{HT}}$ is a $\mathbb{Q}_p$-line that is G_K-invariant. Then $L = \mathbb{Q}_p v$ for some v; it is easily seen that in order for this to be G_K-invariant, we must have $v = at^i$ for some i, since otherwise the different action on different powers of t make it impossible for v to be G_K-invariant. But $at^i \in B_{\mathrm{HT}}^*$ and we are done. Thus B_{HT} is $(\mathbb{Q}_p, G_K)$-regular. □

Definition 145. V is *Hodge-Tate* if V is B_{HT}-admissible. If V is Hodge-Tate, we write $D_{\mathrm{HT}}(V) = D_{B_{\mathrm{HT}}}(V)$.

Definition 146. Note that if V is Hodge-Tate, then $D_{\mathrm{HT}}(V) = \oplus_{n\in\mathbb{Z}}(V \otimes \mathbb{C}_p(n))^{G_K}$. The i for which $\dim(V \otimes \mathbb{C}_p(i))^{G_K} > 0$ are called the *Hodge-Tate weights of* V, and in this case $\dim(V \otimes \mathbb{C}_p(i))^{G_K}$ is called the multiplicity of the Hodge-Tate weight $-i$.

In other words, $k \in \mathbb{Z}$ is a Hodge-Tate weight of V of multiplicity $\dim(V \otimes \mathbb{C}_p(n))^{G_K}$.

Lemma 147. *If V is a dimension d representation of G_K, then V is Hodge-Tate if and only if the sum of the multiplicities of the Hodge-Tate weights of V is d.*

Proof. Obvious. □

For example, ω_p is Hodge-Tate of weight -1, and is not $\mathbb{C}_p$-admissible.

Proposition 148. *V is Hodge-Tate if and only if $V \otimes \mathbb{C}_p \cong \oplus_{k\in\mathbb{Z}}\mathbb{C}_p(k)^{m_k}$ as a $\mathbb{C}_p$-semi-linear representation of G_K. In this case $\sum m_k = \dim V$, and m_k is the multiplicity of the Hodge-Tate weight k.*

Thus a Hodge-Tate representation is not exactly the trivial semi-linear representation.

Proof. $\Leftarrow$:

$$V \otimes B_{\mathrm{HT}} = (V \otimes_{\mathbb{Q}_p} \mathbb{C}_p) \otimes_{\mathbb{C}_p} B_{\mathrm{HT}} = \oplus_k \mathbb{C}_p(k)^{m_k} \otimes \oplus_n \mathbb{C}_p(n) = \oplus_{k,n}\mathbb{C}_p(n+k)^{m_k}$$

and thus

$$D_{\mathrm{HT}}(V) = \oplus_{k,n}(\mathbb{C}_p(n+k)^{G_K})^{m_k}$$

and we know from the above analysis that $\mathbb{C}_p(n+k)^{G_K} = 0$ unless $n + k = 0$. Thus

$$D_{\mathrm{HT}}(V) = \oplus_k K^{m_{-n}}$$

so that $\dim D_{\mathrm{HT}}(V) = \sum_n m_{-n} = d$ where we know the sum is in fact d since $\dim V \otimes \mathbb{C}_p = d$. Thus V is Hodge-Tate, and the Hodge-Tate weight k has multiplicity m_k.

$\Rightarrow$: Very similar. Exercise. Exercise

□

Theorem 149. *V is Hodge-Tate if and only if φ acts semi-simply on $D_{\mathrm{sen}}(V)$ with integral eigenvalues. If this holds, the eigenvalues of φ are the Hodge-Tate weights of V, counted with multiplicity.*

Proof. If V is Hodge-Tate, then $V \otimes \mathbb{C}_p = \oplus\mathbb{C}_p(k)^{m_k}$ with $\sum m_k = d$. Now, $(V \otimes \mathbb{C}_p)^H$ is a $\hat{K}_\infty$ vector space isomorphic to $\oplus(\mathbb{C}_p(k)^{m_k})^H$. But V is always H-admissible (Proposition **??**), so this is just $\oplus\hat{K}_\infty(k)^{m_k}$

Why does the last direct sum follow?
why is this the action? Presumably because it acts thru the log map

Now, φ acts on $K_\infty(k)$ as multiplication by k. Thus φ is semi-simple with eigenvalues as stated. □

Thus Sen theory is in some sense more general than Hodge-Tate representations: For every V, there is φ. When the Hodge-Tate-Sen weights are rational integers and φ is semi-simple, V is Hodge-Tate and we retrive the Hodge-Tate weights.

Note by the way that ω_p^λ for $\lambda \notin \mathbb{Z}$ is never Hodge-Tate because there are no G_K-invariants ($n+\lambda \neq 0$ for any n). Thus semi-simple is not a sufficient condition in the above theorem - integrality of weights really is necessary as well.

Corollary 150. *If $0 \to U \to V \to W \to 0$ is an exact sequence of G_K representations and if U, W are Hodge-Tate with no weights in common, then V is Hodge-Tate.*

Proof. $D_{\text{sen}}(V)$ is an extension of $D_{\text{sen}}(U)$ by $D_{\text{sen}}(W)$, i.e.

$$0 \to D_{\text{sen}}(U) \to D_{\text{sen}}(V) \to D_{\text{sen}}(W) \to 0$$

is exact as modules with φ actions (note that a priori this sequence is not short exact since the final map need not be surjective; in this case, however, it is by dimensional analysis once we know that V is Hodge-Tate). The actions of φ on $D_{\text{sen}}(U), D_{\text{sen}}(W)$ are semi-simple with integral eigenvalues since U, W are Hodge-Tate. It is thus clear that $D_{\text{sen}}(V)$ has integral eigenvalues. But if the weights are distinct, this sequence splits under the φ action, so the action of φ on $D_{\text{sen}}(V)$ is semi-simple as well. □

why split?

Remark 151. This corollary need not in fact hold if the weights of U and W are not disjoint. For example, let (ρ, V) be a representation with

$$\rho(g) = \begin{pmatrix} 1 & \alpha(g) \\ 0 & 1 \end{pmatrix}, \qquad \alpha : G_K \to (\mathbb{Q}_p, +)$$

and choose α such that $\alpha(I_K)$ is infinite; we can do this by Class Field Theory since $\mathcal{O}_K^* \cong I(K^{\text{ab}}/K)$. We then get an exact sequence $0 \to \mathbb{Q}_p \to V \to \mathbb{Q}_p \to 0$. But V is not Hodge-Tate, for if it were, its weights would be $0, 0$, so it would be $\mathbb{C}_p$-admissible so the image of inertia would be finite.

To figure out: why would its weights be $0, 0$. Also, why do weights of 0 imply $\mathbb{C}_p$-admissible?

Remark 152. If K'/K is a finite extension, then V is Hodge-Tate over G_K if and only if V is Hodge-Tate over $G_{K'}$.

Why is this true?

5.3.5 Tate elliptic curves over a p-adic field

Recall that if $E/\mathbb{C}$ is an elliptic curve, we can write

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda = \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}w), \quad w \in \mathbb{C} - \mathbb{R}$$

Now, $\mathbb{C}/\mathbb{Z} \xrightarrow[\cong]{e^{2\pi i \cdot}} \mathbb{C}^*$, so

$$E(\mathbb{C}) \cong \mathbb{C}^*/q^{\mathbb{Z}}, \qquad q = e^{2\pi i w}$$

We denote this curve E_q and note that over $\mathbb{C}$, every elliptic curve is E_q for some q; an equation for $E_q(\mathbb{C})$ is

$$y^2 + xy = x^3 - b_2(q)x - b_3(q)$$

where

$$b_2(q) = 5 \sum_{n \geq 1} n^3 \frac{q^n}{1 - q^n}$$

$$b_3(q) = \sum_{n \geq 1} \left(7n^5 + 5n^3\right) \frac{q^n}{12(1 - q^n)}$$

from the Weierstrass theorems. Additionally,

$$j(E_q) = j(q) = \frac{1}{q} + 744 + 19688q + \cdots \in \mathbb{Z}[[q]] + \frac{1}{q}$$

Now, over $\mathbb{Q}_p$ instead of $\mathbb{C}$, if $q \in \mathbb{Q}_p^*$ is well-chosen, the series for b_2, b_3 will converge and we will get $E_q \cong \mathbb{Q}_p^*/q^{\mathbb{Z}}$.

Theorem 153. *(Tate) Let $K/\mathbb{Q}_p$ be a finite extension, $q \in K^*$, $|q| < 1$. Then $b_2(q), b_3(q)$ converge, and*

$$E_q : y^2 + xy = x^3 - b_2(q)x - b_3(x)$$

is an elliptic curve over K (that is, its discriminant is nonzero). Further, if K'/K is any algebraic extension, then there is a natural isomorphism of groups $E_q(K') \cong K'^*/q^{\mathbb{Z}}$ (natural in the sense that the appropriate diagrams commute; in particular, if K'/K is Galois, the isomorphism is compatible with the Galois action).

We won't give a formal proof of this. Note that most of this is purely a computation; the final statement reduces to an equality of power series; these power series are equal over $\mathbb{C}$, thus over $\mathbb{Q}$, thus over $\mathbb{Q}_p$ and thus over K.

Note that in contrast to the $\mathbb{C}$ case, not all elliptic curves over K are E_q for some q with $|q| < 1$.

Also note that over $\mathbb{C}$, there is no Galois action since $\mathbb{C}$ is algebraically closed.

Proposition 154. *Every elliptic curve E/K such that $j(E) \in K - \mathcal{O}_K$ (i.e. such that $|j(E)| > 1$) becomes isomorphic to some E_q after replacing K by a finite extension.*

Proof. If $|j(E)| > 1$, then there is some $q \in K$ with $|q| < 1$ such that $j(q) = j(E)$. This is so since for $|q| < 1$, $|j(q)| > 1$; solve the equation $j(E) = \frac{1}{q} + 744 + \cdots$ for q by inverting the series. Then $j(E_q) = j(E)$. But two elliptic curves with the same j-invariant are isomorphic after a finite extension. □

The converse is also true - if $j(E) \in \mathcal{O}_K$, then E is not isomorphic to E_q in any finite extension.

Looking at p^n-torsion, then,

$$E_q(\bar{K})[p^n] = (\bar{K}^*/q^{\mathbb{Z}})[p^n]$$

and we have an exact sequence

$$1 \to \mu_{p^n}(\bar{K}) \to (\bar{K}^*/q^{\mathbb{Z}})[p^n] \to q^{1/p^n}\mathbb{Z}/q^{\mathbb{Z}} \to 1$$

since, first, all p^n roots of unity in $\bar{K}$ are clearly p^n torsion, and none of those are of the form $q^{\mathbb{Z}}$ since $|q| < 1$, so the first map is injective, and it is also clear that the remaining p^n torsion points are as given in the exact sequence.

Now, the cardinalities of the first and last groups in the exact sequence are both p^n, so that the cardinality of the middle group is $(p^n)^2$.

Additionally, G_K acts on $(\bar{K}^*/q^{\mathbb{Z}})[p^n]$, and $\mu_{p^n}(\bar{K})$ is stable under that G_K action, so we get a quotient action. Now take the projective limit, noting that the exact sequence is compatible with the maps and the G_K action is as well, to get

$$\begin{array}{ccccccccc} 1 & \to & \varprojlim \mu_{p^n}(\bar{K}) & \to & T_p(E_q) & \to & \varprojlim q^{1/p^n}\mathbb{Z}/q^{\mathbb{Z}} & \to & 1 \\ 0 & \to & \mathbb{Z}_p & \to & T_p(E_q) & \to & \mathbb{Z}_p & \to & 0 \end{array}$$

The Galois action on the left-hand $\mathbb{Z}_p$ is ω_p since we defined ω_p precisely from the action on the inverse limit of the roots of unity. Since $\det(T_p(E)) = \omega_p$, the Galois action on the right-hand $\mathbb{Z}_p$ is trivial. Using the notation $\mathbb{Z}_p(i)$ as before for $\mathbb{C}_p(i)$, we can write this exact sequence, after tensoring with $\mathbb{Q}_p$, as

$$0 \to \mathbb{Q}_p(1) \to V_p(E_q) \to \mathbb{Q}_p \to 0$$

Corollary 155. *If E/K is an elliptic curve with $j(E) \in K - \mathcal{O}_K$, then $V_p(E)$ is Hodge-Tate with Hodge-Tate weights $0, -1$.*

Proof. The property of being Hodge-Tate, and the Hodge-Tate weights, are invariant under finite extension. So assume $E = E_q$ for some q. Then $V_p(E_q)$ is an extension of $\mathbb{Q}_p(0)$ with Hodge-Tate weight 0 by $\mathbb{Q}_p(1)$ with Hodge-Tate weight -1. Since the Hodge-Tate weights are disjoint, it follows that $V_p(E_q)$ is also Hodge-Tate and the weights are as given. □

Note that

$$H^1_{\text{et}}(E, \mathbb{Q}_p) = V_p(E)^* = V_p(E) \otimes \omega_p^{-1} =_{\text{df}} V_p(E)(-1)$$

so that $H^1_{\text{et}}(E, \mathbb{Q}_p)$ is Hodge-Tate of weights $0, 1 = \{0, -1\} + 1$.

Note also that the exact sequence

$$0 \to \mathbb{Q}_p(1) \to V_p(E_q) \to \mathbb{Q}_p \to 0$$

for if it were, we'd get a lift from $q^{1/p^n}\mathbb{Z}/q^{\mathbb{Z}}$ to $(\bar{K}^*/q^{\mathbb{Z}})[p^n]$ invariant under G_K on all p^n roots of unity for all n; this is impossible. This exact sequence determines q up to $q \mapsto q^r$ for $r \in \mathbb{Q}$; thus $V_p(E)$ determines E_q up to isogeny. The exact sequence does, however, split after tensoring with $\mathbb{C}_p$.

Notes say "torsion in K, impossible"

Theorem 156. *(Tate) Actually, any elliptic curve E/K has $V_p(E)$ Hodge-Tate with weights $0, -1$.*

In general, $V_p(E)$ is irreducible, so the general case is not as easy as the above; the proof proceeds by tensoring with $\mathbb{C}_p$.

Theorem 157. *(Raynaud): Any abelian variety over K of dimension g is Hodge-Tate with weights $0, -1$, each of multiplicity g.*

Theorem 158. *(Faltings) [first version] Let X/K be a proper and smooth variety of dimension d. Then for $0 \le n \le 2d$, $H^n_{\text{et}}(X, \mathbb{Q}_p)$ is Hodge-Tate.*

Note the following facts about cohomology:

- If X is a real manifold, then the deRham cohomology is defined as

$$H^n_{\text{dR}}(X, \mathbb{C}) = \frac{\{\text{closed smooth } n\text{-differential forms}/X\}}{\{\text{exact smooth } n\text{-differential forms}/X\}}$$

- If X is an algebraic variety over $\mathbb{C}$, proper and smooth, then the Hodge decomposition of X is given by

$$H^n_{\text{dR}}(X(\mathbb{C}), \mathbb{C}) \cong \bigoplus_{p+q=n} H^{p,q}(X(\mathbb{C}), \mathbb{C})$$

  The isomorphism is canonical, and the groups $H^{p,q}$ satisfy:

  1. $\dim H^{p,q}(X(\mathbb{C}), \mathbb{C}) = \dim H^{q,p}(X(\mathbb{C}), \mathbb{C})$

2. $H^{p,q}(X(\mathbb{C}),\mathbb{C}) = H^p(X,\Omega_X^q)$ where X is the underlying algebraic variety and Ω_X^q is the coherent sheaf $\Lambda^q\Omega_X$ and Ω_X is the sheaf of algebraic differential forms over X (which is larger than the sheaf of smooth forms).

- If X is an algebraic variety, proper and smooth over K (assume $\operatorname{char} K = 0$ for simplicity) we get a similar theory with slightly less information. Grothendieck defined a purely algebraic deRham cohomology $H^n_{\mathrm{dR}}(X)$ which is a K-vector space such that for $K = \mathbb{C}$, there is a canonical isomorphism $H_{\mathrm{dR}}(X(\mathbb{C}),\mathbb{C}) \cong H_{\mathrm{dR}}(X)$. $H^n_{\mathrm{dR}}(X)$ is defined to be the hypercohomology of the functor Γ of global sections applied to the complex of sheaves

$$0 \to \Omega_x \xrightarrow[d]{} \Omega^2_X \xrightarrow[d]{} \Omega^3_x \xrightarrow[d]{} \cdots \xrightarrow[d]{} \Omega^d_X \to 0$$

  $H^n_{\mathrm{dR}}(X)$ comes with a decreasing filtration

$$\cdots \supset F^pH^n_{\mathrm{dR}}(X) \supset F^{p+1}H^n_{\mathrm{dR}}(X) \supset \cdots$$

  and for $p \ll 0$, $F^pH^n_{\mathrm{dR}}(X) = H^n_{\mathrm{dR}}(X)$; for $p \gg 0$, $F^pH^n_{\mathrm{dR}}(X) = 0$. Additionally,

$$F^pH^n_{\mathrm{dR}}(X)/F^{p+1}H^n_{\mathrm{dR}}(X) = H^p(X,\Omega_X^{n-p})$$

  so we get the same dimensional result as in the complex case - the filtration gives quotients, not subspaces. Of course the associated exact sequence splits, but not canonically.

This arises from spectral sequences - see appendix in Eisenbud

Theorem 159. *(Faltings) [complete version] Let X/K be a proper and smooth variety, $[K : \mathbb{Q}_p] < \infty$. Then*

$$H^n_{\mathrm{et}}(X,\mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \mathbb{C}_p \cong \bigoplus_q \mathbb{C}_p(-q) \otimes H^{n-q}(X,\Omega_X^q)$$

as groups with G_K action.

The Galois action on the left arises from the action of G_K on each factor; on the right, the Galois action on $\mathbb{C}_p(-q)$ is clear; the Galois action on cohomology is trivial.

Interpreted as a statement about $\mathbb{C}_p$-vector spaces, we get the same dimensional statement as before. But interpreted as G_K-modules, the right-hand side is

$$\bigoplus_q \mathbb{C}_p(-q)^{m_q}, \qquad m_q = \dim H^{n-q}(X,\Omega_X^q)$$

and we get that $H^n_{\mathrm{et}}(X,\mathbb{Q}_p)$ is Hodge-Tate with weights q and multiplicities m_q.

This theorem arose by analogy with the complex situation. Over $\mathbb{C}$, when you tensor with $\mathbb{C}$, you get a direct sum decomposition, so try the same thing over $\mathbb{Q}_p$. Over $\mathbb{C}$, it turns out that the process works because complex conjugation exists (i.e. things are compatible with the Galois action of $\mathbb{C}/\mathbb{R}$). So the tensor product here is with $\mathbb{C}_p$ with its Galois action. This is where the entire idea of tensoring with big rings to get information about the representation came from.

Another way of stating this theorem is that

$$D_{HT}(H^n_{\mathrm{et}}(X,\mathbb{Q}_p)) = \bigoplus_q H^{n-q}(X,\Omega_X^q)$$

as a graded vector space. Thus from étale cohomology, one can retrieve an approximation of deRham cohomology.

Finally, note that Faltings' theorem generalizes Tate's theorem (let X be of dimension 1).

5.3.6 deRham representations and the mysterious functor

Grothendieck wanted to be able to retrieve the entire deRham cohomology, which required a bigger ring. Fontaine considered a ring B_{dR}^+ with a Galois action of G_K and a topology; in this ring, there exists t such that $gt = \omega_p(g)t$ (i.e. the action of $g \in G_K$ on t is given by multiplying $\omega_p(g) \in \mathbb{C}_p$ by t). B_{dR}^+ turns out to be a DVR with uniformizer t and residue field $\mathbb{C}_p$; set $B_{\mathrm{dR}} = \mathrm{Frac}(B_{\mathrm{dR}}^+) = B_{\mathrm{dR}}^+[t^{-1}]$. Then $B_{\mathrm{dR}}^{G_K} = K$ and $F^k B_{\mathrm{dR}} = t^k B_{\mathrm{dR}}^+$ for $k \in \mathbb{Z}$.

Definition 160. A representation V is *deRham* if it is B_{dR}-admissible.

If V is deRham, then $D_{\mathrm{dR}}(V)$ is a K-vector space of dimension $\dim V$, with a decreasing filtration

$$F^i D_{\mathrm{dR}}(V) = (t^i B_{\mathrm{dR}}^+ \otimes V)^{G_K}$$

Since D_{dR} is finite-dimensional, we have $F^i D_{\mathrm{dR}}(V) = D_{\mathrm{dR}}(V)$ for $i \ll 0$ and $F^i D_{\mathrm{dr}}(V) = 0$ for $i \gg 0$.

We can say more explicitly what the dimensions of the filtration quotients are:

Proposition 161. *If V is deRham, then V is Hodge-Tate and $D_{\mathrm{HT}}(V)$ is the graded space attached to the filtered space $D_{\mathrm{dR}}(V)$; that is,*

$$D_{\mathrm{HT}}(V) = \oplus_{i \in \mathbb{Z}} F^i D_{\mathrm{dR}}(V)/F^{i+1} D_{\mathrm{dR}}(V)$$

Concretely, i is a Hodge-Tate weight of V of multiplicity $m_i = \dim_K F^i D_{\mathrm{dR}}(V)/F^{i+1} D_{\mathrm{dR}}(V)$.

Proof.

$$\frac{F^i D_{\mathrm{dR}}(V)}{=} \frac{[F^{i+1} D_{\mathrm{dR}}(V)}{V \otimes t^{i+1} B_{\mathrm{dR}}^+)^{G_K}} \frac{(V \otimes t^i B_{\mathrm{dR}}^+)^{G_K}}{} \hookrightarrow (V \otimes \mathbb{C}_p(i))^{G_K}$$

The inclusion is seen by starting with the exact sequence

$$0 \to V \otimes_{\mathbb{Q}_p} t^{i+1} B_{\mathrm{dR}}^+ \to V \otimes_{\mathbb{Q}_p} t^i B_{\mathrm{dR}}^+ \to V \otimes_{\mathbb{Q}_p} (t^i B_{\mathrm{dR}}^+)/(t^{i+1} B_{\mathrm{dR}}^+) \to 0$$

and noting that $B_{\mathrm{dR}}^+/tB_{\mathrm{dR}}^+ = \mathbb{C}_p$, so that the quotient on the right is $V \otimes \mathbb{C}_p(i)$. Taking invariants under G_K gives

$$0 \to 0 \to (V \otimes_{\mathbb{Q}_p} t^{i+1} B_{\mathrm{dR}}^+)^{G_K} \to (V \otimes_{\mathbb{Q}_p} t^i B_{\mathrm{dR}}^+)^{G_K} \to (V \otimes_{\mathbb{Q}_p} (t^i B_{\mathrm{dR}}^+)/(t^{i+1} B_{\mathrm{dR}}^+))^{G_K}$$

The final map is not in general surjective. If for example G_K were finite with order not a multiple of p, we could average the elements in the inverse image to show that the map was surjective, but in general it is not; the sequence extends to a long exact sequence in cohomology. But this sequence gives the inclusion above, and that is good enough, for since V is deRham, we have

$$d = \sum_i \dim_K F^i D_{\mathrm{dR}}(V)/F^{i+1} D_{\mathrm{dR}}(V) \leq \sum_i (V \otimes \mathbb{C}_p(i))^{G_K} = \sum_i \dim(V \otimes B_{\mathrm{HT}}(V))^{G_K} \leq d$$

which means that equality holds for every i. Thus V is Hodge-Tate with Hodge-Tate weights as given above. The decomposition of $D_{\mathrm{HT}}(V)$ also follows. □

Theorem 162. *(Faltings) If X/K is proper and smooth with $[K : \mathbb{Q}_p]$ finite, then*

$$D_{\mathrm{dR}}(H^n(X, \mathbb{Q}_p)) = H_{\mathrm{dR}}(X)$$

as filtered K-vector spaces. Note that the left-hand side is a K-vector space since $B_{\mathrm{dR}}^{G_K} = K$.

Corollary 163. *$H_{\mathrm{et}}^n(X, \mathbb{Q}_p)$ is a deRham representation since $\dim H^n(X, \mathbb{Q}_p) = \dim H_{\mathrm{dR}}(X)$.*

Thus deRham implies Hodge-Tate.

5.3.7 Crystalline representations

B_{crys} is a subring of B_{dR} that is not a field. It also contains t, and has a decreasing filtration given by $F^i B_{\text{crys}} = B_{\text{crys}} \cap F^i B_{\text{dR}}$. Additionally,

$$F^i B_{\text{crys}} / F^{i+1} B_{\text{crys}} \cong \mathbb{C}_p(i)$$

Finally, $B_{\text{crys}}^{G_K} = K_0$, where K_0 is the largest unramified extension of $\mathbb{Q}_p$ contained in K.

Definition 164. V is *crystalline* if V is B_{crys}-admissible.

Proposition 165. *If V is crystalline, then V is deRham.*

Proof. This follows from the general fact that if $B \subset A$ are (F, G)-regular rings and V is B-admissible, then V is A-admissible, proven by showing that the A-semi-linear representation is trivial as well. □

How does this proof go?

Theorem 166. *(Faltings) Let X/K be a proper and smooth variety with $[K : \mathbb{Q}_p]$ finite which also has a proper and smooth model over $\mathcal{O}_K$. Then $H^n_{\text{et}}(X, \mathbb{Q}_p)$ is crystalline, and*

$$D_{\text{crys}} H^n_{\text{et}}(X, \mathbb{Q}_p) = H^n_{\text{crys}}(\bar{X})$$

where $\bar{X}$ is the special fiber of the model.

This is somehow the same as having good reduction.

We have thus shown the following inclusions:

$$\text{crystalline} \subset \text{deRham} \subset \text{Hodge-Tate} \subset \text{general representation}$$

All of these inclusions are proper. We have already seen that, for example, ω_p^λ is not Hodge-Tate unless λ is integral; in general, a representation is Hodge-Tate only if its Hodge-Tate-Sen weights are integral.

The proof that there are Hodge-Tate representations that are not deRham uses deformation theory to show that the dimension of the space of Hodge-Tate representations (as a vector space over some field) exceeds that of the space of deRham representations.

Proposition 167. *If $\chi : G_K \to L^*$ is a character, where $[K : \mathbb{Q}_p] < \infty, [L : \mathbb{Q}_p] < \infty$, then TFAE:*

1. *χ is Hodge-Tate as a representation of degree $[L : \mathbb{Q}_p]$ over $\mathbb{Q}_p$,*
2. *χ is deRham,*
3. *$\chi \circ Art : K^* \to L^*$, a character of K^*, is such that for some open (i.e. finite index) subgroup U of $\mathcal{O}_K^*$ and $n_\sigma \in \mathbb{Z}$,*
$$(\chi \circ Art)|_U\ (x) = \prod_{\sigma \in \text{Hom}(K, \bar{L})} \sigma(x)^{n_\sigma}$$

If these conditions hold and if L contains the normal closure of K, then the Hodge-Tate weights of χ as a $\mathbb{Q}_p$-representation are the n_σ with multiplicity $[L : K]$. (Note that if two of the n_σ are the same, then the multiplicity of n_σ will be $2[L : K]$, and so on). Thus the sum of the weights, counting multiplicities, is $[L : K][K : \mathbb{Q}_p] = [L : \mathbb{Q}_p]$.

Finally, χ is crystalline if and only if (3) holds for $U = \mathcal{O}_K^*$.

Remark 168. Note that since χ maps into L^*, it factors through G_K^{ab}, and $K^* \hookrightarrow G_K^{\mathrm{ab}}$ with dense image. Under the Artin map, $\mathcal{O}_K^*$ maps to inertia in G_K^{ab}, so $U \subset \mathcal{O}_K^*$ means that U corresponds to a subgroup of inertia in G_K^{ab}.

Remark 169. Note that the product in (3) has no *a priori* reason to be in L^*.

Remark 170. Note that for K'/K finite, χ is Hodge-Tate over K if and only if it is Hodge-Tate over K', and that $G_{K'}$ is open in G_K so that $I_{K'}$ is open in I_K, so it is not surprising that some open subgroup property is involved.

Remark 171. (3) means that χ is locally algebraic, while the condition on crystallinity means that χ is algebraic.

Remark 172. Note that if all $n_\sigma = 0$, then $\chi = 0$ on some open subgroup U, so that χ is potentially unramified and thus deRham; crystalline means that χ is unramified. So crystalline generalizes unramified.

Proof. Start with the case $K = L = \mathbb{Q}_p$; then $\chi : G_{\mathbb{Q}_p} \to \mathbb{Q}_p^*$. If χ is Hodge-Tate, then it has weights n, so that $\chi\omega_p^n$ has weight 0, so is $\mathbb{C}_p$-admissible, so inertia has finite image. Thus $\chi\omega_p^n \circ Art$ has finite image on $\mathbb{Z}_p^*$ and thus trivial image on some $U \subset \mathbb{Z}_p^*$ of finite index (namely the kernel). But

$$(\chi\omega_p^n \circ Art)(x) = (\chi \circ Art)(\omega_p^n \circ Art)(\chi \circ Art)(x) \cdot x^{-n}$$

On U, this is trivial, so that $\chi \circ Art(x) = x^n$ on U; this implies (3) with $n_\sigma = n$ (there is only one σ). Thus (1) $\Rightarrow$ (3).

(3) $\Rightarrow$ (1) is simply the reverse of this argument.

We already know that (2) $\Rightarrow$ (1), so it remains to show that (3) $\Rightarrow$ (2). For this, choose $K'/\mathbb{Q}_p$ such that $N_{K'/\mathbb{Q}_p}(\mathcal{O}_{K'}^*) \subset U$; this is possible since by Class Field Theory, the image of the norm map corresponds to inclusion of Galois groups. Thus (again using CFT for the first equality)

What part of CFT implies this?

$$(\chi|_{G_{K'}}) \circ Art_{K'} = \chi \circ Art \circ N_{K'/\mathbb{Q}_p} : K'^* \to \mathbb{Q}_p^*$$

on $\mathcal{O}_K^* = (N_{K'/\mathbb{Q}_p}(\cdot))^n$, so that $\chi|_{I_{K'}} = \omega_p^{-n}|_{I_{K'}}$ and thus $\chi|_{G_{K'}}$ deRham implies that χ_{G_K} deRham. □

6 Galois Representations of Number Fields

We now return to our main object of study. Let K be a finite algebraic extension of $\mathbb{Q}$, and assume

$$\rho : G_K \to GL_n(\mathbb{Q}_\ell)$$

is a continuous ℓ-adic representation. We wish to understand which representations arise from geometry.

We know (see the section on Étale Cohomology) that the Étale cohomology of a proper and smooth variety given representations, which are geometric. If we allow twists of these representations by ω_p^n, this turns out to cover all geometric representations.

Geometric representations are almost everywhere unramified because X has good reduction almost everywhere.

Why does this follow?

Thus if ρ is geometric, then

1. ρ is unramified almost everywhere,
2. for all places v of K such that $v \mid l$, $\rho|_{G_{K_v}}$ is deRham by Faltings' theorem. (Note that $\rho|_{G_{K_v}}$ is defined by the inclusion $G_{K_v} \hookrightarrow G_K$ that is defined up to conjugacy.)

Conjecture 173. (Fontaine-Mazur, 1994) Every representation $\rho : G_K \to GL_n(\mathbb{Q}_\ell)$ satisfying (1) and (2) is geometric.

This conjecture is widely believed to be true, but very few specific cases have actually been proven. To see why the conjecture is important, note that is ρ is geometric, then ρ also satisfies

3. ρ is rational, i.e. the characteristic polynomial of $\rho(\mathrm{Frob}_v)$ for v any place of K note dividing ℓ where ρ is unramified lies in $\mathbb{Q}[x]$,
4. ρ has a weight $w \in \mathbb{Z}$, i.e. eigenvalues are Weil numbers of weight w.

Thus a corollary of the conjecture is that any representation satisfying (1) and (2) also satisfies (3) and (4). But (1) is a very weak condition - most representations are unramified almost everywhere, and (2) is also quite weak, particularly for $K = \mathbb{Q}$. (3) and (4), however, are strong conditions, as among other things they are statements that hold almost everywhere.

Theorem 174. *If K is a number field, ρ an abelian representation of G_K (that is, $\rho(G_K)$ is abelian), then the Fontaine-Mazur conjecture holds.*

Proof. (Sketch) First, assume ρ is a character $\chi : G_K \to L^*$ with $[L : \mathbb{Q}_\ell] = n$. Note that any abelian representation is a sum of characters over some extension. Then by the hypotheses of F-M, $\chi|_{G_{K_v}}$ is deRham, so that it has the form

Exercise

$$\chi|_{G_{K_V}} = \prod_\sigma \sigma(x)^{n_\sigma}$$

on some open subgroup of K_v^* for $v \mid \ell$. Thus by Theorem **??**, χ is the λ-adic realization of an algebraic Hecke character ψ, for some $\lambda \mid \ell$. Hence it suffices to show that every algebraic Hecke character is geometric. This was done in the exercises; here is an outline. Recall that K has a maximal CM subfield K_{CM}, and that if $\psi : \mathbb{A}_K^*/K^* \to \mathbb{C}^*$ is algebraic, then there is some $\psi_{\mathrm{CM}} : \mathbb{A}_{K_{\mathrm{CM}}}^*/K_{\mathrm{CM}}^* \to \mathbb{C}^*$ algebraic such that

$$\psi = (\psi_{\mathrm{CM}} \circ N_{K/K_{\mathrm{CM}}})\epsilon$$

where ϵ is a character with finite image. (Exercise Set 4, part 2, exercise 3). So if the result holds for K_{CM}, then $\psi_{\mathrm{CM}} \circ N_{K/K_{\mathrm{CM}}}$ is geometric , and ϵ has finite image thus is geometric, so that the tensor product is geometric by the Kunneth formula.

Why is the norm geometric? Or is that not needed? I totally missed this.

When K is CM, (see exercises) □

Theorem 175. *(Kisin, Wiles, Taylor, Khare) Assume $K = \mathbb{Q}, n = 2$, i.e. $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_\ell)$. Suppose ρ satisfies (1) and (2). If, in addition,*

Why is ϵ geometric?

1. $\operatorname{tr}\rho(c) = 0$ *where c is the nontrivial element of* $\mathrm{Gal}(\mathbb{Q}/\mathbb{R})$ *(the possibilities for the trace are $-2, 0, 2$ depending on the combination of ± 1 that ρ has as eigenvalues), and*
2. $\rho|_{G_{\mathbb{Q}_\ell}}$ *(which is deRham) has distinct Hodge-Tate weights*

then ρ is geometric.

These two theorems are all the results that are known regarding the Fontaine-Mazur conjecture.

Note that we have two notions of weights - the Weil numbers, which are global, or *motivic*, weights, and the Hodge-Tate weights, which are local weights associated to an ℓ-adic representation of an ℓ-adic field.

Example 176. $\rho = \omega_\ell, K = \mathbb{Q}$. The global weight is $w = -2$, and the Hodge-Tate weight of $\rho|_{G_{\mathbb{Q}_\ell}}$ is -1.

why are these the weights?

Example 177. Let $E/\mathbb{Q}$ be an elliptic curve, $\rho = V_\ell(E), K = \mathbb{Q}$. The global weight is -1 ($V_\ell(E)$ is the dual of H^1, which has weight 1), and the Hodge-Tate weights of $\rho|_{G_{\mathbb{Q}_\ell}}$ are $0, -1$.

Theorem 178. *If ρ is a representation of $G_{\mathbb{Q}}$ satisfying (1)-(4) with global weight w, let $k_1, \ldots, k_n$ be the Hodge-Tate weights of $\rho|_{G_{\mathbb{Q}_\ell}}$. Then*

$$k_1 + \cdots + k_n = \frac{nw}{2}$$

There is a similar formula for $K \neq \mathbb{Q}$.

Proof. Look first at $\det\rho$. It will have Hodge-Tate weight $k_1 + \cdots + k_n$ and is Hodge-Tate. Its global weight is nw since all the eigenvalues of Frob have the same absolute value, and its dimension is 1, so it suffices to prove the result for a character.

"$D_B(V)$ is a graded vector space; preserved under Λ^n"

But $\det\rho = \omega_\ell^d\epsilon$. ϵ maps into roots of unity, so won't change either the global weight or the Hodge-Tate weights. The result is true for ω_ℓ^d. □

7 Galois Cohomology

7.1 Introduction and Motivation

The results of Galois cohomology are almost all due to Tate. Before studying this subject, and as motivation, we first compare Galois representations in four different settings: $L = \mathbb{C}$, general representations with $[L : \mathbb{Q}_\ell] < \infty$, geometric representations with $[L : \mathbb{Q}_\ell] < \infty$, and L a finite field (with the discrete topology):

$\rho : G_K \to GL_L(V)$	$L = \mathbb{C}$	$[L : \mathbb{Q}_\ell] < \infty$ ρ arbitrary	$[L : \mathbb{Q}_\ell] < \infty$ ρ geometric	L finite
finite image	Yes	No	No	No
unramified a.e.	Yes (finite image)	No (not obvious)	Yes	Yes (finite image)
algebraic	Yes (roots of unity)	No	Yes (Deligne)	Doesn't make sense
semisimple	Yes (representation of finite group)	No	Should be so, not known	No in general

For representations that are not semi-simple, it is natural to want to understand how the extensions are put together; this leads us to group cohomology.

Thus let L be finite over $\mathbb{Q}_\ell$ with ring of integers $\mathcal{O}_L$ and uniformizer π, and write $k_L = \mathcal{O}_L/(\pi)$. We will show how a representation over $\mathbb{Q}_\ell$ induces a representation over k_L. Many of the initial definitions and statements below hold more generally, but we will be applying them in this situation.

Definition 179. Let V be an L-vector space of dimension $d < \infty$, and Λ an $\mathcal{O}_L$-submodule of V. The following are equivalent:

1. Λ is free over $\mathcal{O}_L$ of rank d;
2. Λ is finitely generated over $\mathcal{O}_L$ and Λ generates V (that is, $\Lambda \otimes_{\mathcal{O}_L} L \cong V$).

Such a Λ is called a *lattice* of V.

In order for this definition to make sense, we must show that the two statements really are equivalent. For (1) $\Rightarrow$ (2), since Λ is free of rank d, $\Lambda \cong \mathcal{O}_l^d$, so that $\Lambda \otimes_{\mathcal{O}_L} L = \mathcal{O}_l^d \otimes_{\mathcal{O}_l} L = L^d \cong V$. For the converse, note that Λ is torsion-free, hence free since it is finitely generated over a PID. But then $\Lambda \otimes_{\mathcal{O}_L} L \cong L^d$ implies that Λ has rank d.

Lemma 180. *Let Λ, Λ' be lattices in V. Then*

1. *There is $x \in L^*$ such that $x\Lambda \subset \Lambda'$*
2. *$\Lambda + \Lambda'$ is a lattice.*

Note that in particular item (2) is clearly false for $\mathbb{Z} \subset \mathbb{R}$; in the case in question, $L = \mathrm{Frac}(\mathcal{O}_L)$.

Proof. (1) Take L-bases $e_1, \ldots, e_d$ and $f_1, \ldots, f_d$ of V for $e_i \in \Lambda, f_i \in \Lambda'$. Then $e_i = \sum_j a_{ij} f_j$, $a_{ij} \in L$. Clear denominators to get $xe_i = \sum_j c_{ij} f_j$ for $x \in \mathcal{O}_L^*$, $c_{ij} \in \mathcal{O}_L$. Then $x\Lambda \subset \Lambda'$ as desired.

(2) $\Lambda + \Lambda'$ is finitely generated and clearly generates V, so it is also a lattice. □

Definition 181. If V is a representation of a group G over L, a lattice $\Lambda \subset V$ is *stable under* G if $\rho(g)\Lambda \subset \Lambda$ for all $g \in G$.

Proposition 182. *Any representation V of a group G over L has a stable lattice.*

Proof. Let $\Lambda \subset V$ be any lattice. Then $\mathrm{Stab}_G\Lambda$ is open in G (to see this, take a basis of Λ; then elements in $\mathrm{Stab}_G\Lambda$ are elements whose matrix has coefficients in $\mathcal{O}_L$; but $\mathcal{O}_L$ is open in L. Thus $\mathrm{Stab}_G\Lambda$ has finite index. Define

Why are the matrix elements in $\mathcal{O}_L$?

$$\Lambda' = \sum_{g \in G} \rho(g)\Lambda$$

This is well-defined since the sum is actually finite. By the lemma, Λ' is a lattice, and it is clearly G-stable. □

Thus if Λ is a stable lattice, we can restrict a representation ρ to Λ, and we get a representation

$$\rho_\Lambda : G \to GL_{\mathcal{O}_L}(\Lambda) \cong GL_d(\mathcal{O}_L)$$

Definition 183.

$$\bar{\rho}_\Lambda : G \xrightarrow{\rho_\lambda} GL_{\mathcal{O}_L}(\Lambda) \to GL_{k_L}(\Lambda/\pi\Lambda), \qquad \Lambda/\pi\Lambda \cong k_L^d$$

Definition 184. If ρ is a representation, its *semi-simplification* ρ^{ss} is the representation determined as follows: let X be any irreducible subrepresentation; then

$$\rho^{\mathrm{ss}} = X \oplus (V/X)^{\mathrm{ss}}$$

That is, the semi-simplification is the direct sum of the irreducible components; it can be shown that this is independent of the choices made in the above process. If the matrix of ρ looks like

$$\begin{pmatrix} \mathbf{X} & * & * \\ 0 & \mathbf{Y} & * \\ 0 & 0 & \mathbf{Z} \end{pmatrix}$$

where $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ are block matrices, then the semisimplification turns this matrix into

$$\begin{pmatrix} \mathbf{X} & 0 & 0 \\ 0 & \mathbf{Y} & 0 \\ 0 & 0 & \mathbf{Z} \end{pmatrix}$$

Proposition 185. *$\bar{\rho}_\Lambda^{\mathrm{ss}} \cong \bar{\rho}_{\Lambda'}^{\mathrm{ss}}$ if Λ, Λ' are two stable lattices.*

Proof. For any representation τ and $g \in G$, write $\chi(\tau(g))(x)$ for the characteristic polynomial of $\tau(g)$. Then clearly $\chi(\bar{\rho}_\Lambda(g))(x) \in k_L[x]$, $\chi(\rho_\Lambda(g))(x) \in \mathcal{O}_L[x]$, and

$$\overline{\chi(\rho_\Lambda(g))(x)} = \chi(\bar{\rho}_\Lambda(g))(x).$$

But also clearly

$$\overline{\chi(\rho_\Lambda(g))(x)} = \overline{\chi(\rho(g))(x)}$$

so that the characteristic polynomial of $\bar{\rho}_\Lambda$ is actually independent of Λ. The result then follows from the Brauer-Nesbitt theorem, which states that two representations with the same characteristic polynomials have the same semi-simplifications. (This theorem generalizes the statement that in characteristic zero, having the same trace implies that the two representations are isomorphic [which is equivalent in characteristic zero to having the same semi-simplifications]). □

The above arguments work for any field L and any subring $\mathcal{O}_L$ such that $\mathcal{O}_L$ is open in L and $L = \mathrm{Frac}(\mathcal{O}_L)$.

Definition 186. $\bar{\rho}^{\mathrm{ss}} : G_K \to GL_d(k_L)$ is defined as $\bar{\rho}^{\mathrm{ss}}_\Lambda$ for any stable lattice Λ.

Remark 187. Note that $\Lambda/\pi^n\Lambda \cong (\mathcal{O}_L/\pi^n\mathcal{O}_l)^d$, so that if Λ is stable, we get

$$\rho_{\Lambda,n} : G_K \to GL_{L/\pi^n}(\Lambda/\pi^n) \cong GL_d(\mathcal{O}_L/\pi^n\mathcal{O}_L)$$

even though $\mathcal{O}_L/\pi^n\mathcal{O}_L$ is not even a domain. Then from the $\rho_{\Lambda,n}$, you can retrieve ρ_Λ and ρ, since

$$\Lambda = \varprojlim \Lambda/\pi^n\Lambda$$

and the inverse limit is compatible with the G-action.

Thus representations over these finite rings allow recovery of representations over $\mathcal{O}_L$. This is the start of deformation theory.

Recall that $H^n(G, A)$ is defined for G any (topological) group, A an abelian (topological) group written additively with a (continuous) G-action. In what follows, we will write H^n for this continuous cohomology.

Galois cohomology is the case of $G = G_K$ or a quotient; the interesting cases are G_K for K a local or global field, and $G_{K,S}$ where S is a finite set of finite places of a global field K.[8]

Ultimately, we will look at $H^n(G_K, V)$ where $\rho : G_K \to GL_L(V)$ is a continuous ℓ-adic representation, i.e. $[L : \mathbb{Q}_\ell] < \infty$. We thus have a G_K action on V as an abelian group, and the natural topology for V is the ℓ-adic topology. Most of Tate's theory, however, is for $H^n(G_K, A)$ for A discrete. This suffices for:

Theorem 188. *(Tate) Let (ρ, V) be an ℓ-adic representation over L, Λ a stable $\mathcal{O}_L$ lattice, G a group (again, think $G = G_K$ for K a local field or $G = G_{K,S}$ for K a number field and S a finite set of finite places of K). Then*

1. *$H^i(G, \Lambda)$ is an $\mathcal{O}_L$-module of finite type (note that it is clearly an $\mathcal{O}_L$-module since Λ is);*
2. *$H^i(G, \Lambda) \otimes_{\mathcal{O}_L} L \cong H^i(G, V)$;*
3. *$H^i(G, \Lambda) = \varprojlim_n H^i(G, \Lambda/\pi^n\Lambda)$*

We will prove this later, but the proof basically amounts to commutativity of various functors. For example, (3) amounts to the fact that inverse limits commute with cohomology.

The meaning of this theorem is that we can compute $H^i(G, V)$ from discrete cohomology.

In what follows, assume A is discrete (it will in practice usually be finite, or at least torsion as an abelian group).

Recall that

1. $H^0(G, A) = A^G$
2. $$H^1(G, A) = \frac{\{f : G \to A \text{ such that } f(gg') = f(g) + gf(g') \text{ (crossed homomorphisms)}\}}{\{f : G \to A \text{ such that } f(g) = ga - a \text{ for some } a \in A\}}$$

[8] Note that in general, when working with infinite Galois groups, one has to remember the Krull topology (i.e. work continuously), otherwise subgroups will not correspond to field extensions. This is why continuous cohomology is the natural thing to work with.

3. $H^2(G, A)$ parameterizes extensions E of G by A. That is it parameterizes exact sequences

$$0 \to A \to E \to G \to 1$$

where the induced action of G on A defined by E [9]is the given action. This is not quite the whole story in the continuous case. In that case, it parameterizes such extensions assuming that there is a continuous section $G \to E$. But for profinite groups, this is always the case.

7.2 Cohomological Dimension

Definition 189. A *supernatural number* is a formal product $\prod_p p^{n_p}$ where p ranges over all rational primes and $n_p \in \{0, 1, 2, \ldots, \infty\}$.

For any family of supernaturalnumbers, one can define divisibility, GCD, LCM, and products.

If G is a profinite group, we define its order

$$|G| = \operatorname{lcm}_{H \trianglelefteq G} |G/H|$$

Thus $|\mathbb{Z}_p| = p^\infty$, and $|\mathbb{Z}_5^*| = 2^2 \cdot 5^\infty$ since $\mathbb{Z}_5^* \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}_5$.

Definition 190. If G is profinite and $|G| = \prod_\ell \ell^{n_\ell}$, a p-Sylow subgroup H of G is a subgroup $H \subset G$ such that $|H| = p^{n_p}$.

Proposition 191. *p-Sylow subgroups always exist, and any two p-Sylow subgroups are conjugate.*

Proof. (Vague sketch) p-Sylow subgroups exist in finite quotients G/H; choose them compatibly and take limits. □

If G is profinite and A is a torsion G-module, then we can write

$$A = \bigoplus_p A(p)$$

where $A(p) = \{x \in A \mid p^n x = 0 \text{ for some } n\}$. $A(p)$ is called the p-primary part of A.

Then

$$H^i(G, A) = \bigoplus_p H^i(G, A(p))$$

and each $H^i(G, A(p))$ is p-primary.

Definition 192. Let G be profinite, p a rational prime. Then the *cohomological dimension at p of G*, written $\operatorname{cd}_p(G)$, is the smallest integer n such that for all p-primary torsion G-modules A, $H^{n+1}(G, A) = 0$. Note that n can be ∞.

Proposition 193. *We can replace "torsion" by either "finite" or "simple finite" in the above definition without changing* $\operatorname{cd}_p(G)$.

[9]The action is defined as follows: for $g \in G$, choose any lift g' of g in E; this defines a homomorphism $i_g : A \to A : a \mapsto g'a(g')^{-1}$; i_a lands in A since A, being a kernel, is normal in E; i_a is independent of the lift since A is abelian.

Proof. If A is torsion and p-primary, then $A = \varinjlim_i A_i$ for $A_i \subset A$ finite and p-primary since any element in A generates a finite subgroup. But then

$$H^q(G, A) = \varinjlim H^q(G, A_i)$$

since any crossed homomorphism $G \to A$ actually maps into some A_i. This proves the result for "finite".

We now show that $H^q(G, A) = 0$ for all simple finite modules A if and only if $H^q(G, A) = 0$ for all finite modules A. $\Leftarrow$ is apparent. For the other direction, use induction on $|A|$. If A is simple, we are done. Otherwise, write

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

where B, A, C are nonzero G-modules with $|B| < |A|$. Then looking at the long exact sequence in cohomology,

$$\cdots \to H^q(G, C) \to H^q(G, A) \to H^q(G, B) \to \cdots$$

the groups on both ends are zero by induction, so that $H^q(G, A) = 0$ as well. □

In fact, we will show that $\mathrm{cd}_p(G_K) = 2$ for both local and global fields, so we need only concern ourselves with H^1 and H^2.

While the definition of cd_p addresses only the $n + 1$ cohomology group, the next proposition shows that all higher cohomology is zero as well. Thus $\mathrm{cd}_p(G)$ is the largest n for which cohomology is nonzero for *some* G-module.

Proposition 194. *If $\mathrm{cd}_p(G) = n$, then $H^q(G, A) = 0$ for all $q > n$ and all p-primary torsion G-modules A.*

Proof. Assume $H^k(G, A) = 0$ for all torsion p-primary modules A. Given any abelian group A with trivial G-action, we can construct the "induced module"

$$M^G(A) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$$

This is a G-module with the action induced by the action of G on $\mathbb{Z}[G]$; the action is continuous since it is continuous on both components. It turns out that for any G-module A, $H^i(G, M^G(A)) = 0, i > 0$. Then consider the exact sequence

$$0 \to A \hookrightarrow M^G(A) \to B \to 0$$

and look at the long exact sequence in cohomology:

$$\cdots \to H^k(G, B) \to H^{k+1}(G, A) \to H^{k+1}(G, M^G(A)) \to \cdots$$

The left-hand term vanishes since B is also p-primary torsion, and the right-hand term vanishes since $M^G(A)$ is cohomologically trivial. Thus the middle term vanishes as well. □

Why is B p-primary?

Note that the induction in this proof requires that the k^{th} cohomology vanish for all G-modules, not just for A itself.

Proposition 195. *If G is pro-p and A a p-primary simple finite module, then $A = \mathbb{Z}/p\mathbb{Z}$ with the trivial action.*

Proof. Since A is finite, there is some normal open subgroup $H \subset G$ that acts trivially on A, so there is an induced action of G/H on A, and A remains simple as a G/H-module. So we may as well assume that G is finite, say $|G| = p^n$. Write A as a union of orbits, $A = \coprod Gx_i$. Then $|A| = p^n = \sum |Gx_i| = \sum p^{n_i}$ where the last equality follows from the orbit-stabilizer theorem. The orbit of $0 \in A$ is $\{0\}$, so at least one $n_i = 0$. Thus there is some nonzero $x \in A$ whose orbit consists of x only (i.e. whose orbit has cardinality $p^0 = 1$). Consider $\langle x \rangle \subset A$. This is fixed by G, and G acts trivially on it. But A is simple and $x \neq 0$, so that $\langle x \rangle = A$ and A has the trivial G-action. It follows that $A = \mathbb{Z}/p\mathbb{Z}$, since other such modules are not simple. □

Corollary 196. *If G is pro-p, then $\mathrm{cd}_p(G)$ is the smallest n such that $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$.*

Proposition 197. *Let G be profinite and $H \subset G$ be a closed subgroup. Then $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$, and equality holds if either (1) H is open in G, or (2) the index of H in G is prime to p.*

Proof. Let A be an H-module, and define $M_H^G(A) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$. Shapiro's lemma then says that $H^q(H, A) \cong H^q(G, M_H^G(A))$ canonically. Thus $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$.

Serre [Local Fields] defines the *restriction* and *corestriction* maps on cohomology induced by a subgroup inclusion $H \subset G$ if G is finite:

$$\mathrm{res} : H^q(G, A) \to H^q(H, A)$$
$$\mathrm{cor} : H^q(H, A) \to H^q(G, A)$$

and proves that $\mathrm{cor} \circ \mathrm{res} = [G : H]$ (§VII.7, Prop. 6). If p is prime to $[G : H]$, then this map is injective; for G profinite, use the finite quotients and pass to the limit. Thus $\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H)$. This proves equality in the case (2).

For case (1), if $\mathrm{cd}_p(G) = q$, then that by the above, $H^q(G, M_H^G(A)) = H^q(H, A)$, so we have a map

$$H^q(G, M_H^G(A)) \to H^q(H, A) \xrightarrow{\mathrm{cor}} H^q(G, A)$$

that is in fact induced by the canonical trace map $M_H^G(A) \to A$. Thus next term in the long exact sequence in cohomology is H^{q+1}, which is 0, so again $\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H)$. □

Corollary 198. *If G is profinite and $G^{(p)}$ is a p-Sylow subgroup of G, then $\mathrm{cd}_p(G) = \mathrm{cd}_p(G^{(p)})$.*

Proof. $G^{(p)}$ is a closed pro-p-group in G, and its index is prime to p. □

Proposition 199. *Let $1 \to H \to G \to G/H \to 1$ be an exact sequence with G profinite, H closed in G (and thus profinite). Then $\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H) + \mathrm{cd}_p(G/H)$.*

Proof. (Sketch) Spectral sequence. The sequence $H^i(G/H, H^j(H, A))$ converges to $H^{i+j}(G, A)$. So for $q \geq \mathrm{cd}_p(H) + \mathrm{cd}_p(G/H)$, if $i + j = q$ then $i > \mathrm{cd}_p(G/H)$ or $j > \mathrm{cd}_p(H)$ so $H^i(G/H, H^j(H, A)) = 0$. □

Example 200. $\mathrm{cd}_p(\hat{\mathbb{Z}}) = 1$. Clearly it is at least 1, since $\hat{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$.. Now, $H^2(\hat{\mathbb{Z}}, A)$ parameterizes extensions E of $\hat{\mathbb{Z}}$, but any sequence

Why does this show $H^1 \neq 0$?

$$0 \to A \to E \xrightarrow{p} \hat{\mathbb{Z}} \to 0$$

splits. For we can define a section $s : \hat{Z} \to E$ of p by defining its value on 1 (since $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$). Again because of density, the map is clearly continuous. Thus $H^2(\hat{\mathbb{Z}}, A) = 0$ for all A.

Note that this shows that if K is a finite field, then $\mathrm{cd}_p(G_K) = 1$.

Remark 201. $H^2(\hat{\mathbb{Z}}, \mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$ where $\hat{\mathbb{Z}}$ acts trivially on $\mathbb{Z}$. To see this, take the long exact sequence in cohomology of $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$:

$$\cdots H^1(\hat{\mathbb{Z}}, \mathbb{Q}) \to H^1(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \to H^2(\hat{\mathbb{Z}}, \mathbb{Z}) \to H^2(\hat{\mathbb{Z}}, \mathbb{Q}) \to \cdots$$

Now, for G profinite, $H^i(G, \mathbb{Q}) = 0$ for all i, since $H^i(G, \mathbb{Q}) = \varinjlim H^i(G/H, \mathbb{Q})$ where H ranges over open subgroups of finite index. But then G/H is finite, so that $H^n(G/H, \mathbb{Q})$ is killed by $|G/H|$ (this is a standard fact about cohomology of finite groups). But $H^n(G/H, \mathbb{Q})$ also has the structure of a vector space over $\mathbb{Q}$, so must be zero.

Thus the term on each end is zero, so that $H^1(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \cong H^2(\hat{\mathbb{Z}}, \mathbb{Z})$. But $H^1(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})$ is simply continuous maps $\hat{Z} \to \mathbb{Q}/\mathbb{Z}$; such a map is determined by the image of 1, so the cohomology is $\mathbb{Q}/\mathbb{Z}$. This example of course does not violate the above theorems since $\mathbb{Z}$ is not torsion.

Example 202.

$$\mathrm{cd}_p(G_{\mathbb{R}}) = \mathrm{cd}_p(\mathbb{Z}/2\mathbb{Z}) = \begin{cases} 0 & p \neq 2 \\ \infty & p = 2 \end{cases}$$

since for $p \neq 2$, $H^2(G, A)$ is killed by 2 and by p^n so is zero for $n \geq 1$, while for $p = 2$, $H^1 \neq 0$ and all odd cohomologies are equal and all even cohomologies are equal.

Also, trivially, $\mathrm{cd}_p(G_{\mathbb{C}}) = 0$.

We will show that for K a p-adic field, $\mathrm{cd}_p(G_K) = 2$.

7.3 Galois Cohomology

Theorem 203. *Let K be a field. TFAE:*

1. $\mathrm{cd}_p(G_K) \leq 1$
2. *For all algebraic extensions L/K, $\mathrm{Br}(L)[p] = 0$ where $\mathrm{Br}(L)$ is the Brauer group.*

Definition 204. If L is a field, the Brauer group $\mathrm{Br}(L) =_{\mathrm{df}} H^2(G_L, \bar{L}^*)$.

Note that $H^1(G_L, \bar{L}^*) = 0$ by Hilbert 90.

Lemma 205. *Let $\boldsymbol{\mu}_n$ denote the n^{th} roots of unity in $\bar{L}^*$, with its G_L action. Assume* $\mathrm{char}\, L = 0$ *(the result holds in general, but is simpler to prove in this case, and characteristic zero is what we need anyway). Then $H^2(G_L, \boldsymbol{\mu}_n) = \mathrm{Br}(L)[n]$.*

Proof. Note that $\boldsymbol{\mu}_n \cong \mathbb{Z}/n\mathbb{Z}$ with a nontrivial G_L action.

The proof uses the "Kummer exact sequence"

$$1 \to \boldsymbol{\mu}_n \to \bar{L}^* \to \bar{L}^* \to 1$$

where the map $\bar{L}^* \to \bar{L}^* : z \mapsto z^n$ is surjective since L is algebraically closed. This map is compatible with the G_L action. The long exact sequence in cohomology is then

$$\cdots \to H^1(G_L, \bar{L}^*) \to H^1(G_L, \bar{L}^*) \to H^2(G_L, \boldsymbol{\mu}_n \to H^2(G_L, \bar{L}^*) \to H^2(G_L, \bar{L}^*) \to \cdots$$

The last two groups in this sequence are $\mathrm{Br}(L)$, and the map between them is $z \mapsto z^n$, so the kernel of the map is $\mathrm{Br}(L)[n]$. $H^1(G_L.\bar{L}^*) = 0$ by Hilbert 90, and the result follows. □

Proof. (of Theorem **??**):
(2) $\Rightarrow$ (1): Let G_L be a p-Sylow subgroup of G_K (to do this, take a p-Sylow subgroup, which is closed, and let L be its fixed field). Then $H^2(G_L, \boldsymbol{\mu}_p) = H^2(G_L, \mathbb{Z}/p\mathbb{Z})$ since the action of G_L on $\boldsymbol{\mu}_p$ is trivial on $\mathbb{Z}/p\mathbb{Z}$. The left-hand side is zero by assumption, so the right-hand side is as well. Thus $\mathrm{cd}_p(G_L) \leq 1$ so that $\mathrm{cd}_p(G_K) \leq 1$. Don't really follow this.

(1) $\Rightarrow$ (2): This is clear: $\mathrm{cd}_p(G_K) \leq 1 \Rightarrow \mathrm{cd}_p(G_L) \leq 1 \Rightarrow H^2(G_L, \boldsymbol{\mu}_p) = 0$.

□

Definition 206. Let K be a field, A a finite K-algebra (associative with unity, but not necessarily commutative). A is *central* if $Z(A) = K$, and *simple* if A has no two-sided ideals except for 0 and A. An algebra that is both central and simple is called a *central simple algebra*, or CSA.

Example 207. $M_n(K)$ is simple, since if $X \in M_n(K)$ it is a standard result of linear algebra that any matrix in $M_n(K)$ can be written as AXA for some $A \in M_n(K)$.

If D is a finite division algebra over K, then $Z(D) = K$ so D is central.

Putting these two together, we have that $M_n(D)$ is a CSA.

There are several important facts about CSAs, none difficult to prove:

1. All central simple algebras are $M_n(D)$ for some finite division algebra D over K.
2. If A, B are two CSAs over K, then $A \otimes_K B$ is also a CSA over K (note that the ideals of $A \otimes_K B$ are of the form $I_A \otimes_K I_B$).
3. The set of all CSAs over K up to the equivalence relation $D \sim M_n(D)$ for each n is an abelian group under $\otimes$. To show this, one must check that the notion is well-defined ($M_n(D) \otimes M_n(D') = M_n(D \otimes D')$, that it is commutative and associative (easy), and that inverses exist. If D is a CSA, its inverse is the opposite algebra D^{opp} obtained by reversing multiplication; then $D \otimes D^{\mathrm{opp}} \cong M_n(K)$.
4. This group is canonically isomorphic to $\mathrm{Br}(K)$.
5. Any CSA has dimension n^2 over K for some n. If L/K is an extension of fields and A a CSA over K, then $A \otimes_K L = A_L$ is a CSA over L, and $A \mapsto A_L$ gives a restriction map $\mathrm{res} : \mathrm{Br}(K) \to \mathrm{Br}(L)$.
6. It follows that over $\bar{K}$, every CSA is trivial (i.e. is $M_n(\bar{K})$ for some n since $G_{\bar{K}}$ is trivial and we have a description of the Brauer group in terms of the cohomology of $G_{\bar{K}}$.
7. Every division algebra D central over K contains a field L of dimension $\sqrt{[D : K]}$, and $D_L \cong M_n(L)$. It is also an amazing fact that any field of degree $\sqrt{[D : K]}$ over K embeds in D. For example, $K = \mathbb{R}$; the CSAs over $\mathbb{R}$ are $\mathbb{R}, \mathbb{H}$, so $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$. In $\mathbb{H}$, the field L is of course $\mathbb{C}$, and $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} = M_2(\mathbb{C})$.
8. $\mathrm{Br}(K)[n]$ is represented by a CSA of dimension n^2.

Theorem 208. *If $[K : \mathbb{Q}_p] < \infty$, then:*

1. $\mathrm{cd}_p(G_K) = 2$
2. $\mathrm{cd}_p(G_{K^{\mathrm{nr}}}) = 1$

Proof. Consider the exact sequence

$$1 \to G_{K^{\mathrm{nr}}} \to G_K \to \hat{\mathbb{Z}} \to 1$$

It follows from Proposition **??** that $\mathrm{cd}_p(G_K) \leq \mathrm{cd}_p(G_{K^{\mathrm{nr}}}) + 1$. Thus (2) implies that $\mathrm{cd}_p(G_K) \leq 2$, which is the hard part (a "dévissage argument").

To prove (2), it suffices to show that $\mathrm{Br}(L) = 0$ for all L/K^{nr} algebraic. This follows from

Lemma 209. *Let $K/\mathbb{Q}_p$ be a finite extension, A a CSA over K. Then there is an* unramified *finite extension K'/K such that $A_{K'}$ is trivial (note that the existence of a finite extension is trivial since we know that A is trivial over $\bar{K}$ and it is finite over K.)*

(2) follows from the lemma, since if A is a CSA over L, then there is some $K \subset L$, K finite over $\mathbb{Q}_p$, and A_K a CSA over K, such that $A_K \otimes_L L = A$. To see this, look at the matrix of A; these are all in some finite extension of $\mathbb{Q}_p$. Choose $K' \subset K^{\mathrm{nr}}$ (by the lemma) such that $A_K \otimes K'$ is trivial; since $K' \subset K^{\mathrm{nr}} \subset L$, A_L is also trivial, so that $\mathrm{Br}(L) = 0$.

Proof. (of lemma): Let D be a central division algebra over K. Claim there is a nontrivial unramified extension K'/K with $K' \subset D$. The proof is by contradiction; assume there are no such nontrivial unramified extensions. Let B be the ring of integers of D (i.e. the elements integral over K), and choose $x \in B$. Then $K[x] \subset D$ is a commutative subalgebra of D finite over K, and it is a domain, so it is a field and a finite extension of K. Thus it is totally ramified (otherwise it would have a subfield properly containing K that was unramified over K). So $K[x]$ and K have the same residue field. If π_K is a uniformizer for K, we then have for some $x_i \in \mathcal{O}_K, y_i \in B$

$$\begin{aligned} x &= x_0 + \pi_K y_1 \\ &= x_0 + \pi_K x_1 + \pi_K^2 y_2 \\ &= x_0 + \pi_K x_1 + \pi_K^2 x_2 + \pi_K^3 x_3 \\ &= \cdots \end{aligned}$$

Thus x is a limit of elements of $\mathcal{O}_K$, so $x \in \mathcal{O}_K$ and thus $B \subset \mathcal{O}_K$. But D is the quotient of integral elements by elements of K; contradiction proving the claim.

Assume $[D : K] = n^2$, and consider $D \otimes K' = D_{K'} \supset K' \otimes K'$ since $D \supset K'$. Then $D_{K'}$ is not a division ring, but is a CSA, so $D_{K'} = M_k(D')$ for $k > 1$, so that $[D' : K'] < n^2$. By (decreasing) induction, we are done. □

We have thus shown that $\mathrm{cd}_p(G_{K^{\mathrm{nr}}}) \leq 1$. It is nonzero since the pro-p-Sylow subgroups have nontrivial H^1. It follows that $\mathrm{cd}_p(G_K) \leq 2$. It also follows that

Why is this true?

Corollary 210. $\mathrm{Br}(K) = \mathbb{Q}/\mathbb{Z}$.

Proof. $H^2(G_K, \bar{K}^*) = H^2(\mathrm{Gal}(K^{\mathrm{nr}}/K), (K^{\mathrm{nr}})^*) = H^2(\hat{\mathbb{Z}}, \mathcal{O}^*_{K^{\mathrm{nr}}} \times \mathbb{Z})$. Now, $H^2(\hat{\mathbb{Z}}, \mathcal{O}^*_{K^{\mathrm{nr}}}) = 0$ since $\mathcal{O}^*_{K^{\mathrm{nr}}}$ is a sequence of extensions of K^{nr}, and we know that $H^2(\hat{\mathbb{Z}}, \mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$. □

Why cohomology is zero?

But this implies that $\mathrm{cd}_p(G_K) = 2$ since the torsion of $\mathrm{Br}(K)$ is nonzero. □

?

We can now explicitly compute cohomology for local fields using duality:

$$H^n(G, A) = H^{2-n}(G, A^* \otimes \omega_p)$$

This gives us H^2 since we know H^0, and the Euler characteristic formula can be used to get H^1 (see below).

Proposition 211. *If A is a finite G_K-module then $H^n(G_K, A)$ is finite.*

Lemma 212. *Let ℓ be a prime. Let $A = \boldsymbol{\mu}_\ell$ be the ℓ^{th} roots of 1 in $\bar{K}$; A is a cyclic group of order ℓ. Assume also that $A \subset K$ so that the Galois action of G_K on A is trivial. (We can get into this setup by taking a finite extension of K). Then $H^m(G_K, A)$ is finite, and*

$$\left|H^0(G_K, A)\right| = \ell$$
$$\left|H^2(G_K, A)\right| = \ell$$
$$\left|H^1(G_K, A)\right| = \begin{cases} \ell^2 & \ell \neq p \\ \ell^{2+[K:Q_p]} & \ell = p \end{cases}$$

Proof. (of Proposition **??** assuming Lemma **??**):
Since A is finite, G_K acts on A through finite quotient, so there is some K'/K finite and normal such that G'_K acts trivially on A. We may assume wlog that K' contains all the $|A|^{\text{th}}$ roots of unity.

As a G_K-module, A is the direct sum $\mathbb{Z}/\ell_i^{n_i}\mathbb{Z}$ for i in some finite index set I and ℓ_i prime. In particular, A is a successive extension of $\mathbb{Z}/\ell_i\mathbb{Z} = \boldsymbol{\mu}_{l_i}$ as G'_K modules, since the action is trivial. (Recall that we think of $\mathbb{Z}/\ell\mathbb{Z}$ as having trivial Galois action and $\boldsymbol{\mu}_\ell$ as having cyclotomic action. They are the same abelian group, but different Galois modules. It's just notation). By the lemma, $H^m(G'_K, \boldsymbol{\mu}_{\boldsymbol{l_i}})$ is finite and thus $H^m(G'_K, A)$ is finite by the LES of cohomology.

Finally, by the Hochshcild-Serre spectral sequence,

$$H^i(Gal(K'/K), H^j(G'_K, A)) \Rightarrow H^{i+j}(G_K, A)$$

and all the left sides are finite, so the limit of the spectral sequence is also finite. □

Proof. (of Lemma **??**):
$H^0(G_K, \boldsymbol{\mu}_\ell) = H^0(G_K, \mathbb{Z}/\ell\mathbb{Z}) = \mathbb{Z}/\ell\mathbb{Z}$ since H^0 is just the invariants and the action is trivial.

From a previous proposition, $H^2(G_K, \boldsymbol{\mu}_\ell) = \mathbb{Z}/\ell\mathbb{Z}$.

Finally, since the Artin map sends $K^* \hookrightarrow G_K^{\text{ab}}$ with dense image,

$$H^1(G_K, \boldsymbol{\mu}_\ell) = H^1(G_K, \mathbb{Z}/\ell\mathbb{Z}) = \text{Hom}_{\text{cont}}(G_K, \mathbb{Z}/\ell\mathbb{Z}) = c\,\text{Hom}_{\text{cont}}(G_K^{\text{ab}}, \mathbb{Z}/\ell\mathbb{Z}) = \text{Hom}_{\text{cont}}(K^*, \mathbb{Z}/\ell\mathbb{Z})$$

But $K^* = \pi_K^{\mathbb{Z}} \times \mathcal{O}_K^* = \pi_K^{\mathbb{Z}} \times \mathbb{F}_K^* \times (1 + \pi_K \mathcal{O}_K)$ where $\mathbb{F}_K$ is the residue field. Note that the last factor is not necessarily isomorphic to $\mathcal{O}_K$ additively (this depends on the ramification of K, which affects the convergence of exp), but in any case it is isomorphic to an open subgroup of $\mathcal{O}_K \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$. So to count up components of $\text{Hom}_{\text{cont}}(K^*, \mathbb{Z}/\ell\mathbb{Z})$, we get one $\mathbb{Z}/\ell\mathbb{Z}$ from $\pi_K^{\mathbb{Z}}$ and one from $\mathbb{F}_K^*$ since all the roots of unity are in K. If $\ell \neq p$, the final factor contributes 0, while if $\ell = p$, it contributes $\ell^{[K:\mathbb{Q}_p]}$. □

Note that the above proof for H^1 uses class field theory, while the proof for H^2 uses the Brauer group - which, in the end, also uses class field theory.

7.4 Pontrjagin Duality

Definition 213. Let A be a finite abelian group. The *Pontrjagin dual* of A is

$$A^* = \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$$

or, equivalently, $\text{Hom}(A, \mathbb{C}^*)$ since A is finite.

A is canonically isomorphic to $A^{*}*$ via $a \mapsto (f \mapsto f(a))$, i.e. evaluation at a. A is non-canonically isomorphic to A^*.

Definition 214. If $B \subset A$ is a subgroup, then $B^{\perp} := \{f \in A^* \mid f(b) = 0\} \subset A^*$.

Proposition 215. *If $B \subset A$ is a subgroup, then (1) $B^{\perp} \cong (A/B)^*$, (2) $|B| \times \left|B^{\perp}\right| = |A|$, and (3) $B^{\perp^{\perp}} = 0$.*

proof?

Proof. □

If A has a G_K-action, then A^* does as well, via

$$(g \cdot f)(a) = f(g^{-1} \cdot a)$$

Theorem 216. *(Pontrjain duality theorem) [Tate, Poitu; this proof is Serre/Groth; there is another proof using Fontaine theory as well]*
Let $I = \varinjlim_{r \to \infty} \boldsymbol{\mu}_r$ (as an abelian group, $I \cong \mathbb{Q}/\mathbb{Z}$); note that I has a nontrivial G_K action. Then

$$H^n(G_K, A)^* \cong H^{2-n}(G_K, A^* \otimes I)$$

canonically, for $n = 0, 1, 2$ and all finite G_K-modules A.

Duality theorems are always hard to prove. The proof below is from Serre/Groth, and may have originated with Grothendieck.

Proof. We first prove the case $n = 2$. Consider the contravariant functor $A \to H^2(G_K, A)^*$ from finite abelian G_K-modules to finite abelian groups. Since $\mathrm{cd}_p(G_K) = 2$, we see that H^2 is right exact, so this functor is left exact. Those categories are Noetherian, so we have Grothendieck's pro-representability theorem (see Serre, Galois Cohomology), except that since the functor is contravariant we get an ind-represented functor: we get that there is an $I = \varinjlim B_\alpha$ for finite G_K modules B_α (I is therefore a torsion G_K module) such that $H^2(G_K, A)^* \cong \mathrm{Hom}_{G_K}(A, I)$. These are just the invariants of G_K in $A^* \otimes I$, which is $H^0(A^* \otimes I)$.

We know that $H^2(G_K, \boldsymbol{\mu}_r) = \mathbb{Z}/r\mathbb{Z}$ for all r, so $(\mathbb{Z}/r\mathbb{Z})^* = \mathrm{Hom}_{G_K}(\boldsymbol{\mu}_r, I)$ in the case of a trivial G_K action (this is the definition of the Pontrjagin dual). But one can reduce to this case by taking a finite extension of K to kill the G_K action. But this implies that $I = \varinjlim \boldsymbol{\mu}_r$ and is unique by Yoneda's lemma. This concludes the proof for $n = 2$.

implication is exercise

Next note that $I \otimes_{\mathbb{Z}} I^* = \mathbb{Q}/\mathbb{Z}$ with trivial G_K action. For A a finite G_K module, write $A' = A^* \otimes I$. Then as G_K modules, $A'' = A$ (this is not formal; it is a particular property of this G_K module I).

Then for $n = 0$, we have $H^0(G_K, A)^* = H^0(G_K, A'')^* = H^(G_K, A')$ as desired.

For $n = 1$, since A is finite, there are finite modules B, C such that $0 \to A \to B \to C \to 0$ for B cohomologically trivial for $n \geq 1$ (for example, take B to be the induced module of A). The primed sequence $0 \to C' \to B' \to A' \to 0$ is also exact since the $'$ operator is an involution. We thus get a map of long exact sequences in cohomology

$$\begin{array}{ccccccccc}
\cdots & H^0(G_K, B) & \to & H^0(G_K, C) & \to & H^1(G_K, A) & \to & H^1(G_K, B) = 0 \\
 & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & H^2(G_K, B')^* & \to & H^2(G_K, C')^* & \to & H^1(G_K, A')^* & \to & 0
\end{array}$$

The first two vertical arrows are isomorphisms by the duality already proved, so by a diagram chase, the rightmost vertical arrow is injective. Applying this to A', A'', we get that the dual of the rightmost vertical arrow is injective so that the map in question is also surjective and thus an isomorphism. The map is canonical as can be seen by looking at the cup product. □

7.5 Euler Characteristic Formula

The Euler characteristic formula can be used to actually compute cohomology given the duality formulas just proved.

Definition 217. If $\{A_i\}_{i\in\mathbb{Z}}$ are finite abelian groups (or finite dimensional vector spaces over a field L) that are 0 for all but finitely many i, then we define the *Euler characteristic*

$$\chi((A_i)_{i\in\mathbb{Z}}) = \prod_{i\in\mathbb{Z}} |A_i|^{(-1)^i}$$
$$\chi((A_i)_{i\in\mathbb{Z}}) = \prod_{i\in\mathbb{Z}} (-1)^i \dim_L A_i$$

respectively.

(Note that these definitions are the same thing, via the log map, if $L = \mathbb{F}_p$, say).

Now if we have a complex $\cdots \to A_{i-1} \to A_i \to A_{i+1} \to \dots$ with

$$H_i = \ker(A_i \to A_{i+1}) / \operatorname{im}(A_{i-1} \to A_i)$$

its cohomology, then we have $\chi((A_i)) = \chi((H_i))$. The proof of this is easy; you get a telescoping sum and use the rank theorem from linear algebra. Note that the H_i are finite abelian groups if the A_i are and are finite dimensional vector spaces if the A_i are.

Definition 218. If A is a finite G_K module, define

$$\chi(A) = \chi((H^i(G_K, A))) = \frac{\left|H^0(G_K, A)\right| \cdot \left|H^2(G_K, A)\right|}{|H^1(G_K, A)|} = \chi((I_i^{G_K}))$$

for $A \to I_0 \to I_1 \to \dots$ an injective resolution.

Proposition 219. *If $0 \to A \to B \to C \to 0$ is a short exact sequence of G_K modules, then $\chi(B) = \chi(A)\chi(C)$.*

Proof. By the long exact sequence in cohomology. The LES is exact, so its cohomology is zero. By the previous proposition, $\chi(\text{LES}) = \chi(\text{cohomologyofLES}) = 1$, and examining the long exact sequence, we see that $\chi(\text{LES}) = \chi(A)\chi(C)/\chi(B)$. □ or its reciprocal

In general, the Euler characteristic tends to be very invariant.

Theorem 220. *Let A be a finite G_K module. Then $\chi(A) = ||A||_K$ where $|\cdot|_K$ is the normalized (for the product formula) norm in K - that is, $\left|N_{K/\mathbb{Q}_p}(\cdot)\right|_{\mathbb{Q}_p}$.*

Proof. (Sketch) Proved by Tate, Poitu, Fontaine. Note first that if $|A| = \prod_{\ell \text{ prime}} \ell^{n_\ell}$, then $\chi(A) = p^{-n_p[K:\mathbb{Q}_p]}$. Start with any A and reduce to the case $A = \mathbb{Z}/\ell\mathbb{Z}$ with the trivial action using the spectral sequence. We are then in the case of the lemama from before, so we get either ℓ^2/ℓ^2 (if $\ell \neq p$) or $l^2/(l^{2+[K:\mathbb{Q}_p]})$ (if $\ell = p$). □

Using this theorem, if M is a torsion module, we can compute $H^0(G_K, M)$ easily, get $H^2(G_K, M)$ by duality, and then compute $H^1(G_K, M)$ from the theorem.

Corollary 221. *If V is an ℓ-adic continuous representation of G_K for K, L finite over $\mathbb{Q}_p$, then*

1. $\dim_L H^n(G_K, V) < \infty$
2. $H^n(G_K, V)^* \cong H^{2-n}(G_K, V^*(1))$ *(the Tate twist - tensor with ω_p)*
3. $\dim H^0(G_K, V) - \dim H^1(G_K, V) + \dim H^2(G_K, V) = (\dim_L V) \cdot [K : \mathbb{Q}_p]$

Proof. V has a stable lattice, which is the limit of finite modules. Use a previous theorem of Tate to transfer the results we've already done for finite modules. □ which theorem?

Definition 222. If A is a finite G_K module, we say that A is *unramified* if I_K acts trivially on A. If A is unramified, define $H^n_{\text{ur}}(G_K, A) = H^n(G_K/I_K, A)$.

Proposition 223.

1. $H^0_{\text{ur}}(G_K, A) = H^0(G_K, A)$
2. $H^1_{\text{ur}}(G_K, A) = \ker(H^1(G_K, A) \to H^1(I_K, A))$ *under the restriction map*
3. $H^2_{\text{ur}}(G_K, A) = 0$
4. $\left|H^1_{\text{ur}}(G_K, A)\right| = \left|H^0(G_K, A)\right|$
5. *If $p \nmid |A|$, then $H^1_{\text{ur}}(G_K, A)^\perp \subset H^1(G_K, A)^* \cong H^1(G_K, A') \supset H^1_{\text{ur}}(G_K, A')$; viewed as subspaces of the same space under those maps, the first and last spaces are the same.*

Proof. (1) is obvious. (2) follows from the inflation-restriction exact sequence. (3) holds because $G_K/I_K \cong \hat{\mathbb{Z}}$, which has cohomological dimension 1. (4) is a computation what computation?

Finally, assume $p \nmid |A|$. If A is unramified, so is A'. We have $H^1_{\text{ur}}(G_K, A) \otimes H^1_{\text{ur}}(G_K, A') \xrightarrow{\text{cup}} H^2_{\text{ur}}(G_K, I) = 0$, so that $H^1_{\text{ur}}(G_K, A)^\perp \supset H^1_{\text{ur}}(G_K, A')$. To see they have the same cardinality, we have by the above "$\otimes I$ ... cyclotomic"

$$\left|H^1_{\text{ur}}(G_K, A')\right| = \left|H^0(G_K, A)\right| = \left|H^2(G_K, A)\right|$$

and

$$\left|H^1_{\text{ur}}(G_K, A)^\perp\right| = \frac{\left|H^1(G_K, A)\right|}{|H^1_{\text{ur}}(G_K, A)|} = \frac{\left|H^1(G_K, A)\right|}{|H^0(G_K, A)|}$$

and these are equal since $\chi(A) = 1$ because $|A|$ is prime to p. □

7.6 Global Galois Theory

Let $[K : \mathbb{Q}]$ be a finite extension.

Theorem 224. $\text{cd}_p(G_K) = 2$ *unless $p = 2$ and K has a real place. In this case,* $\text{cd}_2(G_K) = \infty$.

Proof. (Sketch) The second statement follows since $\text{cd}(\mathbb{Z}/2\mathbb{Z}) = \infty$. For the first statement, use the same argument as in the local case: find L/K such that $\text{Gal}(L/K) \cong \hat{\mathbb{Z}}$ and argue as before using the Brauer group. □

Remark 225. There is no finiteness result for number fields. For example, $H^2(G_K, \boldsymbol{\mu}_n) = \mathrm{Br}(K)[n] = \oplus_p \mathbb{Z}/p\mathbb{Z}$.

The right group to look at is $G_{K,S}$ where S is a finite set of places.

Theorem 226. $\mathrm{cd}_p(G_{K,S}) \leq 2$ *for* $p \neq 2$.

8 Appendix - Topological Groups

A topological group G is a topological space together with a group structure in which multiplication and inverse are continuous maps. G is often assumed Hausdorff in the topology.

Proposition 227. *Let G be a topological group and H a subgroup. Then*

1. *If H is open, then it is closed.*
2. *If G is compact and H is open, then H is of finite index.*
3. *If H is closed and of finite index, then it is open.*
4. *The connected component of $1 \in G$ is a subgroup.*
5. *If G is connected, then its only open subgroup is G itself.*
6. *If $H \subset G$ contains an open set, then H is open.*

Proof. (1) follows by noting that H together with its (open) cosets covers G, and H is the complement of the union of all the cosets except for H itself, so is the complement of an open set.

(2): The collection of cosets of H is a cover of G by disjoint open sets, so removing any coset results in a non-cover. Since G is compact, the number of cosets must be finite.

(3): This is the same argument as for (1): H is the complement of the union of all its cosets other than H itself; this is a finite union of closed sets, so its complement H is open.

(4): Let H be the connected component of 1, and consider the map $G \to G : x \mapsto x^{-1}$, restricted to H. Clearly the image is connected, but also contains 1, so is contained in H. Similarly, the restriction of multiplication to H, $H \times H \to G : (x, y) \mapsto xy$, has connected image containing 1. Thus H is a subgroup.

(5): Let H be the connected component of the identity; its cosets form a disjoint open cover of G. Since G is connected, there can be only one coset and $H = G$.

(6): Suppose H contains an open set U around $h \in H$. Then if $y \in H$, we have that $yh^{-1}U \subset$ is an open set in H containing y. □

Finite index does not imply either closed or open. However, it was recently shown that if a profinite group is topologically finitely generated (i.e. has a finitely generated subgroup that is dense), then finite index implies open (implies closed).

Note that the only closed subgroups of $\mathbb{R}$ are the groups $a\mathbb{Z}$ for $a \in \mathbb{R}$. There are no proper open subgroups. (In fact, any closed subgroup of $\mathbb{R}^n$ is isomorphic to something like free abelian groups on $k \leq n$ generators.)

Note that $\mathbb{Z}_p$ is Hausdorff: given any two distinct integers, choose n so that the integers are not congruent $\mod p^n$. Then the balls of radius p^n around the integers are disjoint.

Any locally compact group has a Haar measure, which is a (left- or right-) invariant measure.

Locally compact abelian groups have a nice theory that generalizes Fourier analysis. If G is locally compact abelian, define G^* to be the group of homomorphisms $G \to S^1$; this is also a locally compact abelian group, and there is a natural isomorphism $G^{**} \cong G$. Then any function $G \to \mathbb{C}$ can be written as a sum of functions in the dual group G^*; for $\mathbb{R}$, this is simply Fourier series.