Math 160c Spring 2013 Caltech
Applications of Global Class Field Theory
Course Notes

Andrei Jorza

Contents

Lecture 1
2013-04-01

1 Local Class Field Theory

1.1 Main results

(1.1.1) Have an upper ramification filtration G_K^u for $u \geq -1$ such that $G_K^{-1} = G_K$, $G_K^{(-1,0]} = I_K$, $G_K^{(0,1]} = P_K$. If L/K is an algebraic extension then $G_{L/K}^u = G_K^u/(G_K^u \cap G_L)$.

(1.1.2) The invariant map is an isomorphism $\mathrm{inv}_K : \mathrm{Br}(K) \cong H^2(G_K, \overline{K}^\times) \cong \mathbb{Q}/\mathbb{Z}$ such that if L/K then $\mathrm{inv}_K \circ \mathrm{cor} = \mathrm{inv}_L$ and $\mathrm{inv}_L \circ \mathrm{res} = [L:K]\,\mathrm{inv}_K$.

(1.1.3) Tate duality. If M is a finite G_K-module let $M^* = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$. The Galois group G_K acts on $m^* \in M^*$ via $(gm^*)(m) = m^*(g^{-1}m)$. Write $M(1) \cong M \otimes_{\mathbb{Q}/\mathbb{Z}} \mu_\infty$. Write $H^i_{\mathrm{ur}}(G_K, M) = H^i(G_K/I_K, M^{I_K})$. Then there exists a perfect pairing

$$H^i(G_K, M) \otimes H^{2-i}(G_K, M^*(1)) \to H^2(G_K, M \otimes M^*(1)) \to H^2(G_K, \mu_\infty) \to H^2(G_K, \overline{K}^\times) \to \mathbb{Q}/\mathbb{Z}$$

such that $H^i_{\mathrm{ur}}(G_K, M)^\perp = H^{2-i}_{\mathrm{ur}}(G_K, M^*(1))$.

(1.1.4) The Artin map. For $K/\mathbb{Q}_p$ finite write $\mathcal{U}_K^{-1} = K^\times$, $\mathcal{U}_K^0 = \mathcal{O}_K^\times$ and $\mathcal{U}_K^n = 1 + (\varpi)^n$ for $n \geq 1$. There exists a homomorphism $r_K : K^\times \cong W_K^{\mathrm{ab}}$ such that $r_K(\mathcal{U}_K^n) = G_K^{n,\mathrm{ab}}$. It has the property that $r_K(N_{L/K}x) = r_L(x)$ for $x \in L^\times$ and $r_K(x) = \mathrm{cor}^\vee(r_L(x))$ for $x \in K^\times \subset L^\times$.

1.2 Application

We will prove Kronecker-Weber for local fields.

Theorem 1.1. *The maximal abelian extension of $\mathbb{Q}_p$ is $\mathbb{Q}_p(\mu_\infty)$.*

Proof. Recall that $G_K = I_K \rtimes \mathrm{Frob}_K^{\widehat{\mathbb{Z}}}$ and $W_K = I_K \rtimes \mathrm{Frob}_K^{\mathbb{Z}}$. Thus $G_{\mathbb{Q}_p}^{\mathrm{ab}} \cong (I_{\mathbb{Q}_p}^{\mathrm{ab}})_{\mathrm{Frob}_p} \times \mathrm{Frob}_p^{\widehat{\mathbb{Z}}}$ and $I_{\mathbb{Q}_p}^{\mathrm{ab}} \cong \mathbb{Z}_p^\times$ and so $G_{\mathbb{Q}_p}^{\mathrm{ab}}$ is a quotient of $\mathbb{Z}_p^\times \rtimes \widehat{\mathbb{Z}}$ which we will show to be equal to $G_{\mathbb{Q}_p(\mu_\infty)/\mathbb{Q}_p}$ under the reciprocity map.

First, recall $\mathbb{Q}_p^{\mathrm{ur}} = \mathbb{Q}_p(\omega(\alpha) | \alpha \in \overline{\mathbb{F}}_p^\times)$ and since $p^{\varphi(n)} \equiv 1 \pmod{n}$ if $p \nmid n$ it follows that $\mathbb{Q}_p^{\mathrm{ur}} = \mathbb{Q}_p(\zeta_n | p \nmid n)$. Next $\mathbb{Q}_p(\zeta_p)$ is ramified over $\mathbb{Q}_p$ and so $\zeta_p \notin \mathbb{Q}_p^{\mathrm{ur}}$ and therefore $\mathbb{Q}_p^{\mathrm{ur}} \cap \mathbb{Q}_p(\mu_{p^\infty}) = \mathbb{Q}_p$. This gives $G_{\mathbb{Q}_p(\mu_\infty)/\mathbb{Q}_p} \cong G_{\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p} \times G_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p}$. □

2 Glocal Class Field Theory

2.1 Adeles

(2.1.1) If $K/\mathbb{Q}$ is a finite extension then $K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R}$, $K_\infty^{\times,0}$ is the connected component of 1 in $K_\infty^\times$. For an embedding $v : K \hookrightarrow \mathbb{R}$ write $v \mid \mathbb{R}$ and $v : K \hookrightarrow \mathbb{C}$ write $v \mid \mathbb{C}$. Then $K_\infty = \prod_{v|\infty} K_v$, $K_\infty^\times = \prod_{v|\infty} K_v^\times$ and $K_\infty^{\times,0} = \prod_{v|\mathbb{R}}(0,\infty)\prod_{v|\mathbb{C}} \mathbb{C}^\times$.

(2.1.2) Write $\mathbb{A}_K = \prod'_{\{\mathcal{O}_v\}} K_v$ with the restricted product topology. For a finite set of places S write $K_S = \prod_{v\in S} K_v$ and $\mathbb{A}_K^S = \prod'_{v\notin S,\{\mathcal{O}_v\}} K_v$ in which case $\mathbb{A}_K = K_S \times \mathbb{A}_K^S$. Then the ring $\mathbb{A}_K = \prod'_{\{\mathcal{O}_v\}} K_v$ has the product topology, $K \subset \mathbb{A}_K$ is a discrete subgroup and $\mathbb{A}_K/K$ is compact.

(2.1.3) Write $\mathbb{A}_K^\times = \prod'_{\{\mathcal{O}_v^\times\}} K_v^\times$ with the restricted product topology. As above $\mathbb{A}_K^\times = K_S^\times \times \mathbb{A}_K^{S,\times}$. The natural inclusion $\mathbb{A}_K^\times \subset \mathbb{A}_K$ is not continuous and in fact the topology on $\mathbb{A}_K^\times$ is the subset topology induced by the map $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$ which takes x to (x, x^{-1}). Write $|\cdot|_{\mathbb{A}_K} : \mathbb{A}_K^\times \to (0,\infty)$. Define $\mathbb{A}_K^1 \subset \mathbb{A}_K^\times$ as the kernel of $|\cdot|_{\mathbb{A}_K}$. Then $K^\times \subset \mathbb{A}_K^1$ is a discrete subgroup, $\mathbb{A}_K^1 \subset \mathbb{A}_K$ is continuous and $\mathbb{A}_K^1/K^\times$ is compact.

(2.1.4) Strong approximation states that if $S \neq \emptyset$ then $K \subset \mathbb{A}_K^S$ is dense.

2.2 The Dirichlet unit theorem using adeles

Theorem 2.1. *Let $K/\mathbb{Q}$ be a number field with r real embeddings and s complex embeddings. Then $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r+s-1$.*

Proof. For a finite set S of places which include the infinite places write $\mathcal{O}_K[1/S] = \{x \in K | v(x) \geq 0, v \notin S\}$. Note that if $S = \{v \mid \infty\}$ then $\mathcal{O}[1/S]^\times = \mathcal{O}_K^\times$. We will show that $\mathcal{O}_K[1/S]^\times$ is a finitely generated abelian group of rank $|S|-1$.

Let $\mathrm{Cl}_S(K)$ be the class group of $\mathcal{O}_K[1/S]$, i.e., the set of ideals modulo the set of principal ideals. An element $a = (a_v)$ of $\mathbb{A}_K^\times$ gives the fractional ideal $\prod_{v\notin S}(\varpi_v)^{v(a_v)}$ of $\mathcal{O}_K[1/S]$ and the set of fractional ideals is isomorphic to $\mathbb{A}_K^\times/K_S^\times \prod_{v\notin S}\mathcal{O}_v^\times$. Write $K_S^1 = \{x \in K_S | \prod_{v\in S}|x_v|_v = 1\}$ in which case $\mathbb{A}_K^\times/K_S^\times \cong \mathbb{A}_K^1/K_S^1$.

It is easy to see that $\mathrm{Cl}_S(K) = \mathbb{A}_K^1/K^\times K_S^1 \prod_{v\notin S}\mathcal{O}_v^\times$ which gives the exact sequence

$$1 \to K_S^1 \prod_{v\notin S} \mathcal{O}_v^\times/\mathcal{O}_K[1/S]^\times \to \mathbb{A}_K^1/K^\times \to \mathrm{Cl}_S(K) \to 1$$

Immediately one sees $\mathrm{Cl}_S(K)$ as a quotient of a compact group by an open subgroup and so $\mathrm{Cl}_S(K)$ is finite.

Define Δ as the kernel of the summation map $\oplus_v \mathbb{R} \to \mathbb{R}$ and write Δ_S the kernel of $\oplus_{v\in S}\mathbb{R} \to \mathbb{R}$. Then one has the map $\log : \mathbb{A}_K^1/K^\times \to \Delta$ given by $(a_v) \mapsto (\log|a_v|_v)$. Clearly $\prod_{v\notin S}\mathcal{O}_v^\times K_S^1 \to \Delta_S$ is surjective and so get an exact sequence

$$K_S^1 \prod_{v\notin S} \mathcal{O}_v^\times/\mathcal{O}_K[1/S]^\times \to \Delta_S/\log \mathcal{O}_K[1/S]^\times \to 0$$

which exhibits $\Delta_S/\log\mathcal{O}_K[1/S]^\times$ as the image via a continuous map of an open subgroup of a compact group, therefore $\Delta_S/\log\mathcal{O}_K[1/S]^\times$ is compact. In particular $\log\mathcal{O}_K[1/S]^\times$ is a lattice in the $(|S|-1)$-dimensional Δ_S.

We would like to prove that $\mathcal{O}_K[1/S]^\times$ is a finitely generated abelian group of rank $|S|-1$. To do this it is enough to show that the intersection of the kernel of log with $\mathcal{O}_K[1/S]^\times$ consists only of torsion. What is the kernel? The kernel of log on $\mathbb{A}_K^1$ is $\{(a_v) \in \mathbb{A}_K^1 | |a_v|_v = 1\}$, i.e., $\prod_{v\nmid\infty}\mathcal{O}_v^\times \times \prod_{v|\mathbb{R}}\{\pm 1\} \times \prod_{v|\mathbb{C}} S^1$. This is compact and its intersection with $K^\times$ is compact and discrete, therefore finite. Since it is finite this intersection must be $\mu_\infty(K)$, i.e., torsion. □

2.3 Main results

(2.3.1) The global Brauer sequence

$$0 \to \mathrm{Br}(K) \to \oplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0$$

is exact where the rightmost map is the sum of the local invariant maps.

Application: a global quaternion algebra over any number field must be nonsplit at an even number of places. (Used to study Hilbert modular forms.)

(2.3.2) The Artin map $r_K : \mathbb{A}_K^\times \to G_K^{\mathrm{ab}}$ has the property that $r_K(1, \ldots, 1, x, 1, \ldots) = r_{K_v}(x)$ where $x \in K_v^\times$ is placed in position v and r_{K_v} is the local Artin map. It gives

$$r_K : \mathbb{A}_K^\times / \overline{K^\times K_\infty^{\times,0}} \cong G_K^{\mathrm{ab}}$$

such that $r_L(x) = r_K(N_{L/K}(x))$ and r_K induces an isomorphism $G_{L/K}^{\mathrm{ab}} \cong \mathbb{A}_K^\times / K^\times N_{L/K}\mathbb{A}_L^\times$.

Lecture 2
2013-04-03

2.4 Conductors

(2.4.1) If $K/\mathbb{Q}_p$ is a finite extension and V is a continuous complex finite dimensional representation of G_K define the conductor $\mathrm{cond}(V) = \displaystyle\int_{-1}^{\infty} \mathrm{codim}_V(V^{G_K^u})du$. Since the Galois action is continuous, V is fixed by an open subgroup of G_K and so the integral is finite. For any V, $\mathrm{cond}(V) \in \mathbb{Z}_{\geq 0}$ and $\mathrm{cond}(V) = 0$ if and only if V is unramified and $\mathrm{cond}(V) \leq 1$ if and only if V is tamely ramified.

(2.4.2) Let $K/\mathbb{Q}$ be a finite extension and V be a continuous complex finite dimensional representation of G_K.

Proposition 2.2. *The representation V is almost everywhere unramified.*

Proof. By the Brauer induction theorem $V = \sum n_i \mathrm{Ind}_{L_i}^K \chi_i$ for finite Galois extensions L_i and characters $\chi_i : G_{L_i} \to \mathbb{C}^\times$. It suffices to show the proposition for V a character χ since then V will be unramified at all finite places where no L_i nor χ_i is ramified. Now $\chi : G_K^{\mathrm{ab}} \to \mathbb{C}^\times$ is continuous and the kernel $\ker\chi$ will be open in $G_K^{\mathrm{ab}} \cong \mathbb{A}_K^\times / \overline{K^\times K_\infty^{\times,0}}$ and so will contain an open set of the form $U_S \prod_{v \notin S} \mathcal{O}_{K_v}^\times$ where $U_S \subset K_S^\times$ is an open set. Then χ will be unramified at $v \notin S$. □

Define the conductor $\mathrm{cond}(V) = \prod_{v \nmid \infty} (\varpi_v)^{\mathrm{cond}(V|_{G_{K_v}})}$ as an ideal of $\mathcal{O}_K$, the product being finite by Proposition 2.2. The representation V is unramified if and only if $\mathrm{cond}(V) = \mathcal{O}_K$ and it is tamely ramified if and only if $\mathrm{cond}(V)$ is square free.

Since V has a continuous action of G_K, one can find a finite Galois extension L/K such that G_L acts trivially on V. Thus the action of G_K factors through the discrete action of $G_{L/K}$. For every finite place v of K choose a place w of L. Then

$$\mathrm{cond}(V) = \prod_{v \nmid \infty} (\varpi_v)^{\mathrm{cond}(V|_{G_{L_w/K_v}})}$$

where $\overline{K}_v$ is chosen as containing L_w.

Proposition 2.3. *Let L/K be a finite extension of number fields. Then L as a vector space over K has a linear action of $G_{L/K}$ and the discriminant $D_{L/K}$ is equal to* $\mathrm{cond}(L)$ *as ideals of $\mathcal{O}_K$.*

Proof. For each place v of K fix an arbitrary place w of L. Recall that $D_{L/K} = N_{L/K}(\prod_v \mathcal{D}_{L_w/K_v})$ where $\mathcal{D}_{L_w/K_v}$ is the different and $v(\mathcal{D}_{L_w/K_v}) = \int_{-1}^{\infty} \left(1 - \frac{1}{|G^u_{L_w/K_v}|}\right) du$. Therefore

$$\begin{aligned} v(\mathrm{cond}(L)) &= \mathrm{cond}(L|G_{L_w/K_v}) \\ &= \int_{-1}^{\infty} \mathrm{codim}_L(L^{G^u_{L_w/K_v}}) du \\ &= \int_{-1}^{\infty} (|G_{L/K}| - |G_{L/K}/G^u_{L_w/K_v}|) du \\ &= [L:K] \int_{-1}^{\infty} ((1 - 1/|G^u_{L_w/K_v}|) du \\ &= [L:K] v_{K_v}(\mathcal{D}_{L_w/K_v}) \\ &= v(N_{L/K}(\mathcal{D}_{L_w/K_v})) \end{aligned}$$

□

2.5 Hilbert, ray and ring class fields

A little classical notation. The class group $\mathrm{Cl}(K)$, also known as the "wide" or "weak" class group, is the set of fractional ideals of $\mathcal{O}_K$ modulo principal ideals, equal to $\mathrm{Cl}_S(K)$ as defined above when $S = \{v \mid \infty\}$. The "narrow" or "strict" class group $\mathrm{Cl}^+(K)$ is the set of fractional ideals modulo principal ideals generated by totally positive elements, i.e., x such that for every real emberdding $\tau : K \hookrightarrow \mathbb{R}$, $\tau(x) > 0$.

Let $K/\mathbb{Q}$ be a number field. For any open subgroup U of $\mathbb{A}_K^\times$, $r_K(U)$ is an open subgroup of G_K^{ab} and so is of the form $G_{L_U}^{\mathrm{ab}}$ for a finite extension L_U/K. In fact $L_U = (K^{\mathrm{ab}})^{r_K(U)}$ is an abelian extension and

$$G_{L_U/K} \cong \mathbb{A}_K^\times / K^\times K_\infty^{\times,0} U$$

2.5.1 The Hilbert class field

Suppose $U = K_\infty^\times \prod_{v \nmid \infty} \mathcal{O}_v^\times$. Then L_U is called the (wide/weak) Hilbert class field H_K of K and $G_{H_K/K} \cong \mathbb{A}_K^\times / K^\times K_\infty^\times \prod \mathcal{O}_v^\times \cong \mathrm{Cl}(K)$.

Suppose $U^+ = K_\infty^{\times,0} \prod_{v \nmid \infty} \mathcal{O}_v^\times$. Then L_{U^+} is called the (narrow/strict) Hilbert class field H_K^+ of K and $G_{H_K^+/K} \cong \mathbb{A}_K^\times / K^\times K_\infty^{\times,0} \prod \mathcal{O}_v^\times \cong \mathrm{Cl}^+(K)$. Note that

$$H_K^+ / H_K = K^\times K_\infty^\times / K^\times K_\infty^{\times,0} \subset \prod_{v|\mathbb{R}} \{\pm 1\}$$

Two facts about Hilbert class fields: H_K/K is the maximal abelian extension which is unramified at every place while H_K^+ is the maximal abelian extension unramified at every finite place, and every ideal of K becomes principal in H_K^+.

We now give an example application.

Example 2.4. If $m \mid n$ then $h_{\mathbb{Q}(\mu_m)} \mid h_{\mathbb{Q}(\mu_n)}$.

Proof. Let H_m be the Hilbert class field of $\mathbb{Q}(\mu_m)$ and H_n be the Hilbert class field of $\mathbb{Q}(\mu_n)$. The extension $\mathbb{Q}(\mu_n)/\mathbb{Q}(\mu_m)$ (which is an extension since $m \mid n$) is totally ramified at every $p \mid n/m$ and so $\mathbb{Q}(\mu_n) \cap H_m = \mathbb{Q}(\zeta_m)$. Now $\mathbb{Q}(\mu_n)H_m/\mathbb{Q}(\mu_n)$ is unramified and abelian and so $\mathbb{Q}(\mu_n)H_m \subset H_n$. Therefore

$$\begin{aligned} h_{\mathbb{Q}(\mu_n)} &= [H_n : \mathbb{Q}(\mu_n)] \\ &= [H_n : H_m\mathbb{Q}(\mu_n)] |G_{H_m\mathbb{Q}(\mu_n)/\mathbb{Q}(\mu_n)}| \\ &= [H_n : H_m\mathbb{Q}(\mu_n)] |G_{H_m/\mathbb{Q}(\mu_m)}| \\ &= [H_n : H_m\mathbb{Q}(\mu_n)] h_{\mathbb{Q}(\mu_m)} \end{aligned}$$

as desired. □

2.5.2 Ray class fields

Suppose $\mathfrak{m}$ is an ideal of $\mathcal{O}_K$. Let $K_{\mathfrak{m}} = \{x \in K | x \equiv 1 \pmod{\mathfrak{m}}\}$ and $K_{\mathfrak{m}}^+$ consist of totally positive $x \in K_{\mathfrak{m}}$. Let $\mathrm{Cl}_{\mathfrak{m}}(K)$ be the set of ideals coprime to $\mathfrak{m}$ modulo the principal ideals generated by $K_{\mathfrak{m}}$ and let $\mathrm{Cl}_{\mathfrak{m}}^+(K)$ be the set of ideals coprime to $\mathfrak{m}$ modulo the principal ideals generated by $K_{\mathfrak{m}}^+$.

Let $U_{\mathfrak{m}}^+ = K_\infty^{\times,0} \prod_{v \nmid \infty} \mathcal{U}_K^{v(\mathfrak{m})}$ and $U_{\mathfrak{m}} = K_\infty^\times \prod_{v \nmid \infty} \mathcal{U}_K^{v(\mathfrak{m})}$. Then $H_{K,\mathfrak{m}} = L_{U_{\mathfrak{m}}}$ is called the weak ray class field and $H_{K,\mathfrak{m}}^+ = L_{U_{\mathfrak{m}}^+}$ is the strict ray class field of conductor $\mathfrak{m}$.

Proposition 2.5. *$\mathrm{Cl}_{\mathfrak{m}}^+ = \mathbb{A}_K^\times / K^\times U_{\mathfrak{m}}^+$ and $\mathrm{Cl}_{\mathfrak{m}} = \mathbb{A}_K^\times / K^\times U_{\mathfrak{m}}$.*

Proof. Let $x = (x_v) \in \mathbb{A}_K^\times$. The Chinese remainder theorem implies that there exists $y \in K^\times$ such that $xy = (x_v y)$ has the property that for $v \mid \mathfrak{m}$, $x_v y \in 1 + (\varpi_v)^{v(\mathfrak{m})} = \mathcal{U}_K^{v(\mathfrak{m})}$ and $x_v y$ is positive for every $v \mid \mathbb{R}$; elements of K with this property are $\equiv 1 \pmod{\mathfrak{m}}$ (and so in $K_{\mathfrak{m}}$) and totally positive. Attach to x the ideal $\prod_{v \nmid \mathfrak{m}} (\varpi_v)^{v(x_v y)}$ in which case $\mathbb{A}_K^\times / K^\times U_{\mathfrak{m}}^+$ becomes the set of ideals coprime to $\mathfrak{m}$ modulo principal ideals generated by totally positive $x \equiv 1 \pmod{\mathfrak{m}}$. Similarly for $U_{\mathfrak{m}}$. □

Then as before $G_{H_{K,\mathfrak{m}}/K} = \mathrm{Cl}_{\mathfrak{m}}(K)$ and $G_{H_{K,\mathfrak{m}}^+/K} = \mathrm{Cl}_{\mathfrak{m}}^+(K)$.

Example 2.6.

1. If $K = \mathbb{Q}$ and $\mathfrak{m} = n\mathbb{Z}$ then $\mathrm{Cl}_n^+(K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ and so the strict ray class field of conductor n is $\mathbb{Q}(\mu_n)$.
2. If $\mathfrak{m} = \mathcal{O}_K$ then $H_K = H_{K,\mathfrak{m}}$ and $H_K^+ = H_{K,\mathfrak{m}}^+$.

Proposition 2.7. *Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$. Then $H_{K,\mathfrak{m}}^+$ is the maximal abelian extension H of K such that $G_{H_w/K_v}^n = 0$ if $n \geq v(\mathfrak{m})$, where $w \mid v$ is an arbitrary place of H. In particular, the strict Hilbert class field H_K^+ is the maximal abelian extension of K which is unramified at every finite place.*

Proof. Let L/K be an abelian extension such that if v is a place of K and $w \mid v$ is an arbitrary place of L then $G_{L_w/K_v}^n = 0$. Recall Herbrandt's theorem that $G_{L_w/K_v}^n = G_{K_v}^{n,\mathrm{ab}} / G_{K_v}^{n,\mathrm{ab}} \cap W_{L_w}^{\mathrm{ab}}$ and so this is equivalent to $W_{L_w}^{\mathrm{ab}} \supset G_{K_v}^{n,\mathrm{ab}}$. Via the inverse of the Artin map this is equivalent to $r_{K_v}^{-1}(W_{L_w}^{\mathrm{ab}}) \supset \mathcal{U}_{K_v}^n$. Equivalently, using the global Artin map, the component at v of the open subgroup $r_K^{-1}(G_L^{\mathrm{ab}})$ of $\mathbb{A}_K^\times$ should contain $\mathcal{U}_{K_v}^n$.

That L is the largest abelian extension of K such that $G_{L_w/K_v}^n = 0$ for $n \geq v(\mathfrak{m})$ is equivalent to the fact that $U = r_K^{-1}(G_L^{\mathrm{ab}})$ is the largest open subgroup of G_K^{ab} such that the component in v is included in $\mathcal{U}_{K_v}^{v(\mathfrak{m})}$. The largest such U is $U_{\mathfrak{m}}^+$. □

Lecture 3
2013-04-05

Proposition 2.8. *Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$. Then the discriminant of $H = H_{K,\mathfrak{m}}$ over K is*

$$\prod_{v \mid \mathfrak{m}} \mathfrak{m}_v^{[H:K]\left(v(\mathfrak{m}) - \frac{1}{q_v - 1}\right)}$$

Proof. For simplicity write $H = H_{\mathfrak{m}}^+$. Since $(D_{L/K}) = N_{H/K}(\prod \mathfrak{m}_v^{v(\mathcal{D}_{H_w/K_v})})$ it suffices to show that for each finite place v of K (and an arbitrary choice $w \mid v$ of H) we have $v(\mathcal{D}_{H_w/K_v}) = v(\mathfrak{m}) - \frac{1}{q_v - 1}$. For this we need to know the cardinality of $G_{H_w/K_v}^n = G_{K_v}^{n,\mathrm{ab}} / G_{K_v}^{n,\mathrm{ab}} \cap W_{H_w}^{\mathrm{ab}}$ and via the inverse of the local Artin map this is $\mathcal{U}_v^n / (\mathcal{U}_v^n \cap N_{H_w/K_v} H_w^\times$. This is trivial if and only if $n \geq v(\mathfrak{m})$ which implies that $\mathcal{U}_v^n \subset N_{H_w/K_v} H_w^\times$ if and only if $n \geq v(\mathfrak{m})$. But H is maximal among such abelian extensions and so $N_{H_w/K_v} H_w^\times = \mathcal{U}_v^{v(\mathfrak{m})}$ giving $G_{H_w/K_v}^n \cong \mathcal{U}_v^n / \mathcal{U}_v^{v(\mathfrak{m})}$. Since $\mathcal{O}_{K_v}^\times / (1 + (\varpi_v)) \cong k_{K_v}^\times$ and $(1 + (\varpi_v)^i)/(1 + (\varpi_v)^{i+1}) \cong k_{K_v}$ it follows that

$|G^n_{H_w/K_v}| = q_v^{v(\mathfrak{m})-n}$ if $n \geq 1$ and $|G^0_{H_w/K_v}| = q_v^{v(\mathfrak{m})-1}(q_v - 1)$ as long as $v \mid \mathfrak{m}$. We compute the conductor of H as a G_{H_w/K_v}-representation (see the proof of Proposition 2.3:

$$\begin{aligned}
\mathrm{cond}(H) &= [H:K]\int_{-1}^{\infty}(1 - 1/|G^u_{H_w/K_v}|)du \\
&= [H:K]\sum_{n=0}^{v(\mathfrak{m})}(1 - 1/|G^n_{H_w/K_v}|) \\
&= [H:K]\left(v(\mathfrak{m}) + 1 - \frac{1}{q_v^{v(\mathfrak{m})-1}(q_v-1)} - \sum_{n=1}^{v(\mathfrak{m})}\frac{1}{q_v^{v(\mathfrak{m})-n}}\right) \\
&= [H:K]\left(v(\mathfrak{m}) - \frac{1}{q_v - 1}\right)
\end{aligned}$$

□

The following section was not covered in lecture

2.5.3 Ring class fields

An order $\mathcal{O} \subset K$ in a number field K is a finitely generated $\mathbb{Z}$-submodule of K such that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$. Every order $\mathcal{O}$ is contained in $\mathcal{O}_K$. The conductor of the order $\mathcal{O}$ is the cardinality of $\mathcal{O}_K/\mathcal{O}$.

If $K = \mathbb{Q}(\sqrt{-d})$ then every order is of the form $\mathcal{O} = \mathbb{Z} + \mathcal{O}_K f$ which has conductor f. An ideal I of $\mathcal{O}$ is said to be proper if $\mathcal{O} = \{x \in K | xI \subset I\}$; I is said to be coprime to f if $I + (f) = \mathcal{O}$. An ideal is proper if and only if it is equivalent to an ideal coprime to f. The ring class group $\mathrm{Cl}(\mathcal{O})$ is defined to be the set of proper ideals of $\mathcal{O}$ modulo principal ideals. There is an isomorphism between ideals of $\mathcal{O}_K$ coprime to the conductor f and proper ideals of $\mathcal{O}$, the map from the first to the second being $I \mapsto I \cap \mathcal{O}$ and the inverse being $I \mapsto I\mathcal{O}_K$. As such $\mathrm{Cl}(\mathcal{O})$ is the set of ideals of $\mathcal{O}$ coprime to f modulo principal ideals generated by x such that $x \equiv n \pmod{f\mathcal{O}_K}$ for some integer n coprime to f.

Finally, $\mathrm{Cl}(\mathcal{O}) \subset \mathrm{Cl}_{f\mathcal{O}_K}(K)$ and so there is an open set $U_{\mathcal{O}} \supset U_{f\mathcal{O}_K}$ such that $Cl(\mathcal{O}) \cong \mathbb{A}_K^\times / K^\times K_\infty^\times U_{\mathcal{O}}$ in which case $\mathrm{Cl}(\mathcal{O}) = G_{L_{\mathcal{O}}/K}$ where $L_{\mathcal{O}}$ is the ring class field of $\mathcal{O}$. It shows up in the study of Heegner points.

Proposition 2.9. *Let $K = \mathbb{Q}(\sqrt{-d})$ with (wide) Hilbert class field H_K. For $f \geq 2$ consider $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ the order of conductor f. Let K_f be the ring class field of $\mathcal{O}$. Then K_f is Galois over H_K and $G_{K_f/H_K} \cong (\mathcal{O}_K/f\mathcal{O}_K)^\times/(\mathbb{Z}/f\mathbb{Z})^\times$.*

Proof. The Galois group $G_{H_{K,f}/H_K}$ is isomorphic to the group of principal ideals of $\mathcal{O}_K$ coprime to f modulo those principal ideals generated by $x \equiv c \pmod{f\mathcal{O}_K}$ with c coprime to f. □

End of section not covered in lecture

---

3 Selmer groups and applications

3.1 Selmer systems and Selmer groups

(3.1.1) Let $K/\mathbb{Q}$ be a number field and M a finite discrete G_K-module. Then M has trivial action of G_L for some finite extension L/K and so M will be unramified at all places v where L/K is unramified.

A **Selmer system** is a collection $\mathcal{L} = \{\mathcal{L}_v\}$ of $\mathcal{L}_v \subset H^1(G_{K_v}, M)$ such that $\mathcal{L}_v = H^1_{\mathrm{ur}}(G_{K_v}, M)$ for almost all v.

Proposition 3.1. *Define $\mathcal{L}_v^\perp \subset H^1(G_{K_v}, M^*(1))$ as the annihilator of $\mathcal{L}_v$ under the local Tate pairing. Then $\mathcal{L}^\perp = \{\mathcal{L}_v^\perp\}$ is also a Selmer system, called the dual Selmer system of $\mathcal{L}$.*

Proof. This follows from the fact that $H^1_{\mathrm{ur}}(G_{K_v}, M)^\perp = H^1_{\mathrm{ur}}(G_{K_v}, M^*(1))$. □

Definition 3.2. The **Selmer group** is $H^1_{\mathcal{L}}(K, M) = \{x \in H^1(G_K, M) | \operatorname{res}_v x \in \mathcal{L}_v\}$.

Proposition 3.3. *Let $\mathcal{L}$ be a Selmer system and let S be a set of places containing the infinite places, finite places v such that $\mathcal{L}_v \neq H^1_{\mathrm{ur}}(G_{K_v}, M)$ and finite places v such that I_{K_v} does not act trivially on M. Let K_S/K be the largest extension which is unramified outside S and let $G_{K,S} = G_{K_S/K}$. Then*

$$0 \to H^1_{\mathcal{L}}(K, M) \to H^1(G_{K,S}, M) \to \oplus_{v \in S} H^1(G_{K_v}, M)/\mathcal{L}_v$$

is exact.

Proof. By definition $H^1_{\mathcal{L}}(K, M)$ is the kernel of the map $H^1(G_K, M) \to \prod_v H^1(G_{K_v}, M)/\mathcal{L}_v$. If $v \notin S$ then $\mathcal{L}_v = H^1_{\mathrm{ur}}(K_v, M)$ is the kernel of the restriction map $H^1(K_v, M) \to H^1(I_v, M) \cong \mathrm{Hom}(I_v, M)$. Therefore $\prod_v H^1(G_{K_v}, M)/\mathcal{L}_v \subset \oplus_{v \in S} H^1(G_{K_v}, M)/\mathcal{L}_v \oplus \prod_{v \notin S} \mathrm{Hom}(I_v, M)$.

Suppose $c \in H^1(K, M)$ is the image of some class in $H^1_{\mathcal{L}}(K, M)$. Then $c|_{I_v}$ is the trivial map $I_v \to M$ when $v \notin S$. The Galois group G_{K_S} is generated by I_v for $v \notin S$ and so $c|_{G_{K_S}}$ is the trivial class. But then by inflation-restriction $c \in H^1(G_{K,S}, M)$ since G_{K_S} acts trivially on M. □

3.2 Global duality and dual Selmer groups

This section is about the Tate-Poitou nine-term exact sequence, which is a global version of local Tate duality, and its application to Selmer groups.

3.2.1 Tate-Poitou duality

Let K be a number field and let S be a finite set of places containing the infinite places. Let M be a finite G_K-module and suppose that S contains all the finite places v such that I_v acts nontrivially on M and all the finite places v such that $v(|M|) > 0$. Then M is naturally a $G_{K,S}$-module.

Define

$$\widehat{H}^0(K_v, M) = \begin{cases} M^{G_{K_v}} & v \nmid \infty \\ M^{G_{K_v}}/N_{\overline{K}_v/K_v} M & v \mid \mathbb{R} \\ 0 & v \mid \mathbb{C} \end{cases}$$

If A is an abelian group write $A^\vee = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$. If M is a finite G_K-module write $M^* = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ with the action $(g\phi)(m) = \phi(g^{-1}m)$.

Theorem 3.4. *Suppose M is a finite $G_{K,S}$ module as above. Then*

1. *There is an exact sequence*

$$\begin{aligned} 0 \to H^0(G_{K,S}, M) \to \oplus_{v \in S} \widehat{H}^0(K_v, M) \to H^2(G_{K,S}, M^*(1))^\vee \to \\ \to H^1(G_{K,S}, M) \to \oplus_{v \in S} H^1(K_v, M) \to H^1(G_{K,S}, M^*(1))^\vee \to \\ \to H^2(G_{K,S}, M) \to \oplus_{v \in S} H^2(K_v, M) \to H^0(G_{K,S}, M^*(1))^\vee \to 0 \end{aligned}$$

2. *If $i \geq 3$ then $H^i(G_{K,S}, M) \cong \oplus_{v \in S} H^i(K_v, M)$.*

Lecture 4
2013-04-08

3.2.2 Dual Selmer groups

Suppose $\mathcal{L}$ is a Selmer system and $\mathcal{L}^\perp$ is the dual Selmer system for the cohomology of a finite G_K-module M.

Proposition 3.5. *There is an exact sequence*

$$0 \to H^0(G_{K,S}, M) \to \oplus_{v\in S}\widehat{H}^0(K_v, M) \to H^2(G_{K,S}, M^*(1))^\vee \to$$
$$\to H^1_{\mathcal{L}}(K, M) \to \oplus_{v\in S}\mathcal{L}_v \to H^1(G_{K,S}, M^*(1))^\vee \to H^1_{\mathcal{L}^\perp}(K, M^*(1))^\vee \to 0$$

Proof. Tate-Poitou implies that

$$0 \to H^0(G_{K,S}, M) \to \oplus_{v\in S}\widehat{H}^0(K_v, M) \to H^2(G_{K,S}, M^*(1))^\vee \to$$
$$\to H^1(G_{K,S}, M) \to \oplus_{v\in S}H^1(K_v, M) \to H^1(G_{K,S}, M^*(1))^\vee$$

is exact. Since $\mathcal{L}_v \subset H^1(K_v, M)$ is sequence gives the exact sequence

$$0 \to H^0(G_{K,S}, M) \to \oplus_{v\in S}\widehat{H}^0(K_v, M) \to H^2(G_{K,S}, M^*(1))^\vee \to \mathcal{K} \to \oplus_{v\in S}\mathcal{L}_v \to H^1(G_{K,S}, M^*(1))^\vee$$

where $\mathcal{K}$ is the preimage of $\oplus_{v\in S}\mathcal{L}_v$ under the restriction map $H^1(G_{K,S}, M) \to \oplus_{v\in S}H^1(K_v, M)$. By definition $\mathcal{K} = H^1_{\mathcal{L}}(K, M)$ and so get an exact sequence

$$0 \to H^0(G_{K,S}, M) \to \oplus_{v\in S}\widehat{H}^0(K_v, M) \to H^2(G_{K,S}, M^*(1))^\vee \to H^1_{\mathcal{L}}(K, M) \to \oplus_{v\in S}\mathcal{L}_v \to H^1(G_{K,S}, M^*(1))^\vee$$

Proposition 3.3 replacing M by $M^*(1)$ and $\mathcal{L}$ by $\mathcal{L}^\perp$ gives

$$0 \to H^1_{\mathcal{L}^\perp}(K, M^*(1)) \to H^1(G_{K,S}, M^*(1)) \to \oplus_{v\in S}H^1(K_v, M^*(1))/\mathcal{L}_v^\perp$$

which after dualizing and using $(H^1(K_v, M^*(1))/\mathcal{L}_v^\perp)^\vee \cong \mathcal{L}_v$ gives

$$\oplus_{v\in S}\mathcal{L}_v \to H^1(G_{K,S}, M^*(1))^\vee \to H^1_{\mathcal{L}^\perp}(K, M^*(1))^\vee \to 0$$

Putting everything together gives the proposition. □

3.3 Euler characteristics and sizes of Selmer groups

3.3.1 The Euler characteristic formulae

Proposition 3.6. *If $K/\mathbb{Q}_p$ is a finite extension and M is a finite G_K-module then $H^i(K, M)$ is finite for $i \geq 0$. Moreover, $H^i(K, M) = 0$ for $i \geq 3$.*

Theorem 3.7. *Let $K/\mathbb{Q}_p$ be a finite extension and M a finite G_K-module. Then*

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

Proposition 3.8. *If M is a finite $G_{K,S}$-module then $H^i(G_{K,S}, M)$ is finite for $i \geq 0$.*

Proof. This is clear when $i = 0$ as $H^0(G_{K,S}, M) \subset M$. When $i \geq 3$ then $H^i(G_{K,S}, M) \cong \oplus_{v\in S}H^i(K_v, M)$ by Theorem 3.4 and finiteness follows from Proposition 3.6. Again by Theorem 3.4 we get exactness for $H^1(G_{K,S}, M^*(1))^\vee \to H^2(G_{K,S}, M) \to \oplus_{v\in S}H^2(K_v, M)$ and finiteness of $H^2(G_{K,S}, M)$ follows from Proposition 3.6 if we assume finiteness of $H^1(G_{K,S}, M^*(1))^\vee$. Therefore it suffices to treat the case of $i = 1$ and show that $H^1(G_{K,S}, M)$ is finite for M finite.

Since M is a $G_{K,S}$-module there exists a finite Galois subextension L/K of K_S/K such that $G_{K_S/L}$ acts trivially on M. Inflation-restriction gives $0 \to H^1(L/K, M) \to H^1(G_{K,S}, M) \to H^1(G_{K_S/L}, M)$. Let S_L for the set of places of L lying above places of K in S in which case $L_{S_L} = K_S$ and so $G_{K_S/L} = G_{L,S_L}$.

Therefore to show finiteness of $H^1(G_{K,S}, M)$ it suffices to treat the case when $G_{K,S}$ acts trivially on M in which case

$$H^1(G_{K,S}, M) \cong \mathrm{Hom}(G_{K,S}, M) \cong \mathrm{Hom}(G_{K,S}^{\mathrm{ab}}, M)$$

It is unfortunate that we use K_S as both the maximal extension of K which is unramified outside S and as $\prod_{v\in S} K_v$ but it should be clear which one we mean from context. So $G_{K,S}^{\mathrm{ab}} \cong \mathbb{A}_K^\times / K^\times K_\infty^{\times,0} \prod_{v\notin S} \mathcal{O}_v^\times$. We have already seen in the proof of Theorem 2.1 that we have an exact sequence

$$0 \to K_S^\times / \mathcal{O}_K[1/S]^\times \to \mathbb{A}_K^\times / K^\times \prod_{v\notin S} \mathcal{O}_v^\times \to \mathrm{Cl}_S(K) \to 0$$

Since $\mathrm{Cl}_S(K)$ is finite to show that $\mathrm{Hom}(G_{K,S}^{\mathrm{ab}}, M)$ is finite is suffices to show that $\mathrm{Hom}(K_S^\times/\mathcal{O}_K[1/S]^\times, M)$ is finite. But $\mathrm{Hom}(K_S^\times/\mathcal{O}_K[1/S]^\times, M) \hookrightarrow \prod_{v\in S} \mathrm{Hom}(K_v^\times, M)$ and $\mathrm{Hom}(K_v^\times, M) \cong \mathrm{Hom}(G_{K_v}, M) \cong H^1(K_v, M)$ is finite by Proposition 3.6. □

Theorem 3.9. *Let $K/\mathbb{Q}$ be a number field, M a finite G_K-module and S as in Theorem 3.4. Then*

$$\chi(K, M) = \frac{|H^0(G_{K,S}, M)||H^2(G_{K,S}, M)|}{|H^1(G_{K,S}, M)|} = \frac{\prod_{v|\infty} |H^0(K_v, M)|}{|M|^{[K:\mathbb{Q}]}}$$

3.3.2 Sizes of Selmer groups and a theorem of Wiles

Lemma 3.10. *Let $K/\mathbb{Q}$ be a number field and M finite, $\mathcal{L}$ and S as in Proposition 3.3. Then $H^1_{\mathcal{L}}(K, M)$ is finite.*

Proof. Proposition 3.3 implies that $H^1_{\mathcal{L}}(K, M) \subset H^1(G_{K,S}, M)$ which we know is finite by Theorem 3.4. □

Theorem 3.11. *Let $K/\mathbb{Q}$ be a number field and M, $\mathcal{L}$ and S as in Proposition 3.3. Then*

$$\frac{|H^1_{\mathcal{L}}(K, M)|}{|H^1_{\mathcal{L}^\perp}(K, M^*(1))|} = \frac{|H^0(K, M)|}{|H^0(K, M^*(1))|} \prod_v \frac{|\mathcal{L}_v|}{|H^0(K_v, M)|}$$

Example 3.12. Let $p > 2$ be a prime and S be a finite set of places of $\mathbb{Q}$ containing p and ∞. What is the number of abelian extensions of $\mathbb{Q}$ of degree p^n which are unramified at all places $\ell \notin S$?

Proof. Recall that $G_{\mathbb{Q}}^\vee \cong G_{\mathbb{Q}}^{\mathrm{ab},\vee}$ and so every continuous homomorphism $\phi : G_{\mathbb{Q}} \to \mathbb{Q}/\mathbb{Z}$ has open kernel $\ker\phi = G_L$ for a finite abelian extension $L/\mathbb{Q}$. If $[L : \mathbb{Q}] = m$ then for every $g \in G_{\mathbb{Q}}$, $g^m \in G_L$ and so $m\phi(g) = \phi(g^m) \in \phi(G_L) = 0$ and so $\phi : G_{\mathbb{Q}} \to \mathbb{Z}/m\mathbb{Z}$. The map taking ϕ to L is not injective, as $\mathrm{Aut}\, G_{L/\mathbb{Q}}$ acts on the set of ϕ. Reciprocally, every $L/\mathbb{Q}$ cyclic of degree m produces $\varphi(m) = |\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})|$ homomorphisms ϕ.

Every $\phi : G_{\mathbb{Q}} \to M = \mathbb{Z}/p^n\mathbb{Z}$ (with trivial $G_{\mathbb{Q}}$-action produces a cyclic extension of degree dividing p^n. Therefore we need to study $\mathrm{Hom}(G_{\mathbb{Q}}, M) \cong H^1(\mathbb{Q}, M)$. If $L/\mathbb{Q}$ is as above then L is unramified at $\ell \notin S$ if and only if $\phi(I_\ell) = 0$ if and only if $\phi|_{G_{\mathbb{Q}_\ell}} \in H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M)$. Therefore $L/\mathbb{Q}$ is unramified outside S if and only if $\phi \in H^1_{\mathcal{L}}(\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z})$ where $\mathcal{L}_\ell = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M)$ for $\ell \notin S$ and $\mathcal{L}_v = H^1(\mathbb{Q}_v, M)$ when $v \in S$. The problem now becomes to compute $h_n = |H^1_{\mathcal{L}}(\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z})|$. The number of ϕ with image $\mathbb{Z}/p^n\mathbb{Z}$ is exactly $h_n - h_{n-1}$ and $\mathrm{Aut}(\mathbb{Z}/p^n\mathbb{Z})$ acts on this giving $\frac{h_n - h_{n-1}}{\varphi(p^n)}$ extensions $L/\mathbb{Q}$ cyclic of order p^n unramified outside S.

Note that $\mathcal{L}_v^\perp = 0$ for $v \in S$ and $\mathcal{L}_\ell^\perp = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M)$ for $\ell \notin S$. Suppose $c \in H^1_{\mathcal{L}^\perp}(\mathbb{Q}, M^*(1))$. Here $M^*(1) = \mu_{p^n}$ and so $c \in H^1(\mathbb{Q}, \mu_{p^n})$ such that $c|_{\mathbb{Q}_\ell} \in \mathcal{L}_\ell^\perp \subset H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, \mu_{p^n})$ for all ℓ.

By Kummer theory $c(g) = \frac{g(\sqrt[p^n]{\alpha})}{\sqrt[p^n]{\alpha}}$ where $\alpha \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^n}$, since $H^1(\mathbb{Q}, \mu_{p^n}) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^n}$. Since c is unramified at all primes ℓ it follows that c is trivial in $H^1(I_{\mathbb{Q}_\ell}, \mu_{p^n}) \cong \mathbb{Q}_\ell^{\mathrm{ur},\times}/(\mathbb{Q}_\ell^{\mathrm{ur},\times})^{p^n}$. Therefore $\alpha \in (\mathbb{Q}_\ell^{\mathrm{ur},\times})^{p^n}$. In particular, $v_\ell(\alpha) \in p^n v_\ell(\mathbb{Q}_\ell^{\mathrm{ur},\times}) = p^n\mathbb{Z}$. Let $\alpha = \pm\prod_\ell \ell^{a_\ell}$ in which case we just showed $p^n \mid a_\ell$. Therefore $\alpha = (\pm\prod_\ell \ell^{a_\ell p^{-n}})^{p^n} \in (\mathbb{Q}^\times)^{p^n}$ since $p > 2$. This shows that c is trivial and so $H^1_{\mathcal{L}^\perp}(\mathbb{Q}, M^*(1)) = 0$.

By Theorem 3.11 it follows that

$$|H^1_{\mathcal{L}}(\mathbb{Q},\mathbb{Z}/p^n\mathbb{Z})| = \frac{|H^0(\mathbb{Q},\mathbb{Z}/p^n\mathbb{Z})|}{|H^0(\mathbb{Q},\mu_{p^n})|}\prod_v \frac{|\mathcal{L}_v|}{|H^0(\mathbb{Q}_v,\mathbb{Z}/p^n\mathbb{Z})|}$$
$$= p^n \prod_{v\in S}\frac{|H^1(\mathbb{Q}_v,\mathbb{Z}/p^n\mathbb{Z})|}{|H^0(\mathbb{Q}_v,\mathbb{Z}/p^n\mathbb{Z})|}$$

since $H^0(\mathbb{Q},\mathbb{Z}/p^n\mathbb{Z}) = \mathbb{Z}/p^n\mathbb{Z}$ and $H^0(\mathbb{Q},\mu_{p^n}) = 0$. The second line in the equation above comes from the first paragraph of the proof of Theorem 3.11. Now $H^1(\mathbb{R},\mathbb{Z}/p^n\mathbb{Z}) \cong \{0\}$ and $H^0(\mathbb{R},\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/p^n\mathbb{Z}$ while for ℓ a prime, Theorem 3.7 implies that

$$\chi(\mathbb{Q}_\ell,\mathbb{Z}/p^n\mathbb{Z}) = \frac{|H^0(\mathbb{Q}_\ell,\mathbb{Z}/p^n\mathbb{Z})||H^2(\mathbb{Q}_\ell,\mathbb{Z}/p^n\mathbb{Z})|}{|H^1(\mathbb{Q}_\ell,\mathbb{Z}/p^n\mathbb{Z})|} = |\mathbb{Z}/p^n\mathbb{Z}|_{\mathbb{Q}_\ell} = |p^n|_{\mathbb{Q}_\ell}$$

Therefore

$$\frac{|H^1(\mathbb{Q}_v,\mathbb{Z}/p^n\mathbb{Z})|}{|H^0(\mathbb{Q}_v,\mathbb{Z}/p^n\mathbb{Z})|} = \frac{|H^2(\mathbb{Q}_\ell,\mathbb{Z}/p^n\mathbb{Z})|}{|p^n|_{\mathbb{Q}_\ell}}$$

But by local Tate duality $|H^2(\mathbb{Q}_\ell,\mathbb{Z}/p^n\mathbb{Z})| = |H^0(\mathbb{Q}_\ell,\mu_{p^n})^\vee| = |H^0(\mathbb{Q}_\ell,\mu_{p^n})| = |\mu_{p^n}(\mathbb{Q}_\ell)| = |\mu_{p^n}(\mathbb{F}_\ell)| = (p^n,\ell-1)$. Finally,

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

Finally the number of $L/\mathbb{Q}$ cyclic of order p^n unramified outside of S is then

$$\frac{h_n - h_{n-1}}{p^{n-1}(p-1)} = \prod_{\ell\in S-\infty}(p^n,\ell-1) + \prod_{\ell\in S-\infty}(p^{n-1},\ell-1)\left(\frac{p^{|\{\ell\in S-\infty|p^n|\ell-1\}|}-1}{p-1}\right)$$

□

Proof of Theorem 3.11. First note that if $v\notin S$ then M is an unramified G_{K_v}-module and so $H^0(K_v^{\mathrm{ur}}/K_v,M)\to M \xrightarrow{\mathrm{Frob}_v^{-1}} M \to H^1_{\mathrm{ur}}(K_v,M)\to 0$ is exact. Therefore $|H^1_{\mathrm{ur}}(K_v,M)| = |H^0(K_v^{\mathrm{ur}}/K_v,M)| = |H^0(K_v,M)|$. In particular the product in the theorem is finite.

Proposition 3.5 then implies that

$$\frac{|H^1_{\mathcal{L}}(K,M)|}{|H^1_{\mathcal{L}^\perp}(K,M^*(1))|} = \frac{|H^2(G_{K,S},M^*(1))^\vee||H^0(G_{K,S},M)|}{|H^1(G_{K,S},M^*(1))^\vee|}\prod_{v\in S}\frac{|\mathcal{L}_v|}{|\widehat{H}^0(K_v,M)|}$$

If A is a finite abelian group then $|A| = |A^\vee|$. Note that M is unramified outside S and so $M^{G_{K_S}} = M$. Thus $H^0(K,M) = M^{G_K} = (M^{G_{K_S}})^{G_{K,S}} = H^0(G_{K,S},M)$. This gives

$$\frac{|H^1_{\mathcal{L}}(K,M)|}{|H^1_{\mathcal{L}^\perp}(K,M^*(1))|} = \chi(K,M^*(1))\frac{|H^0(K,M)|}{|H^0(K,M^*(1))|}\prod_{v\in S}\frac{|\mathcal{L}_v|}{|\widehat{H}^0(K_v,M)|}$$

But Theorem 3.9 implies that

$$\chi(K,M^*(1)) = \frac{\prod_{v|\infty}|H^0(K_v,M^*(1))|}{|M^*(1)|^{[K:\mathbb{Q}]}}$$

and so, since $|M| = |M^*(1)|$,

$$\frac{|H^1_{\mathcal{L}}(K,M)|}{|H^1_{\mathcal{L}^\perp}(K,M^*(1))|} = \frac{\prod_{v|\infty}|H^0(K_v,M^*(1))|}{|M|^{[K:\mathbb{Q}]}}\frac{|H^0(K,M)|}{|H^0(K,M^*(1))|}\prod_{v\in S}\frac{|\mathcal{L}_v|}{|\widehat{H}^0(K_v,M)|}$$

so we only need to show that

$$\frac{\prod_{v|\infty}|H^0(K_v,M^*(1))|}{|M|^{[K:\mathbb{Q}]}} = \prod_{v\in S}\frac{|\widehat{H}^0(K_v,M)|}{|H^0(K_v,M)|}$$

But

$$\begin{aligned}\prod_{v\in S}\frac{|\widehat{H}^0(K_v,M)|}{|H^0(K_v,M)|} &= \prod_{v|\infty}\frac{|\widehat{H}^0(K_v,M)|}{|H^0(K_v,M)|}\\ &= \prod_{v|\mathbb{R}}\frac{|\widehat{H}^0(K_v,M)|}{|H^0(K_v,M)|}\prod_{v|\mathbb{C}}\frac{|\widehat{H}^0(K_v,M)|}{|H^0(K_v,M)|}\\ &= \prod_{v|\mathbb{R}}\frac{|M^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}/N_{\mathbb{C}/\mathbb{R}}M|}{|M^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}|}\prod_{v|\mathbb{C}}|M|^{-1}\end{aligned}$$

and

$$\begin{aligned}\frac{\prod_{v|\infty}|H^0(K_v,M^*(1))|}{|M|^{[K:\mathbb{Q}]}} &= \prod_{v|\mathbb{R}}|M|^{-1}|H^0(K_v,M^*(1))|\prod_{v|\mathbb{C}}|M|^{-2}|H^0(K_v,M^*(1))|\\ &= \prod_{v|\mathbb{R}}|M|^{-1}|H^0(K_v,M^*(1))|\prod_{v|\mathbb{C}}|M|^{-1}\end{aligned}$$

Write $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1,c\}$. Then it suffices to show that

$$\frac{|M^{c-1}/(c+1)M|}{|M^{c-1}|} = \frac{|(M^*(1))^{c-1}|}{|M|}$$

and this follows from

$$\begin{aligned}|(M^*(1))^{c-1}| &= |\ker(c-1 : M^*(1)\to M^*(1))|\\ &= |\ker(c+1 : M^*\to M^*)|\\ &= |\operatorname{coker}(c+1 : M\to M)|\\ &= |M|/|\operatorname{Im}(c+1 : M\to M)|\end{aligned}$$

□

Lecture 6
2013-04-12

---

4 Rational points on elliptic curves

4.1 Facts about elliptic curves

Definition 4.1. Let K be a field. An elliptic curve over K is a smooth curve $y^2z = x^3 + axz^2 + bz^3$ in $\mathbb{P}^2_K$ whose solutions $E(A) = \{(x:y:z)\in\mathbb{P}^2(A) | y^2z = x^3+axz^2+bz^3\}$ form an abelian group with $0 = (0:1:0)$ the point at infinity for any K-algebra A.

Theorem 4.2. *If $K/\mathbb{Q}$ is a number field and E/K is an elliptic curve then $E(K)$ is a finitely generated abelian group. The rank of E is defined as the rank of $E(K)$.*

To prove this theorem we need to collect some facts about elliptic curves.

(4.1.1) First if $M/L/K$ are field extensions then $E(M)$ has an action of $G_{M/L}$ which commuted with the group law. Moreover, $E(M)^{G_{M/L}} = E(L)$.

(4.1.2) If $n > 1$ is an integer there is a map $[n] : E(A) \to E(A)$ given by $P \mapsto P + \cdots + P$ exactly n times. Write $E(A)[n] = \ker([n])$. If E is defined over a field K and L/K is an extension then $E(L)[n]$ is a finite group. Note that $G_{L/K}$ acts on $E(L)[n]$. The map $[n]$ on $E(\overline{K})$ is surjective.

(4.1.3) Let K be a number field. If one clears denominators in the equation of E and v is a place of K such that the equation $y^2z = x^3 + axz^2 + bz^3$ is still smooth over the residue field k_v then E is said to have good reduction at v. If n is an integer such that $v \nmid n$ then

$$E(K)[n] \hookrightarrow E(k_v)$$

(4.1.4) Let K be a number field. Consider the function $H : \mathbb{P}^2(K) \to [1, \infty)$ defined by

$$H(x : y : z) = \left(\prod_v \max(|x|_v, |y|_v, |z|_v) \right)^{1/[K:\mathbb{Q}]}$$

This is well-defined because if $\lambda \in K^\times$ then $\prod_v |\lambda|_v = 1$. Moreover, $H(x : y : z)$ does not depend on the number field K over which $(x : y : z)$ is defined. That $H(x : y : z) \geq 1$ follows from the fact that $H(x : y : z) \geq (\prod_v |x|_v)^{1/[K:\mathbb{Q}]} = 1$.

Consider $h : E(K) \to [0, \infty)$ defined by $h(P) = \log H(P)$. Then

1. for any $C > 0$, $\{P \in E(K) | h(P) \leq C\}$ is a finite set,
2. for any $Q \in E(K)$ there exists a constant $C_{E,Q}$ such that $h(P + Q) \leq 2h(P) + C_{E,Q}$ for all $P \in E(K)$ and
3. there exists a constant $C_{E,n}$ such that $h([n]P) \geq n^2 h(P) - C_{E,n}$.

4.2 Cohomology of elliptic curves over finite fields

In this section k represents a finite field with q elements.

Lemma 4.3. *Let C be a smooth projective curve of genus 1 over k. If C has a rational point over some finite extension of k then it has a rational point over k.*

Proof. Riemann-Roch for curves shows that the zeta function of C has the form

$$Z(C, X) = \frac{1 - aX + qX^2}{(1 - X)(1 - qX)}$$

where

$$Z(C, X) = \exp\left(\sum_{r \geq 1} |C(\mathbb{F}_{q^r})| X^r / r \right)$$

If $C(\mathbb{F}_q) = 0$ then $Z(C, X) \equiv 1 \pmod{X^2}$ by definition. The formula above then gives $a = q + 1$ in which case $Z(C, X) = 1$. But the $C(\mathbb{F}_{q^r}) = 0$ for all r contradicting the hypothesis. □

Proposition 4.4 (Lang)**.** *Let k be a finite field and let E/k be an elliptic curve. Then $H^1(k, E(\overline{k})) = 0$.*

Proof. Let $c \in H^1(k, E(\overline{k}))$. Embed $E(\overline{k}) \hookrightarrow \mathrm{Aut}(E(\overline{k}))$ of automorphisms over $\overline{k}$ by sending P to $t_p(Q) = P + Q$. The Galois cohomology group $H^1(k, \mathrm{Aut}(E(\overline{k})))$ represents forms of E over k. Let C be the form of E over k represented by the cohomology class $-c$. In other words C is a smooth projective curve of genus 1 over k with a $\overline{k}$-isomorphism $\phi : C/\overline{k} \cong E/\overline{k}$ such that $\phi^g \phi^{-1} = t_{-c(g)}$ where $\phi^g(x) = g(\phi(g^{-1}x))$.

Lemma 4.3 implies that C has a point $P \in C(k)$ and let $Q = \phi(P)$. Then $\phi^g\phi^{-1}Q = \phi^g(P) = g(\phi(P)) = g(Q)$ since P is defined over k. But $\phi^g\phi^{-1}Q = t_{-c(g)}Q = Q - c(g)$ which gives $c(g) = Q - g(Q)$. Thus c is trivial in $H^1(k, E(\overline{k}))$. □

4.3 Descent for rational points

Lemma 4.5 (Descent)**.** *Let K be a number field and E/K an elliptic curve. If for some integer m, $E(K)/mE(K)$ is finite, then $E(K)$ is finitely generated.*

Proof. Let $E(K)/mE(K)$ be represented by $Q_1, \ldots, Q_r$ with $Q_1, \ldots, Q_r \in E(K)$. We will show by descent that there exists a constant C such that $Q_1, \ldots, Q_r$ and the finitely many points $\{P \in E(K) | h(P) \leq C\}$ generate $E(K)$.

Indeed, let $C_1 = \max C_{E,-Q_i}$ and $C = 1 + (C_{E,m} + C_1)/2$. Let $P \in E(K)$. We would like to express P as a sum of Q_i and points of height at most C. Write $P = mP_1 + Q_{i_1}$, and for $n \geq 1$ let $P_n = mP_{n+1} + Q_{i_n}$. Then

$$\begin{aligned} h(P_n) &\leq \frac{1}{m^2}(h([m]P_n) + C_{E,m}) \\ &= \frac{1}{m^2}(h(P_{n-1} - Q_{i_n}) + C_{E,m}) \\ &\leq \frac{1}{m^2}(2h(P_{n-1}) + C_{E,m} + C_{E,-Q_{i_n}}) \\ &\leq \frac{1}{m^2}(2h(P_{n-1}) + C_{E,m} + C_1) \end{aligned}$$

Inductively we get

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\sum_{i=1}^{n} \frac{2^{i-1}}{m^{2i}}\right)(C_{E,m} + C_1) \\ &\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_{E,m} + C_1}{m^2 - 2} \\ &\leq 2^{-n}h(P) + C - 1 \end{aligned}$$

Now if $2^n > h(P)$ it follows that $h(P_n) < C$ and $P = [m^n]P_n + \sum_{j=1}^{n} [m^{j-1}]Q_{i_j}$. □

4.4 Selmer groups for elliptic curves

Lemma 4.6. *Let $n > 1$ be an integer, K a field and E an elliptic curve over E. Then*

$$0 \to E(K)/nE(K) \xrightarrow{\delta_K} H^1(K, E(\overline{K})[n]) \xrightarrow{i_K} H^1(K, E(\overline{K}))[n] \to 0$$

Proof. This is Kummer theory for elliptic curves. Take the G_K-cohomology of the short exact sequence $0 \to E(\overline{K})[m] \to E(\overline{K}) \xrightarrow{[n]} E(\overline{K}) \to 0$ and get the long exact sequence

$$E(K) \xrightarrow{n} E(K) \to H^1(K, E(\overline{K})[n]) \to H^1(K, E(\overline{K})) \xrightarrow{n} H^1(K, E(\overline{K}))$$

giving

$$0 \to E(K)/nE(K) \to H^1(K, E(\overline{K})[n]) \to H^1(K, E(\overline{K}))[n] \to 0$$

□

Definition 4.7. Let K be a number field and E an elliptic curve over K. The n-Selmer group of E is

$$\mathrm{Sel}^n(E/K) = \ker\left(H^1(K, E(\overline{K})[n]) \to \prod_v H^1(K, E(\overline{K}_v))[n]\right)$$

where the map to $H^1(K, E(\overline{K}_v))[n]$ is restriction to G_{K_v} followed by j_{K_v}.

The purpose of this section is to express $\mathrm{Sel}^n(E/K)$ as the Selmer group $H^1_{\mathcal{L}}(K, E(\overline{K})[n])$ for a suitable Selmer system $\mathcal{L}$.

Proposition 4.8. *Let $\mathcal{L}_v$ be the image of $E(K_v)/nE(K_v)$ via δ_{K_v} in $H^1(K_v, E(\overline{K}_v)[n])$. Then $\mathcal{L} = \{\mathcal{L}_v\}$ is a Selmer system and*

$$\mathrm{Sel}^n(E/K) = H^1_{\mathcal{L}}(K, E(\overline{K})[n])$$

Lecture 7
2013-04-15

Proof. The equality $\mathrm{Sel}^n(E/K) = H^1_{\mathcal{L}}(K, E(\overline{K})[n])$ follows from the fact that

$$\begin{aligned}
\mathrm{Sel}^n(E/K) &= \{c \in H^1(K, E(\overline{K})[n]) | i_{K_v} \circ \mathrm{res}_{K_v} c = 0\} \\
&= \{c \in H^1(K, E(\overline{K})[n]) | \mathrm{res}_{K_v} c \in \ker i_{K_v}\} \\
&= \{c \in H^1(K, E(\overline{K})[n]) | \mathrm{res}_{K_v} c \in \mathrm{Im}\, \delta_{K_v}\} \\
&= \{c \in H^1(K, E(\overline{K})[n]) | \mathrm{res}_{K_v} c \in \mathcal{L}_v\} \\
&= H^1_{\mathcal{L}}(K, E(\overline{K})[n])
\end{aligned}$$

To show that $\mathcal{L}$ is a Selmer system we only need to check that for $v \notin S$ for some finite set S one has $\mathcal{L}_v = H^1_{\mathrm{ur}}(K_v, E(\overline{K})[n])$. We will do this by showing that each group is contained in the other whenever $v \notin S$ where S is an explicit finite set of places. Define S to be the set of places consisting of infinite places, of finite places where E has bad reduction and finite places above n.

Let $v \notin S$. Consider $c \in \mathcal{L}_v$ with $c = \delta_{K_v}(P)$ for some $P \in E(K_v)$. Kummer theory gives that for any $Q \in E(\overline{K}_v)$ such that $[n]Q = P$ then $\delta_{K_v} P$ is the cochain $(\delta P)(g) = g(Q) - Q \in E(\overline{K}_v)[n]$. Suppose M/K_v is the smallest finite extension such that $Q \in E(M)$.

There exists a reduction map $E(M) \to E(k_M)$ as follows: if $x = (a : b : c) \in E(M)$ there exists $\lambda \in M^\times$ such that $\lambda a, \lambda b, \lambda c \in \mathcal{O}_M$ and at least one of them is in $\mathcal{O}_M^\times$. Then $\overline{x} = (\lambda a : \lambda b : \lambda c) \in E(k_M)$. The projection map $E(M) \to E(k_M)$ is Galois equivariant where the Galois group G_{M/K_v} acts on $E(k_M)$ via the projection to $G_{M/K_v}/I_{M/K_v} \cong G_{k_M/k_{K_v}}$.

Let $\overline{Q} \in E(k_M)$ be the reduction of Q. Let $\sigma \in I_{M/K_v}$. Then $\sigma(Q) - Q \in E(M)[n]$ because $[n](g(Q) - Q) = g(P) - P = 0$. Moreover, $\sigma(\overline{Q}) - \overline{Q} = 0$ as σ is trivial in G_{k_M/k_v}. But $E(M)[n]$ injects into $E(k_M)$ (E has good reduction at v and $v \nmid n$ as $v \notin S$) and so, since $\sigma(Q) - Q$ projects to $\sigma(\overline{Q}) - \overline{Q} = 0$, it follows that $\sigma(Q) = Q$. But then $Q \in E(M)^{I_{M/K_v}} = E(M \cap K_v^{\mathrm{ur}})$ and since M is the smallest extension of K_v such that $Q \in E(M)$ it follows that M/K_v is unramified and so $I_{K_v} = I_M$. Finally for $\sigma \in I_{K_v} = I_M \subset G_M$, $\sigma(Q) = Q$ and so $c(\sigma) = 0$ which implies that $c = \delta_v P \in H^1_{\mathrm{ur}}(K_v, E(\overline{K}_v)[n])$. Therefore $\mathcal{L}_v \subset H^1_{\mathrm{ur}}(K_v, E(\overline{K}_v)[n])$.

Reciprocally, suppose $c \in H^1_{\mathrm{ur}}(K_v, E(\overline{K}_v)[n])$. By definition $H^1_{\mathrm{ur}}(K_v, E(\overline{K}_v)[n]) \cong H^1(k_{K_v}, E(\overline{k}_{K_v})[n])$ which, by Lemma 4.6, stays in the exact sequence

$$0 \to E(k_{K_v})/nE(k_{K_v}) \to H^1(k_{K_v}, E(\overline{k}_{K_v})[n]) \to H^1(k_{K_v}, E(\overline{k}_{K_v}))[n] \to 0$$

But Proposition 4.4 implies that $H^1(k_{K_v}, E(\overline{k}_{K_v})) = 0$ and therefore $E(k_{K_v})/nE(k_{K_v}) \cong H^1(k_{K_v}, E(\overline{k}_{K_v})[n])$. Thus there exists $\overline{P} \in E(k_{K_v})$ such that $c = \delta\overline{P}$. Now Hensel's lemma allows one to find $P \in E(K_v)$ such that its image in $E(k_{K_v})$ is $\overline{P}$. Then $c = \delta P$ and so $H^1_{\mathrm{ur}}(K_v, E(\overline{K}_v)[n]) \subset \mathcal{L}_v$. □

4.5 Mordell-Weil

We are now ready to prove the Mordell-Weil Theorem

Proof of Theorem 4.2. Proposition prop:selmer elliptic shows that $\mathrm{Sel}^n(E/K) \cong H^1_{\mathcal{L}}(K, E(\overline{K})[n])$. We know that $E(\overline{K})[n]$ is finite and therefore Lemma 3.10 implies that $\mathrm{Sel}^n(E/K)$ is finite. We have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/nE(K) & \longrightarrow & H^1(K, E(\overline{K})[n]) & & \\ & & \downarrow & & \downarrow & \searrow & \\ 0 & \longrightarrow & E(K_v)/nE(K_v) & \longrightarrow & H^1(K_v, E(\overline{K}_v)[n]) & \longrightarrow & H^1(K_v, E(\overline{K}_v))[n] \end{array}$$

and therefore the image of $E(K)/nE(K)$ in $H^1(K_v, E(\overline{K}_v))[n]$ is trivial for every v. By definition, the image of $E(K)/nE(K)$ in $H^1(K, E(\overline{K})[n])$ is included in $\mathrm{Sel}^n(E/K)$ and therefore $E(K)/nE(K)$ is finite.

Now Lemma 4.5 implies that $E(K)$ is finitely generated. □

The following section was not covered in lecture

4.6 Standard proof of Mordell-Weil

I include here the proof from Silverman's book, for comparison.

Lemma 4.9. *Suppose E is an elliptic curve over a number field K and L/K is a finite Galois extension. If $E(L)/mE(L)$ is finite then $E(K)/mE(K)$ is finite.*

Proof. Consider the G_K-cohomology sequence attached to $1 \to E(\overline{K})[m] \to E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \to 1$:

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

which gives the Kummer isomorphism

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

Kummer and inflation restriction gives the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(L)/mE(L) & \longrightarrow & H^1(L, E(\overline{K})[m]) & \longrightarrow & H^1(L, E(\overline{K}))[m] \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(K, E(\overline{K})[m]) & \longrightarrow & H^1(K, E(\overline{K}))[m] \\ & & \uparrow & & \uparrow & & \uparrow \\ & & \ker & \longrightarrow & H^1(G_{L/K}, E(L)[m]) & \longrightarrow & H^1(G_{L/K}, E(L))[m] \\ & & \uparrow & & \uparrow & & \uparrow \\ & & 0 & & 0 & & 0 \end{array}$$

From the diagram it is clear that the map $\ker \to H^1(G_{L/K}, E(L)[m])$ is injective. We know that $E(L)[m]$ is finite and $G_{L/K}$ is a finite group and so ker injects into a finite group and thus it is finite. Now $E(K)/mE(K) \to E(L)/mE(L)$ is a map with finite kernel and image and so $E(K)/mE(K)$ is finite. □

We are not ready to prove Theorem 4.2.

Proof of Theorem 4.2. By Lemma 4.5 it suffices to show that $E(K)/mE(K)$ is finite. By Lemma 4.9 to show this we may replace K by any finite extension. In particular we may assume that $E(\overline{K})[m]) \subset E(K)$, which we may do since $E(\overline{K})[m]$ is finite. This implies that $E(\overline{K})[m] = E(K)[m]$ has trivial G_K-action and so $H^1(K, E(\overline{K})[m]) \cong \mathrm{Hom}(G_K, E(K)[m])$.

If $P \in E(\overline{K})$ let $K(P)$ be the finite extension of K generated by the coordinates of P. The Kummer sequence now implies that $E(K)/mE(K) \hookrightarrow \mathrm{Hom}(G_K, E(K)[m])$. This map is described explicitly as attaching to $P \in E(K)$ the map $\phi_P : G_K \to E(K)[m]$ given by $\phi_P(g) = g(Q) - Q$ for any $Q \in E(\overline{K})$ such that $[m]Q = P$. What is the kernel of ϕ_P? It is $K(Q)$ for the chosen Q with $[m]Q = P$. Let L be the compositum of all $K(Q)$ such that $[m]Q \in E(K)$. Thus ϕ_P vanishes on $G_L \subset G_K$.

Moreover, $E(K)/mE(K) \times G_{L/K} \to E(K)[m]$ defined by $(P, g) \mapsto \phi_P(g)$ is a perfect pairing. Since $E(K)[m]$ is finite to show that $E(K)/mE(K)$ is finite is is enough to show that L/K is a finite extension. First, note that $\phi_P(g^m) = m\phi_P(g) = 0$ and so $g^m = 1$ in $G_{L/K}$ and so L/K has exponent m.

Second, let S be a finite set of places containing the places where E has bad reduction, places v dividing m and the infinite places of K. We now show that L/K is unramified outside S. Since the compositum of unramified extensions is unramified it suffices to show that if $[m]Q \in E(K)$ then $K(Q)$ is unramified at $v \notin S$. We know that $E(K)[m] \hookrightarrow E(k_v)$ as $v \nmid m$ and E has good reduction at v. We need to show that I_{K_v} acts trivially on Q. Let $\sigma \in I_{K_v}$. Recall that $[m]Q = p \in E(K)$ and so $[m](\sigma(Q) - Q) = \sigma(P) - P = 0$. Therefore $\sigma(Q) - Q \in E(\overline{K})[m] = E(K)[m] \hookrightarrow E(k_v)$. But G_{K_v} acts on $E(k_v)$ via the projection $G_{k_v} \cong G_{K_v}/I_{K_v}$ and so $\sigma(Q) - Q = 0$ in $E(k_v)$. Therefore $\sigma(Q) = Q$ in $E(K)$ and so I_{K_v} acts trivially on $K(Q)$ as desired.

Finally, $K(Q)/\mathbb{Q}$ is an abelian extension because G_L appears as the kernel of the map $\phi_P : G_K \to E(K)[m]$ and $E(K)[m]$ is abelian. Therefore L/K is an abelian extension of exponent m which is unramified outside S. We want to show that L/K is finite. The inverse of the global Artin map gives an injection

$$G_{L/K} \hookrightarrow \mathbb{A}_K^\times / K^\times K_\infty^{\times,0} \prod_{v \in S - \infty} (K_v^\times)^m \prod_{v \notin S} \mathcal{O}_v^\times$$

and $\mathbb{A}_K^\times / K^\times K_\infty^{\times,0} \prod_{v \in S-\infty} (K_v^\times)^m \prod_{v \notin S} \mathcal{O}_v^\times \subset \prod_{v \in S - \infty} K_v^\times / (K_v^\times)^m$. This is so because $K^\times$ is dense in $\mathbb{A}_K^{\times,S}$ and so for every $(a_v) \in \mathbb{A}_K^\times$ there exists $x \in K^\times$ such that $a_v x^{-1} \in \mathcal{O}_v^\times$ when $v \notin S$ and $a_v x^{-1} \in K_v^{\times,0}$ when $v \mid \infty$.

Therefore it suffices to show that $K_v^\times / (K_v^\times)^m$ is finite. But by Kummer theory $K_v^\times / (K_v^\times)^m \cong H^1(K_v, \mu_m(\overline{K}_v))$ which is finite because $\mu_m(\overline{K}_v)$ is finite. □

End of section not covered in lecture

---

5 Characters with prescribed behavior

5.1 Grunwald-Wang

Let K be a number field. The Grunwald-Wang problem asks whether if $x \in K^\times$ is an n-th power in almost all $K_v^\times$ then x is also an n-th power in $K^\times$. Another way of putting this problem is to study the kernel of the map

$$K^\times / (K^\times)^n \to \prod_{v \notin S} K_v^\times / (K_v^\times)^n$$

where S is some finite set of places of K. Since $k^\times / (k^\times)^n = H^1(k, \mu_n)$ for any field k this kernel is

$$Ш_S^1(K, \mu_n) \cong \ker \left(H^1(K, \mu_n) \to \prod_{v \notin S} H^1(K_v, \mu_n) \right)$$

Lemma 5.1. *Let L/K be a Galois extension of number fields. If all but finitely many places v of K split completely in L then $L = K$.*

Proof. Suppose S is a finite set of places of K, containing the infinite places, such that if $v \notin S$ then $v = w_1 \cdots w_n$ splits completely in L. For each $v \in S - \infty$ and $w \mid v$ a place of L let $n_w \in \mathbb{Z}_{\geq 0}$ be an integer such that $\mathcal{U}_{K_v}^{n_w} \subset N_{L_w/K_v} L_w^\times$ which is an open subgroup of $K_v^\times$. Let $n_v = \max(n_w)$.

For each $a = (a_v) \in \mathbb{A}_K^\times$ one may find $x \in K^\times$ such that $a_v x^{-1} \in \mathcal{U}_{K_v}^{n_v}$ for all $v \in S - \infty$ and $a_v x^{-1} \in K_v^{\times,0}$ for $v \mid \infty$. Indeed, choosing $u \notin S$ strong approximation states that $K^\times$ is dense in $\mathbb{A}_K^{\{u\},\times}$. Therefore there exists $x \in K^\times$ whose image in $\mathbb{A}_K^{\{u\},\times}$ is in the open subset

$$\prod_{v|\infty} a_v K_\infty^{\times,0} \prod_{v \in S-\infty} a_v \mathcal{U}_{K_v}^{n_v} \prod_{v \notin S \cup \{u\}} \mathcal{O}_v^\times$$

Then if $v \mid \infty$ one has $a_v x^{-1} \in N_{L_w/K_v} L_w^\times = K_v^{\times,0}$, if $v \in S - \infty$ one has $a_v x^{-1} \in \mathcal{U}_{K_v}^{n_v} \subset N_{L_w/K_v} L_w^\times$ by choice of n_v and if $v \notin S$ and $w \mid v$ then $L_w = K_v$ so trivially $a_v x^{-1} \in N_{L_w/K_v} L_w^\times$. Therefore $ax^{-1} \in N_{L/K} \mathbb{A}_L^\times$ and so $a \in K^\times N_{L/K} \mathbb{A}_L^\times$. We deduce that

$$G_{L/K}^{\mathrm{ab}} \cong \mathbb{A}_K^\times / K^\times N_{L/K} \mathbb{A}_L^\times \cong 0$$

If L/K were abelian then $L = K$.

Suppose L/K is not abelian. Let $L/M/K$ be a subextension such that L/M is abelian and nontrivial. This is always possible as there exists a cyclic subgroup of $G_{L/K}$. Then let S_M be the set of places of M lying above places $v \in S$. Thus for every $w \notin S_M$, w splits completely in L. Since L/M is abelian it follows that $L = M$ contradicting the fact that L/M is nontrivial. Therefore $L = K$. □

Lecture 8
2013-04-17

Theorem 5.2 (Weak Grunwald-Wang)**.** *Let K be a number field and $t = v_2(n)$.*

1. *If $K(\zeta_{2^t})/K$ is a cyclic extension then $Ш_S^1(K, \mu_n) = 1$. In particular this is so when $8 \nmid n$.*
2. *If $K(\zeta_{2^t})/K$ is not cyclic then $Ш_S^1(K, \mu_n)$ is a finite 2-torsion group, i.e., if $\alpha \in Ш_S^1(K, \mu_n)$ then $\alpha \in (K^\times)^{n/2}$.*

Proof. If $(m, n) = 1$ and $\alpha = a^m = b^n$ then for $pm + qn = 1$ one obtains $\alpha = (a^q b^p)^{mn}$. Therefore it is enough to show the result when $n = p^r$ for a prime p.

If $\zeta_n \in K$ and $\alpha \in Ш_S^1(K, \mu_n)$ then $K(\sqrt[n]{\alpha})/K$ is a Galois extension. For every $v \notin S$ one knows that $\sqrt[n]{\alpha} \in K_v$ and therefore the prime v of K splits completely in $K(\sqrt[n]{\alpha})$. Lemma 5.1 now shows that $K(\sqrt[n]{\alpha}) = K$ and therefore $\alpha = 1$ in $Ш_S^1(K, \mu_n)$.

If $\zeta_n \notin K$ consider $K(\zeta_n)$. The above shows that $\alpha = \beta^n$ for some $\beta \in K(\zeta_n)$. Let $X^n - \alpha = \prod f_i(X)$ the factorization into irreducibles over K. Over $K(\zeta_n)$ we know that $X^n - \alpha = \prod (X - \beta\zeta_n^i)$ and therefore $f_i(X)$ has a root of the form $\beta_i = \beta\zeta_n^j \in K(\zeta_n)$. The extension $K(\beta_i)/K$ is therefore abelian Galois.

For $v \notin S$ let $\alpha = \alpha_v^n$ for $\alpha_v \in K_v$ in which case $\prod f_i(\alpha_v) = 0$ and so $f_i(\alpha_v) = 0$ for some i. Since $K(\beta_i)/K$ is abelian the Galois group acts transitively on the roots of f_i and so f_i splits completely in K_v and so v splits completely in $K(\beta_i)$. If $K(\zeta_n)/K$ is cyclic of prime power degree then its subfields are ordered linearly and we may assume that $K(\beta_1) \subset K(\beta_2) \subset \ldots$. Since v splits completely in some $K(\beta_i)$ it must also split completely in $K(\beta_1)$ and so $K(\beta_1) = K$ by Lemma 5.1. Finally, $\alpha = \beta_1^n$ for $\beta_1 \in K$.

If $n = p^r$ with $p > 2$ then $K(\zeta_n)/K$ is cyclic of degree p^r. If $n = 2^r$ and $K(\zeta_{2^t})/K$ is assumed cyclic then $Ш_S^1(K, \mu_n) = 1$.

If $K(\zeta_{2^t})/K$ is not cyclic then $K(\sqrt{-1}) \neq K$ as $K(\zeta_{2^t})/K(\sqrt{-1})$ is cyclic. Therefore $\alpha \in (K(\sqrt{-1})^\times)^n$. Let $\beta \in K(\sqrt{-1})$ such that $\alpha = \beta^n$ in which case taking norms one gets $\alpha^2 = (N_{K(\sqrt{-1})/K}\beta)^n$ and the conclusion follows. □

The following section was not covered in lecture

I include, without proof, the full Grunwald-Wang theorem.

Theorem 5.3 (Strong Grunwald-Wang)**.** *For $r \geq 1$ let $\eta_r = \zeta_r + \zeta_r^{-1}$. Let K be a number field and S a finite set of places of K. Let r be the largest integer such that $\eta_r \in K$. Then $Ш^1_S(K, \mu_n) = 1$ unless:*

1. *-1, $2+\eta_r$ and $-(2+\eta_r)$ are non-squares in K and*
2. *$v_2(n) > r$ and*
3. *S contains the set S_K of all the places $v \mid 2$ such that -1, $2+\eta_r$ and $-(2+\eta_r)$ are non-squares in K_v.*

End of section not covered in lecture

5.2 Characters with prescribed finite order local behavior

Let K be a number field and S a finite set of places of K.

Lemma 5.4. *For every finite index open subgroup P_0 of $P = \prod_{v \in S} K_v^\times$ there exists an open subgroup U of $\mathbb{A}_K^\times / K^\times$ such that $U \cap P = P_0$.*

Proof. This proof has some missing topological details. See [AT09, Chapter 10, Lemma 4]. Let $C_K = \mathbb{A}_K^\times / K^\times$. First, for $n > 1$, $P_0 C_K^n$ and $P C_K^n$ are closed subgroups of C_K and $P_0 C_K^n$ is open in $P C_K^n$. Therefore there exists $V \subset C_K$ open such that $P C_K^n \cap V \subset P_0 C_K^n$. Let $U = V P_0 C_K^n$. Then $P \cap U = P \cap P C_K^n \cap P_0 C_K^n V = P \cap P_0 C_K^n (P C_K^n \cap V) = P \cap P_0 C_K^n = P_0 (P \cap C_K^n)$.

Now P_0 is finite index in P and so for some integer n one has $P^n \subset P_0$ in which case we take the open U of C_K such that $P \cap U = P_0(P \cap C_K^{2n})$. Now suppose $\alpha \in P \cap C_K^{2n}$. Then there exists $(\alpha_v) \in P \subset \mathbb{A}_K^\times$ and $x \in K^\times$ such that $(\alpha_v)x \in (\mathbb{A}_K^\times)^{2n}$. Since $\alpha_v = 1$ if $v \notin S$ it follows that $x \in (K_v^\times)^{2n}$ for $v \notin S$. Now Theorem 5.2 implies that $x \in (K^\times)^n$ and so $(\alpha_v) \in (\mathbb{A}_K^\times)^n$ so $(\alpha_v) \in P^n$. Thus $P \cap C_K^{2n} \subset P^n$ and therefore $P \cap U = P_0(P \cap C_K^{2n}) = P_0$ as desired. □

Theorem 5.5. *Let K be a number field and S a finite set of (not necessarily finite) places. For each $v \in S$ let $\chi_v : K_v^\times \to \mathbb{C}^\times$ be a continuous character of finite order n_v. Then there exists a continuous finite order character $\chi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times$ such that $\chi|_{K_v^\times} = \chi_v$ when $v \in S$.*

Proof. Let $P = \prod_{v \in S} K_v^\times$. Have a character $\otimes_{v \in S} \chi_v : P \to \mathbb{C}^\times$ and let $P_0 = \ker \otimes \chi_v$ be a finite index subgroup of P. Lemma 5.4 provides an open subgroup U of $\mathbb{A}_K^\times$ such that $P \cap U = P_0$. But then $PU/U \cong P/P \cap U \cong P/P_0$ and therefore the character $\chi_S = \otimes_{v \in S} \chi_v : P/P_0 \to S^1$ extends to a character $\chi_S : PU/U \to S^1$. Finally, $PU \subset C_K$ is finite index and so χ_S extends to a character $\chi_S : \mathbb{A}_K^\times / K^\times U \to S^1$ which is a global finite order Hecke character. □

5.3 Characters with prescribed local behavior at infinite places

Write $|\cdot|$ for the usual absolute value on $\mathbb{C}^\times$ and $|\cdot|_{\mathbb{C}}$ for its square.

Lemma 5.6. *Continuous characters of $\mathbb{R}^\times$ are of the form $x \mapsto \operatorname{sign}(x)^\varepsilon |x|^t$ for $\varepsilon \in \{0, 1\}$ and $t_v \in \mathbb{C}$. Continuous characters of $\mathbb{C}^\times$ are of the form $x \mapsto (x/|x|)^m |x|_{\mathbb{C}}^t$ for some $m \in \mathbb{Z}$ and $t \in \mathbb{C}$.*

Proof. All continuous homomorphisms from $\mathbb{R}$ to $\mathbb{C}$ are obtained by scalar multiplication and so all continuous homomorphisms from $(0, \infty)$ to $\mathbb{C}^\times$ are of the form $x \mapsto x^t$ for $t \in \mathbb{C}$. The result then follows from the fact that $\mathbb{R}^\times \cong \{-1, 1\} \times (0, \infty)$ and $\mathbb{C}^\times \cong S^1 \times (0, \infty)$. □

Definition 5.7. A Hecke character $\psi : \mathbb{A}_K^\times / K^\times$ is unitary if for each $v \mid \infty$ one has $\psi_v(x) = (x/|x|)^{m_v} |x|_v^{it_v}$ where $t_v \in \mathbb{R}$. The character ψ is said to be algebraic of type A_0 if $t_v = 0$ for all $v \mid \infty$. The character ψ is algebraic of type A if

Proposition 5.8. *Let K be a number field and for each $v \mid \infty$ let $m_v \in \mathbb{Z}$ (0 or 1 if $v \mid \mathbb{R}$) and $t_v \in \mathbb{R}$. There exists a Hecke character $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$ such that for $v \mid \infty$, $\chi_v(x) = (x/|x|_v)^{m_v} |x|_{\mathbb{C}}^{it_v}$ if and only if*

$$\prod_{v|\infty} \left(\frac{\iota_v(\alpha)}{|\iota_v(\alpha)|_v} \right)^{m_v} |\iota_v(\alpha)|_{\mathbb{C}}^{it_v} = 1$$

for α in a finite index subgroup of $\mathcal{O}_K^\times$.

Proof. If χ is a global Hecke character let U be the finite index open subgroup of $\prod_{v \nmid \infty} \mathcal{O}_v^\times$ such that $\chi|_U = 1$, i.e., U is the conductor of χ. Then for every $\alpha \in \mathcal{O}_K^\times \cap U$ one has $\prod_{v \nmid \infty} \chi_v(\alpha) = 1$ and therefore since $\prod_v \chi_v(\alpha) = 1$ one also has $\prod_{v|\infty} \chi_v(\alpha) = 1$.

Reciprocally, let $V \subset \mathcal{O}_K^\times$ be a finite index subgroup. There exists a finite index subgroup $U \subset \prod_{v \nmid \infty} \mathcal{O}_v^\times$ such that $V \supset \mathcal{O}_K^\times \cap U$. There is an exact sequence

$$1 \to K_\infty^\times U / (\mathcal{O}_K^\times \cap U) \to \mathbb{A}_K^\times / K^\times \to \mathrm{Cl}(U) \to 1$$

where $\mathrm{Cl}(U)$ is a finite group.

Define χ on $K_\infty U$ by letting χ_v as required when $v \mid \infty$ and $\chi_v = 1$ when $v \nmid \infty$. The hypothesis implies that χ factors through $K_\infty^\times U / (\mathcal{O}_K^\times \cap U)$. Choosing a section to the exact sequence above, since $\mathrm{Cl}(U)$ is finite, one may extend to a Hecke character χ. (Such a section exists because to an ideal $I \in \mathrm{Cl}(U)$ one may attach $\prod_{v \nmid \infty} \varpi_v^{v(I)}$ which is a homomorphism.) □

Lecture 9
2013-04-19

Lemma 5.9. *Let K be a number field. A continuous Hecke character has finite order if and only if it is trivial on $K_\infty^{\times,0}$.*

Proof. If $v \mid \infty$ then $\phi_v(x) = (x/|x|)^m |x|_{\mathbb{C}}^t$ for $m \in \mathbb{Z}$ and $t \in \mathbb{C}$. If $v = \mathbb{R}$ then on $K_v^{\times,0} = (0, \infty)$ this is $\phi_v(x) = |x|_{\mathbb{C}}^t$ and if this is finite order then $t = 0$ and so $\phi_v|_{K_v^{\times,0}} = 1$. If $v = \mathbb{C}$ then on $K_v^{\times,0} = \mathbb{C}^\times$ this is $\phi_v(re^{i\theta}) = e^{im\theta} r^t$. If ϕ_v is finite order then necessarily $t = 0$ and, since for θ irrational the set $\{m\theta \bmod 2\pi\} \subset [0, 2\pi)$ is dense, also $m = 0$ which gives again $\phi_v|_{K_v^{\times,0}} = 1$.

Reciprocally, suppose $\phi|_{K_\infty^{\times,0}} = 0$. Since ϕ is continuous there exists an open subgroup $U \subset \mathbb{A}_K^{f,\times}$ such that $U \subset \ker \phi$. But then ϕ factors through $\mathbb{A}_K^\times / K^\times K_\infty^{\times,0} U$ which is finite, thereby showing that ϕ has finite order. □

Theorem 5.10 (Weil-Artin)**.** *Let K be a number field and $K_{\mathrm{CM}} \subset K$ be the maximal CM subfield (where $K_{\mathrm{CM}} = \mathbb{Q}$ if K has no CM subfields). Let $\psi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$ be an algebraic Hecke character of type A_0. Then there exists an algebraic Hecke character ψ_{CM} of K_{CM} of type A_0 and a finite order character χ of K such that $\psi = \chi \cdot \psi_{\mathrm{CM}} \circ N_{K/K_{\mathrm{CM}}}$. In particular every algebraic Hecke character of type A of a totally real field is the product of a finite order character and $|\cdot|_{\mathbb{A}_K}^m$ for some integer m.*

Proof. By Lemma 5.9 a continuous Hecke character has finite order if and only if it is trivial on $K_\infty^{\times,0}$. Therefore it suffices to show that ψ and $\psi_{\mathrm{CM}} \circ N_{K/K_{\mathrm{CM}}}$ agree on $K_\infty^\times$ for some algebraic character ψ_{CM}.

First, assume $K/\mathbb{Q}$ is Galois with Galois group G. Since $G = G_{K/\mathbb{Q}}$ acts transitively on places of K above a place of $\mathbb{Q}$, the infinite places of K are either all real or all complex.

Suppose that K is totally real. Then for $v \mid \infty$, $\psi_v(x) = (x/|x|)^{m_v} = (\operatorname{sign} x)^{m_v}$ which is trivial on $K_v^{\times,0}$ and so ψ readily has finite order and the theorem follows.

Suppose that K is totally complex. The character ψ is algebraic of type A_0 and so for an infinite place v, $\psi_v(x) = (x/|x|)^{m_v}$ and Proposition 5.8 implies the existence of an open subgroup U of $\mathcal{O}_K^\times$ such that for

$\alpha \in U$ one has $\prod_{v|\infty}(\iota_v(\alpha)/|\iota_v(\alpha)|)^{m_v} = 1$. Squaring we get

$$\prod_{v|\infty}\left(\frac{\iota_v(\alpha)}{|\iota_v(\alpha)|}\right)^{2m_v} = \prod_{v|\infty}\left(\frac{\iota_v(\alpha)}{\overline{\iota_v(\alpha)}}\right)^{m_v}$$
$$= 1$$

Fixing an embedding $\tau : K \hookrightarrow \mathbb{C}$, we have $\{\iota_v, \overline{\iota_v}\} = \{\tau \circ g | g \in G\}$ and for $g \in G$ we write $m_g = m_{\tau\circ g}$ if $\tau \circ g = \iota_v$ and $m_g = -m_{\tau\circ g}$ if $\tau \circ g = \overline{\iota_v}$. Then the equation above becomes

$$\prod_{g\in G} \tau \circ g(\alpha)^{m_g} = 1$$

and since τ is injective

$$\prod_{g\in G} g(\alpha)^{m_g} = 1$$

For any complex embedding $\iota : K \hookrightarrow \mathbb{C}$ let c_ι be the (necessarily nontrivial) element of G induced by complex conjugation on $\mathbb{C}$, i.e., $\overline{\iota(x)} = \iota(c_\iota(x))$. Suppose $\iota_v = \tau \circ g$. Then $\overline{\iota_v} = \iota_v \circ c_{\iota_v} = \tau \circ (c_{\iota_v} g)$ and so by definition $m_{c_{\iota_v} g} = -m_g$.

The field K_{CM} is the fixed field of $\{c_\iota c_{\iota'} | \iota, \iota' : K \hookrightarrow \mathbb{C}\}$. The equation above becomes

$$\prod_{G/c_\iota} g(\alpha)^{m_g} c_\iota g(\alpha)^{m_{c_\iota g}} = 1$$

for $\alpha \in U \subset \mathcal{O}_K^\times$.

Note that $|\iota(g(\alpha))|_{\mathbb{C}} = |\iota(c_\iota g(\alpha))|_{\mathbb{C}}$ so taking logarithms get

$$\sum_{G/c_\iota} (m_g + m_{c_\iota g}) \log |\iota(g(\alpha))|_{\mathbb{C}} = 0$$

Theorem 2.1 implies that $\mathcal{O}_K^\times$ and therefore the finite index subgroup U of $\mathcal{O}_K^\times$ have rank $\#\infty - 1 = |G|/2 - 1$ which is also the rank of $\Delta_\infty = \ker\left(\mathbb{R}^{\#\infty} \to \mathbb{R}\right)$ and so $w_\iota = m_g + m_{c_\iota g}$ is independent of g. But $w_\iota |G|/2 = \sum_{g\in G/c_\iota}(m_g + m_{c_\iota g}) = \sum_{g\in G} m_g$ is also independent of ι and so w_ι is independent of ι. Therefore for any other $\iota' : K \hookrightarrow \mathbb{C}$ one has $m_{c_\iota g} + m_{c'_\iota c_\iota g} = w_{\iota'} = w_\iota = m_g + m_{c_\iota g}$ and so $m_g = m_{c'_\iota c_\iota g}$. Thus m_g is constant on $G_{K/K_{\mathrm{CM}}}$-orbits and so

$$\prod_{g\in G} g(\alpha)^{m_g} = \prod_{g\in G_{K_{\mathrm{CM}}/\mathbb{Q}}} g(N_{K/K_{\mathrm{CM}}}\alpha)^{m_g} = 1$$

and if α ranges over a finite index subgroup of $\mathcal{O}_K^\times$ then $N_{K/K_{\mathrm{CM}}}\alpha$ ranges over a finite index subgroup U' of $\mathcal{O}_{K_{\mathrm{CM}}}^\times$. What we get is that for $\alpha \in U' \subset \mathcal{O}_{K_{\mathrm{CM}}}^\times$ have

$$\prod_{g\in G_{K_{\mathrm{CM}}/\mathbb{Q}}} g(\alpha)^{m_g} = 1$$

and $m_{c_\iota g} = -m_g$ from the fact that over K have $m_{c_{\iota_v} g} = -m_g$. Suppose $\tau : K_{\mathrm{CM}} \hookrightarrow \mathbb{C}$ is a complex embedding. Then writing c for the unique complex conjugation on K_{CM} we have

$$\prod_{g\in G_{K_{\mathrm{CM}}/\mathbb{Q}}/c}\left(\frac{\tau(g(\alpha))}{\overline{\tau(g(\alpha))}}\right)^{m_g} = \prod_{g\in G_{K_{\mathrm{CM}}/\mathbb{Q}}/c}\left(\frac{\tau(g(\alpha))}{|\tau(g(\alpha))|}\right)^{2m_g} = 1$$

and by restricting the finite index subgroup U' a little more we conclude by Proposition 5.8 the existence of an algebraic Hecke character ψ_{CM} of K_{CM} such that at $v \mid \infty$ in K_{CM}, $\psi_{\mathrm{CM},v}(x) = (x/|x|)^{m_v}$ where $m_v = m_g$ if $\iota_v = \tau \circ g$. In that case $\psi \cdot \psi_{\mathrm{CM}} \circ N_{K/K_{\mathrm{CM}}}^{-1}$ is trivial on $K_\infty^\times$ and so has finite order.

Now if $K/\mathbb{Q}$ is not Galois let L/K be its Galois closure and L_{CM} the maximal CM subfield of L. Let $H_1 = G_{L/K}$ and $H_2 = G_{L/L_{\mathrm{CM}}}$. By definition $K \cap L_{\mathrm{CM}} = K_{\mathrm{CM}}$ and so $G_{L/K_{\mathrm{CM}}} = H_1 H_2$. Now $\psi \circ N_{L/K}$ is a character on L which is Galois over $\mathbb{Q}$ and so $\psi \circ N_{L/K} = \chi \cdot \eta \circ N_{L/L_{\mathrm{CM}}}$ where η is an algebraic character of L_{CM}. As before we need to show that the integers $\{m_v\}$ where $v \mid \infty$ runs over places of L are constant on orbits of $G_{L/K_{\mathrm{CM}}} = H_1 H_2$. But the integers are constant along H_1-orbits since they are attached to $\psi \circ N_{L/K}$ and they are constant along H_2 orbits because $\psi \circ N_{L/K} = \chi \cdot \eta \circ N_{L/L_{\mathrm{CM}}}$. □

Lecture 10
2013-04-22

Proposition 5.11. *Let $n > 1$ be an integer not divisible by 8 and $\omega : \mu_n(K)\backslash\mu_n(\mathbb{A}_K) \to S^1$ be a continuous character such that $\omega_v = 1$ for $v \mid \mathbb{C}$. Then there exists a finite order character $\widetilde{\omega} : K^\times\backslash\mathbb{A}_K^\times \to S^1$ whose restriction to $\mu_n(\mathbb{A}_K)$ is ω. Here $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$.*

Proof. We have an exact sequence

$$\mu_n(K)\backslash\mu_n(\mathbb{A}_K) \to (\mathbb{A}_K^\times/K^\times)[n] \to Ш^1_\emptyset(K, \mu_n) \to 1$$

as follows: if $(\alpha_v) \in C_K[n]$ then $(\alpha_v^n) = x$ for some $x \in K^\times$. Let y be the image of x in $Ш^1_\emptyset(K, \mu_n)$. What is the kernel of this map? If $y = 1$ then $x \in (K^\times)^n$. But $(\alpha_v)x^{-1} = (\alpha_v)$ in C_K and $\alpha_v x^{-1} \in \mu_n(K_v)$ and so $(\alpha_v)x^{-1} \in \mu_n(\mathbb{A}_K)$. By Theorem 5.2 since $8 \nmid n$, $Ш^1_\emptyset(K, \mu_n) = 1$ and so ω is a character of $C_K[n] \to S^1$.

For an abelian topological group G denote by $G^\vee = \mathrm{Hom}(G, S^1)$ the Pontryagin dual consisting of continuous homomorphisms. Then $(G/H)^\vee \cong H^\perp$, where $H^\perp = \{\phi \in G^\vee \mid \phi(H) = 1\}$, and $G^{\vee\vee} \cong G$. Thus $(C_K^\vee/nC_K^\vee)^\vee \cong (nC_K^\vee)^\perp \cong \{x \in C_K \mid \phi(x^n) = 1, \forall \phi \in C_K^\vee\} = C_K[n]$. By duality get $C_K[n]^\vee \cong C_K^\vee/nC_K^\vee$ and so we get an extension $\widetilde{\omega} : C_K \to S^1$ which is well-defined up to n-th power characters. We only need to show that the lift can be chosen to have finite order.

Theorem 5.10 implies that there exists an algebraic character η of K_{CM} such that $\widetilde{\omega}$ and $\eta \circ N_{K/K_{\mathrm{CM}}}$ differ by a finite order character. Thus it suffices to show that η can be chosen to have finite order, i.e., to be trivial on $K_{\mathrm{CM},\infty}^\times$. But we know that at $v \mid \mathbb{C}$, $\omega_v = 1$ on μ_n and so $n \mid m_v$ which implies that $n \mid m_{\eta_v}$ for every (necessarily complex) place of K_{CM}. Proposition 5.8 implies that there exists a Hecke character μ of K_{CM} such that $\mu_v(x) = (x/|x|)^{m_{\eta_v}/n}$ (the condition of Proposition 5.8 is automatically satisfied because it is satisfied for η) and in that case $\eta\mu^{-n}$ is finite order and thus $\widetilde{\omega}(\mu \circ N_{K/K_{\mathrm{CM}}})^{-n}$ is finite order with the same restriction to $\mu_n(\mathbb{A}_K)$ as $\widetilde{\omega}$. □

6 Projective Galois representations

6.1 A theorem of Tate

The setup of the first lemma is that $K/\mathbb{Q}_\ell$ is a finite extension such that $\mu_p(\overline{K}) \subset K$ and we may choose $\zeta_p \in \mu_p(K)$ a primitive root of unity. Then the G_K-cohomology sequence of $1 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p} \mathbb{Q}_p/\mathbb{Z}_p$ gives

$$H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p} H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\delta} H^2(K, \mathbb{Z}/p\mathbb{Z})$$

where $H^2(K, \mathbb{Z}/p\mathbb{Z}) \cong H^2(K, \mu_p(K)) = H^2(K, \overline{K}^\times)[p] \cong \mathrm{Br}(K)[p] \xrightarrow{\cong} \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ where the first isomorphism is via the identification of G_K-modules $\mathbb{Z}/p\mathbb{Z} \cong \mu_p(K)$ via $x \mapsto \zeta_p^x$ and the last map is the invariant map inv_K. The local Artin map $r_K : K^\times \cong W_K^{\mathrm{ab}} \subset G_K^{\mathrm{ab}}$ permits the identification of continuous homomorphisms $\phi : G_K \to \mathbb{Q}_p/\mathbb{Z}_p$ with continuous homomorphisms $\phi \circ r_K : K^\times \to \mathbb{Q}_p/\mathbb{Z}_p$.

Lemma 6.1. *Let $K/\mathbb{Q}_\ell$ be as above.*

1. *If $\phi \in H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}(G_K, \mathbb{Q}_p/\mathbb{Z}_p)$ then $\delta(\phi)$ only depends on $(\phi \circ r_K)|_{\mu_p(\overline{K})}$. In fact there exists $a \in \mathbb{Z}/p\mathbb{Z}$, independent of ϕ, such that $\mathrm{inv}_K(\delta(\phi)) = a\phi(r_K(\zeta_p))$.*

2. *The connecting homomorphism δ is an isomorphism, i.e., $a \neq 0$.*

3. *The constant a is independent of $K/\mathbb{Q}_\ell$.*

4. *If F is a number field such that $\zeta_p \in F$ and u_1 and u_2 are two finite places of F then $a_{F_{u_1}} = a_{F_{u_2}}$.*

Proof. Note that $H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p} H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\delta} H^2(K, \mathbb{Z}/p\mathbb{Z})$ is exact and so factors through

$$0 \to H^1(K, \mathbb{Q}_p/\mathbb{Z}_p)/pH^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\delta} H^2(K, \mathbb{Z}/p\mathbb{Z})$$

But $H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}(G_K, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p)$. The sequence $1 \to \mu_p(K) \to K^\times \xrightarrow{p} K^\times$ is exact and so $\mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Hom}(\mu_p, \mathbb{Q}_p/\mathbb{Z}_p)$ is exact which means that $H^1(K, \mathbb{Q}_p/\mathbb{Z}_p)/pH^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \hookrightarrow \mathrm{Hom}(\mu_p, \mathbb{Q}_p/\mathbb{Z}_p)$. Therefore $\delta(\phi)$ only depends on the restriction $\delta \circ r_K|_{\mu_p(K)}$.

Since $\mu_p \subset K$ it follows that $\mu_{p^n} \subset K^\times$ for a maximal $n > 0$. Let $\phi : K^\times \to \mathbb{Q}_p/\mathbb{Z}_p$ such that $\phi(\zeta_{p^n}) = p^{-n}$; such a ϕ exists by the decomposition $K^\times \cong \varpi_K^{\mathbb{Z}} \times \mu_\infty(K) \times (\mathcal{O}_K^\times)^{\mathrm{TF}}$ where TF stands for torsion free. If there exists $\psi : K^\times \to \mathbb{Q}_p/\mathbb{Z}_p$ such that $\phi = p\psi$ then $p\psi(\zeta_{p^n}) = p^{-n}$ and so $\psi(\zeta_{p^n}) = \frac{a}{p^{n+1}}$ for $a \in \mathbb{Z}_p^\times$. But then $p^n\psi(\zeta_{p^n}) = \frac{a}{p} \neq 0$ in $\mathbb{Q}_p/\mathbb{Z}_p$ whereas $p^n\psi(\zeta_{p^n}) = \psi(1) = 0$. We conclude that $\mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p) \neq p\,\mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p)$ and so $0 \neq \mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p)/p\,\mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p) \hookrightarrow \mathrm{Hom}(\mu_p, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}/p\mathbb{Z}$ and so $\mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p)/p\,\mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}/p\mathbb{Z}$.

Then $\mathrm{inv}_K \circ \delta$ is a homomorphism $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ and it follows that there exists $a \in \mathbb{Z}/p\mathbb{Z}$ such that $\mathrm{inv}_K(\delta(\phi)) = a\phi(r_k(\zeta_p))$ for all ϕ.

To check that δ is an isomorphism simply note that δ injects $\mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p)/p\,\mathrm{Hom}(K^\times, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}/p\mathbb{Z} \hookrightarrow H^2(K, \mu_p)$ and so δ is injective which implies that $a \neq 0$ and so δ is an isomorphism.

Let L/K be a finite extension. Under $\mu_p \subset K^\times \subset L^\times$, $r_L(\zeta_p) = \mathrm{cor}^\vee \circ r_K(\zeta_p)$ and for $\phi : L^\times \to \mathbb{Q}_p/\mathbb{Z}_p$ one has

$$\begin{aligned}
\mathrm{inv}_K(\delta_K(\mathrm{cor}\,\phi)) &= a_K \,\mathrm{cor}\,\phi(r_K(\zeta_p)) \\
\mathrm{inv}_L(\delta_L(\phi)) &= a_L\phi(r_L(\zeta_p)) \\
&= a_L\phi(\mathrm{cor}^\vee\, r_K(\zeta_p)) \\
&= a_L \,\mathrm{cor}\,\phi(r_K(\zeta_p))
\end{aligned}$$

But $\mathrm{inv}_K(\delta_K(\mathrm{cor}\,\phi)) = \mathrm{inv}_L(\delta_L(\phi))$ and so $a_K = a_L$.

Consider the number field $K = \mathbb{Q}(\zeta_p)$. It suffices to show that if u_1 and u_2 are finite places of K then $a_{K_{u_1}} = a_{K_{u_2}}$. Let $\phi \in \mathrm{Hom}(G_K, \mathbb{Q}_p/\mathbb{Z}_p) \cong H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\delta} H^2(K, \mu_p) \cong H^2(K, \overline{K}^\times)[p] \cong \mathrm{Br}(K)[p]$. Then $\sum_v \mathrm{inv}_v\,\delta(\phi) = 0$ because $0 \to \mathrm{Br}(K) \to \oplus\,\mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0$. Therefore $\sum a_{K_v}\phi(r_{K_v}(\zeta_p)) = 0$. Since $r_K : \mathbb{A}_K^\times \to G_K^{\mathrm{ab}}$ is trivial on $K^\times$ it follows that $\phi(r_K(\zeta_p)) = \sum_v \phi(r_{K_v}(\zeta_p)) = 0$. Suppose one may choose ϕ such that $\phi(r_{K_v}(\zeta_p))$ is nonzero at exactly u_1 and u_2. Then the equations $\phi(r_{K_{u_1}}(\zeta_p)) + \phi(r_{K_{u_2}}(\zeta_p)) = 0$ and $a_{K_{u_1}}\phi(r_{K_{u_1}}(\zeta_p)) + a_{K_{u_2}}\phi(r_{K_{u_2}}(\zeta_p)) = 0$ give $a_{K_{u_1}} = a_{K_{u_2}}$ as desired.

We now show the existence of such a global character ϕ. Let $\eta : \mu_p \to \mathbb{Z}/p\mathbb{Z}$ be a nontrivial character. Since for v finite have $\mathrm{Hom}(K_v^\times, \mathbb{Q}_p/\mathbb{Z}_p)/p\,\mathrm{Hom}(K_v^\times, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}(\mu_p(K_v), \mathbb{Q}_p/\mathbb{Z}_p)$ one may extend η to a character $\eta : K_v^\times \to \mathbb{Q}_p/\mathbb{Z}_p$ and be restriction get a character $\eta : K^\times \to \mathbb{Q}_p/\mathbb{Z}_p$. Now $K^\times \subset K_v^\times$ is dense and so there exist $\phi_{u_i} : K_{u_i}^\times \to \mathbb{Z}/p\mathbb{Z}$ such that $\phi_{u_1}|_{K^\times} = \eta$ and $\phi_{u_2}|_{K^\times} = \eta^{-1}$. Let $S = \{u_1, u_2\}$. Recall that $G_{\overline{K}/K_S}$ is generated by the inertia groups $I_{K_{u_1}}$ and $I_{K_{u_2}}$ and so $G_{K,S}^{\mathrm{ab}} \cong \mathbb{A}_K^\times/K^\times K_\infty^\times \prod_{v \notin S} \mathcal{O}_{K_v}^\times$. Consider the exact sequence

$$1 \to \mathcal{O}_{K_{u_1}}^\times \mathcal{O}_{K_{u_2}}^\times / K^\times \cap \mathcal{O}_{K_{u_1}}^\times \mathcal{O}_{K_{u_2}}^\times \to G_{K,S}^{\mathrm{ab}} \to \mathrm{Cl}(K) \to 1$$

The character $\phi = \phi_{u_1} \otimes \phi_{u_2}$ on $\mathcal{O}_{K_{u_1}}^\times \mathcal{O}_{K_{u_2}}^\times$ will then be trivial on $K^\times \cap \mathcal{O}_{K_{u_1}}^\times \mathcal{O}_{K_{u_2}}^\times$ and, since the cokernel $\mathrm{Cl}(K)$ is finite, will extend to a character of $G_{K,S}^{\mathrm{ab}}$. Let's check that ϕ satisfies the requirements. For $v \neq u_1, u_2$, $r_{K_v}(\zeta_p) \in I_{K_v}$ and so $\phi(r_{K_v}(\zeta_p)) \in \phi(I_{K_v}) = 0$. If $v \in S$ then $\phi(r_{K_v}(\zeta_p)) = \eta^{\pm 1}(\zeta_p) \neq 0$. $\square$

Theorem 6.2. *Let K be a number field. Then $H^2(K, \mathbb{Q}/\mathbb{Z}) = 0$.*

Proof. Since $\mathbb{Q}/\mathbb{Z} = \oplus \mathbb{Q}_p/\mathbb{Z}_p$ it is enough to show that $H^2(K, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Inflation-restriction gives

$$1 \to H^2(G_{K(\mu_p)/K}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(K, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(K(\mu_p), \mathbb{Q}_p/\mathbb{Z}_p)$$

Since $G_{K(\mu_p)/K} \subset (\mathbb{Z}/p\mathbb{Z})^\times$ and $\mathbb{Q}_p/\mathbb{Z}_p$ is pro-p it follows that $H^2(G_{K(\mu_p)/K}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Therefore to show that $H^2(K, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ it is enough to do the same for $K(\mu_p)$. We now assume that $\mu_p \subset K$.

Consider the exact sequence

$$H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\delta} H^2(K, \mathbb{Z}/p\mathbb{Z}) \to H^2(K, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p} H^2(K, \mathbb{Q}_p/\mathbb{Z}_p)$$

The group $H^2(K, \mathbb{Q}_p/\mathbb{Z}_p)$ is p-power torsion so to show it is trivial it is enough to show that multiplication by p is injective, i.e., the connecting homomorphism δ is surjective. Note that $H^2(K, \mathbb{Z}/p\mathbb{Z}) \cong H^2(K, \mu_p) = H^2(K, \overline{K}^\times)[p] \cong \mathrm{Br}(K)[p]$ so we need to show that $H^1(K, \mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Br}(K)[p]$ is surjective.

In other words we need to show that for every torsion Brauer class $\alpha \in \mathrm{Br}(K)[p]$ there exists a $\phi : G_K^{\mathrm{ab}} \to \mathbb{Q}_p/\mathbb{Z}_p$ such that $\delta\phi = \alpha$. We know that $0 \to \mathrm{Br}(K) \to \oplus \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0$ and so $\alpha \in \mathrm{Br}(K)[p]$ projects injectively to a collection (α_v) with $\alpha_v \in \mathrm{Br}(K_v)[p]$. By Lemma 6.1 there exists $\phi_v : G_{K_v} \to \mathbb{Q}_p/\mathbb{Z}_p$ such that $\delta\phi_v = \alpha_v$ and some $a \in \mathbb{Z}/p\mathbb{Z}$ such that $\mathrm{inv}_v\, \alpha_v = a\phi(r_{K_v}(\zeta_p))$. For all but finitely many v, $\alpha_v = 0$ and so $\phi_v(\mu_p(\overline{K}_v)) = 0$ and therefore we get a character $\phi = \sum \phi_v : \mu_p(\mathbb{A}_K) \to \mathbb{Q}_p/\mathbb{Z}_p$. Also for $\zeta_p \in \mu_p(K^\times)$ we have $\phi(\zeta_p) = \sum \phi_v(r_{K_v}(\zeta_p)) = a^{-1} \sum \mathrm{inv}_v\, \alpha_v = 0$ and so ϕ factors through $\phi : \mu_p(K)\backslash\mu_p(\mathbb{A}_K) \to \mathbb{Q}_p/\mathbb{Z}_p$.

Since $\mathrm{Br}(\mathbb{C}) = 0$, for $v \mid \mathbb{C}$ one has $\phi_v = 0$. Moreover, as $p\alpha_v = 0$ it follows that $p\phi = 0$ and so $\mathrm{Im}\,\phi \subset \frac{1}{p}\mathbb{Z}/\mathbb{Z}$. Writing $\psi(x) = \exp(2\pi i x)$ we get $\Phi = \psi \circ \phi : \mu_p(K)\backslash\mu_p(\mathbb{A}_K) \to \mathbb{C}^\times$ having finite order p and such that $\Phi_v = 1$ for $v \mid \mathbb{C}$. Proposition 5.11 implies the existence of a finite order extension of Φ from $\mu_p(K)\backslash\mu_p(\mathbb{A}_K)$ to $\mathbb{A}_K^\times/K^\times$. As Φ has finite order it is necessarily trivial on $K_\infty^{\times,0}$ and so Φ factors through $\mathbb{A}_K^\times/\overline{K^\times K_\infty^{\times,0}} \cong G_K^{\mathrm{ab}}$. As Φ has finite order, its image lies in $\psi(\mathbb{Q}/\mathbb{Z})$ and so composing with logarithm we get an extension $\phi : G_K^{\mathrm{ab}} \to \mathbb{Q}/\mathbb{Z}$ and composing again with projection to $\mathbb{Q}_p/\mathbb{Z}_p$ gives $\phi : G_K^{\mathrm{ab}} \to \mathbb{Q}_p/\mathbb{Z}_p$. By construction $\delta\phi = \alpha$ as desired. □

6.2 Lifting projective Galois representations

Lemma 6.3. *Let Γ be a profinite group and let $H \subset G$ be topological groups such that $H \subset Z(G)$. Let $\overline{\rho} : \Gamma \to G/H$ be a homomorphism. For each $g \in \Gamma$ let a_g be an arbitrary lift of $\overline{\rho}(g)$ to G. Then $c(g,h) = a_{gh}a_h^{-1}a_g^{-1}$ is well-defined in $H^2(\Gamma, H)$ and there exists a homomorphism $\rho : \Gamma \to G$ such that the image of $\rho(g)$ in G/H is $\overline{\rho}(g)$ if and only if c is cohomologically trivial.*

Proof. Since the image of $c(g,h)$ in G/H is $\overline{\rho}(gh)\overline{\rho}(h)^{-1}\overline{\rho}(g)^{-1} = 1$ it follows that $c(g,h) \in H$. Moreover, as $c(g,h) \in Z(G)$ it follows that we also have $c(g,h) = a_h^{-1}a_g^{-1}a_{gh} = a_g^{-1}a_{gh}a_h^{-1}$. Using these and the fact that $c(g,h) \in Z(G)$ one may check that $(dc)(g,h,i) = c(h,i)c(gh,i)^{-1}c(g,hi)c(g,h)^{-1} = 1$ and so $c \in Z^2(\Gamma, H)$, where H has trivial Γ action.

Also note that if a'_g is any other lift of $\overline{\rho}(g)$ to G then writing $\phi(g) = a'_g a_g^{-1}$ one has $\phi(g) \in H$. Writing $c'(g,h) = a'_{gh}(a'_h)^{-1}(a'_g)^{-1}$ one gets $c'(g,h) = \phi(gh)\phi(g)^{-1}\phi(h)^{-1}c(g,h)$ and so c' and c are equal in $H^2(\Gamma, H)$. Certainly the lift a'_g comes from a homomorphism $\rho : \Gamma \to G$ if and only if $c' = 1$ if and only if $c = c'$ is cohomologically trivial in $H^2(\Gamma, H)$. □

Theorem 6.4. *Let K be a number field and $\overline{\rho} : G_K \to \mathrm{PGL}(n, \overline{\mathbb{Q}}_p)$ be a continuous homomorphism. Then there exists a continuous representation $\rho : G_K \to \mathrm{GL}(n, \overline{\mathbb{Q}}_p)$ such that the image of $\rho(g)$ in $\mathrm{PGL}(n, \overline{\mathbb{Q}}_p)$ is $\overline{\rho}(g)$ for any g.*

Proof. Note that $H_m = \mathrm{SL}(n, \overline{\mathbb{Q}}_p)\mu_{nm}(\overline{\mathbb{Q}}_p) \twoheadrightarrow \mathrm{PGL}(n, \overline{\mathbb{Q}}_p)$ via the natural projection and that the kernel is $1 \to \mu_{nm}(\overline{\mathbb{Q}}_p) \to H_m \twoheadrightarrow \mathrm{PGL}(n, \overline{\mathbb{Q}}_p)$.

Let $c_m \in H^2(G_K, \mu_{mn})$ be the cohomology class associated by Lemma 6.3 to an arbitrary lift of $\overline{\rho}$ to H_m. The cohomology classes are compatible under the maps $H^2(G_K, \mu_{nm}) \to H^2(G_K, \mu_{nm'})$ if $m \mid m'$ and so we get a cohomology class

$$c = \varinjlim c_m \in \varinjlim H^2(G_K, \mu_{mn}(\overline{\mathbb{Q}}_p)) = H^2(G_K, \mathbb{Q}/\mathbb{Z}) = 0$$

where the last equality if the content of Theorem 6.2. But then $c = 0$ implies that $c_m = 0$ for some m and therefore $\overline{\rho}$ lifts to a homomorphism $\rho : G_K \to H_m \subset \mathrm{GL}(n, \overline{\mathbb{Q}}_p)$. □

Lecture 12
2013-04-26

Proposition 6.5. *Suppose K is a number field and $\overline{\rho} : G_K \to \mathrm{PGL}(n, \overline{\mathbb{Q}}_p)$ is a projective Galois representation which is unramified almost everywhere. Let $\rho : G_K \to \mathrm{GL}(n, \overline{\mathbb{Q}}_p)$ be a lift of $\overline{\rho}$. Then ρ is unramified almost everywhere.*

Proof. Let $F/\mathbb{Q}_p$ be a finite extension such that $\rho : G_K \to \mathrm{GL}(n, F)$ (standard Baire category theory argument). The representation ρ is continuous and so there exists L/K finite such that $\rho(G_L) \subset 1 + p^2 M_{n\times n}(\mathcal{O}_F)$ (the composition of ρ with projection to the discrete group $\mathrm{GL}(n, F)/(1 + p^2 M_{n\times n}(\mathcal{O}_F))$ has open kernel). Note that $\log : 1 + p^2 M_{n\times n}(\mathcal{O}_F) \to p^2 M_{n\times n}(\mathcal{O}_F)$ and $\exp : p^2 M_{n\times n}(\mathcal{O}_F) \to 1 + p^2 M_{n\times n}(\mathcal{O}_F)$ are inverses to each other and satisfy the Baker-Campbell-Hausdorff formula. Thus the log map is injective and has the property that $\log((1 + p^2 X)^n) = n \log(1 + p^2 X)$. Therefore $\log \rho(G_L)$ is a pro-p torsion-free group.

Let v be a place such that $v \nmid p$, L_w/K_v is unramified at $w \mid v$ and $\overline{\rho}(I_{K_v}) = 1$. This implies that $I_{K_v} = I_{L_w}$ and so it suffices to show that $\rho(I_{L_w}) = 1$. But $\rho(I_{L_w}) \subset F^\times = \ker(\mathrm{GL}(n, F) \to \mathrm{PGL}(n, F))$ is abelian and so $\rho(I_{L_w}) = \rho(I_{L_w}^{\mathrm{ab}})$. Now $I_{L_w}^{\mathrm{ab}} \cong \mathcal{O}_{L_w}^\times \cong k_{L_w}^\times \times \mu_{p^\infty}(L_w) \times (1 + (\varpi_w))^{\mathrm{TF}}$ where TF stands for torsion-free and $\mu_{p^\infty}(L_w)$ is finite because the ramification of $L_w(\mu_{p^n})/L_w$ grows with n. Since $\rho(I_{L_w})$ is torsion-free it follows that $\rho(\mu_\infty(L_w)) = 1$ and so $\rho(I_{L_w}) = \rho((1 + (\varpi_w))^{\mathrm{TF}})$. But $(1 + (\varpi_w))^{\mathrm{TF}}$, being a subgroup of $1 + (\varpi_{L_w})$, is pro-q_w-group whereas its image is in $1 + p^2 M_{n\times n}(\mathcal{O}_F)$ which is pro-p with $p \nmid q_w$. All subgroups of pro-p groups must be pro-p and so $\rho((1 + (\varpi_w))^{\mathrm{TF}}) = 1$ and it follows that $\rho(I_{L_w}) = 1$. □

6.3 Local Galois representations in the "tame" case

Theorem 6.6. *Let $K/\mathbb{Q}_p$ be a finite extension and $\rho : G_K \to \mathrm{GL}(n, \mathbb{C})$ be an irreducible continuous representation. If $p \nmid n$ (the "tame" case) then there exists an order n extension L/K and a continuous character $\chi : L^\times \to \mathbb{C}^\times$ such that $\rho \cong \mathrm{Ind}_L^K \chi$.*

Before proving the theorem we give two results of Clifford.

Proposition 6.7. *Let G be a profinite group and let $N \lhd G$ be an open normal subgroup. Let (ρ, V) be an irreducible representation of G over a field K and let $(\rho, W) \subset V|_N$ be an irreducible component. Then*

1. *$V = \sum_{g\in G/N} \rho(g)W$ and there exist $g_1, \ldots, g_n$ such that $V = \oplus \rho(g_i)W$ as representations of N.*
2. *If U is an irreducible representation of N write $V[U]$ be the U-isotypical component in V, i.e., the set of $v \in V$ lying in the image of some N-equivariant map $U \to V$. Then the set of U such that $V[U] \neq 0$ is finite, G acts transitively on it and $V = \oplus V[U]$.*
3. *Let U be an irreducible representation of N such that $V[U] \neq 0$ and write $H = \{g \in G | gV[U] = V[U]\}$. Then $V \cong \mathrm{Ind}_H^G V[U]$ as representations of G.*

Proof. Clearly $\sum_{g\in G/N}\rho(g)W \subset V$ is G-invariant and must be equal to V since V is an irreducible G-representation. Now since N is normal in G, $\rho(g)W$ is also a (necessarily irreducible) representation of N and thus $\rho(g)W \cap \rho(g')W$ is either 0 or equal to $\rho(g)W$ and therefore V becomes a direct sum of $\rho(g_i)W$ for finitely many g_i.

That the set of U with $V[U] \neq 0$ is clear from the fact that V is finite dimensional. Next, let $U \subset V|_N$ irreducible, then $U \subset \oplus\rho(g_i)W$ and since each $\rho(g_i)W$ is irreducible it follows that $U = \rho(g_i)W$ for some g_i. Finally $V[U] = \oplus U'$ where $U' \subset V|_N$ such that $U \cong U'$ as N-representations and so $V = \oplus V[U]$ as N-representations.

Finally, let $U = U_1, U_2, \ldots, U_m$ be the finitely many irreducible representations of N such that $V = \oplus V[U_i]$ and let g_i such that $U_i = \rho(g_i)U$. It follows that $G/H = \{g_1, \ldots, g_m\}$. Any $v \in V$ can be represented uniquely as $v = \sum \rho(g_i)v_i$ where $v_i \in U$. The map $V \to K[G] \otimes_{K[H]} V[U]$ given by $v \mapsto \sum [g_i] \otimes v_i$ is an isomorphism of vector spaces which can easily be checked to be G-equivariant and therefore is an isomorphism of G-representations. Finally, $K[G] \otimes_{K[H]} V[U] \cong \mathrm{Ind}_H^G V[U]$ via the G-equivariant map sending $[g] \otimes v$ to the function sending g to v and every coset other than gH to 0. □

Lecture 13
2013-04-29

Proposition 6.8. *Let G, N, V and W as in Proposition 6.7 such that K is algebraically closed and $V = V[W]$ (in which case immediately $\dim W \mid \dim V$). Then there exist irreducible projective representations $\sigma : G \to \mathrm{PGL}(\dim W, K)$ and $\tau : G \to \mathrm{PGL}(\dim V/\dim W, K)$ with τ trivial on N, such that $\rho = \sigma \otimes \tau$ in $\mathrm{PGL}(\dim V, K)$.*

Proof. The group N acts on $\rho(g)W$ via $\rho(n)\rho(g)w = \rho(g)\rho^g(n)w$ which makes sense since N is normal in G. Recall that $V = \oplus\rho(g)W$ as N-representations where $\rho(g)W$ has the action $\rho|_W^g(n)w = \rho|_W(g^{-1}ng)w$. Since $\rho(g)W \cong W$ as V is isotypic there exist matrices A_g such that $\rho|_W^g(n) = A_g\rho|_W(n)A_g^{-1}$ for all $n \in N$, where A_g is defined up to scalars. Let $\sigma(g) = A_g : G \to \mathrm{PGL}(W)$ be the first projective representation; the fact that this is a homomorphism is straightforward to check.

Proposition 6.7 shows that $V = \oplus\rho(g_i)W$ for finitely many g_i in which case $\dim W \mid \dim V$ as desired. Let $r = \dim V/\dim W$ and let U be a vector space spanned by $u_1, \ldots, u_r$, let $w_1, \ldots, w_m$ be a basis of W and let $w_{ij} = \rho(g_i)w_j$ be a basis of $\rho(g_i)W$. For $g \in G$ write $\rho(g_ig)w_j = \sum \beta_{ijkl}(g)w_{kl}$ (the order really is g_ig!) which can be done since w_{kl} is a basis for V. Define $U \otimes_K W$ as a G-representation by $\mu(g)(u_i \otimes w_j) = \sum_{k,l} \beta_{ijkl}(g)u_k \otimes w_l$ which exhibits $U \otimes W \cong V$ as G-representations. It suffices to construct the projective representation τ on $\mathrm{PGL}(U)$ such that $\rho \cong \sigma \otimes \tau$.

Note that for $n \in N$ one has $\rho(g_in)w_j = \rho(g_i)\rho|_W(n)w_j \in \rho(g_j)W$ and so $\mu(n) = 1 \otimes \rho|_W(n)$. For every $g \in G$ one has that $\rho|_W^g(n) = A_g\rho|_W(n)A_g^{-1}$ and therefore get that

$$\begin{aligned}
\mu^g(n) &= 1 \otimes \rho^g|_W(n) \\
&= (1 \otimes A_g^{-1})(1 \otimes \rho|_W(n))(1 \otimes A_g) \\
\mu^g(n) &= \mu(g)^{-1}\mu(n)\mu(g) \\
&= \mu(g)^{-1}(1 \otimes \rho|_W(n))\mu(g)
\end{aligned}$$

So $\mu(g)(1 \otimes A_g)$ commutes with $1 \otimes \rho|_W(n)$ for all $g \in G$. For $g \in G$ let $F(g) = \mu(g)(1 \otimes A_g) \in \mathrm{End}(U \otimes W)$. Since every element of $U \otimes_K W$ can be written uniquely as a linear combination of $u_i \otimes v_i$ for some $v_i \in W$ and the basis vectors u_i of U, one can write $F(g)(u_i \otimes w)$ as $\sum u_j \otimes F_{ij}(g)(w)$ for linear maps $F_{ij}(g) \in \mathrm{End}(W)$. Since $F(g)$ commutes with $1 \otimes \rho|_W(n)$ it follows that $F_{ij}(g)$ commutes with $\rho|_W(n)$. But $(\rho|_N, W)$ is irreducible and so $F_{ij}(g) \in Z(\mathrm{End}_N(W)) \cong K^\times$ by Schur's lemma. Therefore $F_{ij}(g) = \alpha_{ij}(g)$ for scalars $\alpha_{ij}(g) \in K^\times$. Writing $\tau(g)u_i = \sum \alpha_{ij}(g)u_j$ it follows that $\tau(g) \in \mathrm{End}(U)$ giving a projective representation $\tau : G \to \mathrm{PGL}(U)$ (since A_g is defined up to scalars only). That τ is trivial on N follows from the fact that for $n \in N$, $\mu(n) = 1 \otimes \rho|_W(n)$.

Finally, σ and τ are irreducible because otherwise V would be reducible, which it is not. □

Definition 6.9. A **supersolvable** finite group is a finite group G with a descending filtration $G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$ such that $G_i \lhd G$ and the successive quotients G_i/G_{i+1} are cyclic.

Proposition 6.10. *If (ρ, V) is an irreducible representation of the supersolvable group G over an algebraically closed field K then there exists a subgroup $H \subset G$ and a character $\chi : H \to K^\times$ such that $\rho \cong \mathrm{Ind}_H^G \chi$.*

Proof. If G is abelian then ρ is a character to begin with. We will prove the result by induction on $|G|$. If $\rho : G \to \mathrm{GL}(V)$ is not faithful, i.e., if $\ker \rho = H \lhd G$ then ρ factors through $\rho : G/H \to \mathrm{GL}(V)$ where $|G/H| < |G|$ and so by induction ρ is induced from a character. Suppose therefore that ρ is faithful.

The group $G/Z(G)$ is supersolvable with filtration $G/Z(G) = H_0 \supset H_1 \supset \cdots \supset H_m = 1$ with $H_i \lhd G/Z(G)$ and H_i/H_{i+1} cyclic. Let $H = H_{m-1}Z(G)$ which will be proper in G if G is not abelian. Since $H_{m-1} = H_{m-1}/H_m$ is a cyclic normal subgroup of $G/Z(G)$, $H \lhd G$ is abelian. Since $H \not\subset Z(G)$ and ρ is injective it follows that $\rho(H) \not\subset Z(\rho(G)) = K^\times$ where the last equality follows from the irreducibility of ρ.

Now Proposition 6.7 implies, since H is normal in G that if $U \subset V|_H$ is a (necessarily one dimensional) irreducible then $V[U]$ is irreducible as a representation of $H_U = \{g \in G | gV[U] = V[U]\}$ and that $V \cong \mathrm{Ind}_{H_U}^G V[U]$. If $V \neq V[U]$ then by the inductive hypothesis $V[U] \cong \mathrm{Ind}_T^{H_U} \chi$ for $T \subset H_U$ and χ a character in which case $V \cong \mathrm{Ind}_T^G \chi$. If $V = V[U]$ then as representations of H, $V \cong U^{\oplus d}$ where U is one-dimensional and so $\rho(H)$ consists of scalar matrices contradicting the construction of H. □

Lemma 6.11. *Let $G \to H$ be a surjection of finite groups with abelian kernel and let $\rho : H \to \mathrm{GL}(V)$ be a finite dimensional representation. Suppose $F \subset H$ is a subgroup and $E \subset G$ is its preimage in G. Suppose $\widetilde{\rho} : G \to \mathrm{GL}(V)$ is the composition of $G \to H \to \mathrm{GL}(V)$ and that there exists $\tau : E \to \mathrm{GL}(W)$ such that $\widetilde{\rho} \cong \mathrm{Ind}_E^G \tau$. Then $\rho \cong \mathrm{Ind}_F^H \sigma$ for a representation σ.*

Proof. Let $\pi : G \to H$. If $k \in \ker \pi$ then $k \in \ker \rho$ so $\widetilde{\rho}(k) = 1$. But at the same time $\ker \pi \subset E$ and so $\widetilde{\rho}(k) = \oplus_{g \in G/E} \tau^g(k)$ which implies that τ is trivial on $\ker \pi$. Thus τ descends to a representation $\sigma : E/\ker \pi \cong F \to \mathrm{GL}(W)$. The map π gives $G/H \cong E/F$ and so $\mathrm{Ind}_E^G \tau \cong (\mathrm{Ind}_F^H \sigma) \circ \pi$ which, since π is surjective, gives $\rho \cong \mathrm{Ind}_F^H \sigma$ as desired. □

Lemma 6.12. *Let G be a finite group and $H \lhd G$ a normal subgroup such that G/H is supersolvable. If (ρ, V) is an irreducible representation of G that cannot be written as the induction from a subgroup of G, then $V|_H$ is irreducible.*

Proof. Suppose $V|_H$ is reducible and let W an irreducible H-subrepresentation. Proposition 6.7 implies that unless V is isotypic, i.e., $V = V[W]$, V can be written as an induction. Therefore $V = V[W]$ and so $V = \oplus \rho(g_i)W$ where all the $\rho(g_i)W$ are isomorphic to W. We may therefore apply Proposition 6.8. We obtain $\sigma : G \to \mathrm{PGL}(W)$ and $\tau : G \to \mathrm{PGL}(U)$ where U has dimension $\dim V/\dim W > 1$, $\tau|_H = 1$ and $\sigma|_H \cong \rho|_H$. Since $\tau|_H = 1$, the projective representation τ factors through $G/H \to \mathrm{PGL}(U)$. For simplicity denote $G' = G/H$ supersolvable.

Recall from §6.2 that attached to $\tau : G' \to \mathrm{PGL}(U)$ is a cohomology class $c \in H^2(G', \mu_N)$ for some integer N in which case one get a genuine representation $\widetilde{\tau} : G' \rtimes \mu_N \to \mathrm{GL}(U)$ as follows: let $\widetilde{\tau}$ be a fixed lifting of τ to $G' \to \mathrm{GL}(U)$ (not necessarily a homomorphism) and define $G' \rtimes \mu_N$ by letting multiplication be given by $(g, \alpha)(h, \beta) = (gh, \alpha\beta c(g, h))$ in which case setting $\widetilde{\tau}(g, \alpha) = \widetilde{\tau}(g)\alpha$ is in fact a homomorphism. Indeed, $\widetilde{\tau}(g, \alpha)(h, \beta) = \widetilde{\tau}(gh)\alpha\beta c(g, h) = \widetilde{\tau}(g, \alpha)\widetilde{\tau}(h, \beta)$. Now $G' \rtimes \mu_N$ is also supersolvable because if $G' = G'_0 \supset \ldots \supset G'_i \supset \ldots \supset 1$ is such that $G'_i \lhd G'$ and G'_i/G'_{i+1} is cyclic then $G' \rtimes \mu_n = G'_0 \rtimes \mu_N \supset \ldots \supset G'_i \rtimes \mu_N \supset \ldots \supset 1 \rtimes \mu_N \supset 1$ is such that $G'_i \rtimes \mu_N \lhd G' \rtimes \mu_N$ and $G'_i \rtimes \mu_N / G'_{i+1} \rtimes \mu_N \cong G'_i/G'_{i+1}$ is cyclic while $\mu_N/1$ is also cyclic. As $\widetilde{\tau}$ is irreducible and $G' \rtimes \mu_N$ is supersolvable it follows that $\widetilde{\tau} \cong \mathrm{Ind}_{H'}^{G' \rtimes \mu_N} \chi$ for a character $\chi : H' \to K^\times$ by Proposition 6.10. The group $1 \rtimes \mu_N \lhd G' \rtimes \mu_N$ and so Mackey[1] gives

$$\widetilde{\tau}|_{1 \rtimes \mu_N} = \oplus_{g \in G' \rtimes \mu_N / H(1 \rtimes \mu_N)} (\mathrm{Ind}_{H' \cap 1 \rtimes \mu_N}^{1 \rtimes \mu_N} \chi)^g$$

[1] If $H \subset G$, V is a representation of G and $N \lhd G$ then

$$(\mathrm{Ind}_H^G V)|_N = \oplus_{g \in G/HN} (\mathrm{Ind}_{H \cap N}^N V)^g$$

But evaluating $\widetilde{\tau}(1,\alpha) = (\mathrm{Ind}_{H'}^{G'\rtimes\mu_N}\chi)(1,\alpha)$ we get a scalar matrix and so χ is in fact a character of $H'(1\rtimes\mu_N)$ as all $1\rtimes\mu_N/H'\cap(1\rtimes\mu_N)$ conjugates of χ are equal. If $1\rtimes\mu_N\not\subset H'$ then this would imply that $\widetilde{\tau}\cong\mathrm{Ind}_{H'}^{G'\rtimes\mu_N}\chi$ would be reducible. Thus $1\rtimes\mu_N\subset H'$. Writing $H''=\{(g,1)|(g,\alpha)\in H'\}$ gives $H'=H''\rtimes\mu_N$. Note that composing $\widetilde{\tau}$ with the projection $G\to G/H$ gives $\widetilde{\tau}=\mathrm{Ind}_{H''H\rtimes\mu_N}^{G\rtimes\mu_N}\chi$ where χ extends to $H''H$ by its action on H''.

For some integer M a lift to $\mathrm{GL}(\dim W)$ of $\sigma(g,\alpha)$ defined as $\sigma(g)$ will give an actual homomorphism $\widetilde{\sigma}:G\rtimes\mu_N\rtimes\mu_M\to\mathrm{GL}(\dim W)$ whereas $\widetilde{\tau}$ lifts to $G\rtimes\mu_N\rtimes\mu_M\to\mathrm{GL}(\dim V/\dim W)$ by sending (g,α,β) to $\widetilde{\tau}(g,\alpha)$. Then as a representation of $G\rtimes\mu_N\rtimes\mu_M$ have $\widetilde{\tau}\cong\mathrm{Ind}_{H''H\rtimes\mu_N\rtimes\mu_M}^{G\rtimes\mu_N\rtimes\mu_M}\chi$ where χ on $H''H\rtimes\mu_N\rtimes\mu_M$ is defined via the projection to $H''H\rtimes\mu_N$.

Let $\widetilde{\rho}=\widetilde{\sigma}\otimes\widetilde{\tau}\cong\mathrm{Ind}_{H''H\rtimes\mu_N\rtimes\mu_M}^{G\rtimes\mu_N\rtimes\mu_M}(\widetilde{\sigma}\otimes\chi)$. Let $\widetilde{\rho}'$ be the composition of the representation ρ with the projection $G\rtimes\mu_N\rtimes\mu_M\to G$. Then $\widetilde{\rho}$ and $\widetilde{\rho}'$ are representations of $G\rtimes\mu_N\rtimes\mu_M$ whose projectivisations agree. Therefore they differ by a character ψ of $G\rtimes\mu_N\rtimes\mu_M$. Therefore $\widetilde{\rho}'$ is an induced representations which implies that ρ is induced by Lemma 6.11. □

Lecture 14
2013-05-01

Proof of Theorem 6.6. First, ρ is a continuous representation and thus factors through $G_{L/K}$ for some finite Galois extension L/K. Next, write $\rho\cong\mathrm{Ind}_{G_{L/M}}^{G_{L/K}}\rho'$ such that ρ' cannot be written as an induction. Since ρ is irreducible it follows that ρ' is irreducible and $p\nmid\dim\rho'\mid\dim\rho$. Therefore it suffices to show that if ρ cannot be written as an induction then ρ has dimension 1.

Let $P_{L/K}=G_{L/K}^1$ be the wild inertia. Note that $G_0=G_{L/K}/P_{L/K}$ contains $G_1=I_{L/K}/P_{L/K}$ as a normal subgroup and $G_0/G_1\cong G_{k_L/k_K}$ which is cyclic. Moreover, $I_{L/K}=I_K/I_K\cap G_L$ and $P_{L/K}=P_K/P_K\cap G_L$ by the Herbrandt quotient theorem and so $I_{L/K}/P_{L/K}\cong I_K/P_K(I_K\cap G_L)$. But $I_K/P_K\cong\prod\mathbb{Z}_p(1)$ and so $I_{L/K}/P_{L/K}$ is a finite quotient of an abelian group which must therefore be supersolvable. Lemma 6.12 then shows that $\rho|_{P_{L/K}}$ is irreducible.

But $P_{L/K}$ is a p-group and so $\dim\rho\mid|P_{L/K}|$ must be a power of p. But $p\nmid\dim\rho$ and so $\dim\rho=1$ as desired. □

7 Iwasawa theory for $\mathbb{Z}_p$-extensions

The main result of this section is the following theorem of Iwasawa on $\mathbb{Z}_p$-extensions. The main reference is [Was97, §13].

Theorem 7.1. *Suppose $p>2$ is a prime. Let K_∞/K be any $\mathbb{Z}_p$ extension of the number field K. Then there exist integers $\lambda,\mu\geq 0$ and ν depending only on K such that $v_p(h_{K_n})=\lambda n+\mu p^n+\nu$ for $n>>0$.*

7.1 $\mathbb{Z}_p$-extensions and Leopoldt's conjecture

Proposition 7.2. *Let K be a number field. There exists a tower of extensions $K=K_0\subset K_1\subset\ldots$ such that $K_\infty=\cup K_n$ is Galois over K with Galois group $G_{K_\infty/K}\cong\mathbb{Z}_p$ and $G_{K_\infty/K_n}\cong p^n\mathbb{Z}_p$.*

Proof. The extension $\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}$ is abelian with Galois group $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times\cong(\mathbb{Z}/p\mathbb{Z})^\times\times\mathbb{Z}/p^n\mathbb{Z}$. Let $\mathbb{Q}_n$ be the subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ fixed under $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $G_{\mathbb{Q}_n/\mathbb{Q}}\cong\mathbb{Z}/p^n\mathbb{Z}$. Writing $\mathbb{Q}_\infty=\cup\mathbb{Q}_n$ gives $G_{\mathbb{Q}_\infty/\mathbb{Q}}\cong\varprojlim\mathbb{Z}/p^n\mathbb{Z}\cong\mathbb{Z}_p$.

Now let $K_\infty=K\mathbb{Q}_\infty$ with Galois group $G_{K_\infty/K}\cong G_{\mathbb{Q}_\infty/\mathbb{Q}_\infty\cap K}$. But the latter is an open subgroup of $G_{\mathbb{Q}_\infty/\mathbb{Q}}\cong\mathbb{Z}_p$ and so is of the form $p^k\mathbb{Z}_p$ for some $k\geq 0$ giving $G_{K_\infty/K}\cong p^k\mathbb{Z}_p\cong\mathbb{Z}_p$ additively. This is the cyclotomic $\mathbb{Z}_p$-extension. Writing K_n to be the subfield of K_∞ fixed by $p^n\mathbb{Z}_p$ produces the desired tower. □

Having produced a $\mathbb{Z}_p$ extension of K we would like to answer the question of how many such extensions there exist. To answer such question we need the following result from group theory:

Lemma 7.3. *Let G be a pro-p group. Then G is generated by $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$ elements. The maximal torsion free subgroup of G is generated by $\operatorname{rank}_{\mathbb{Z}_p} H^1(G, \mathbb{Z}_p)$ elements.*

Proof. See [NSW08, Proposition 3.9.1]. □

Lemma 7.4. *Let G be a profinite group and let H be the maximal abelian pro-p torsion-free subquotient of G. Then*

$$\operatorname{rank}_{\mathbb{Z}_p} H^1(G, \mathbb{Z}_p) = \operatorname{rank}_{\mathbb{Z}_p} H^1(H, \mathbb{Z}_p)$$

Proof. As G acts trivially on $\mathbb{Z}_p$ it follows that $H^1(G, \mathbb{Z}_p) \cong \operatorname{Hom}(G, \mathbb{Z}_p) \cong \operatorname{Hom}(G^{\mathrm{ab}}, \mathbb{Z}_p) \cong H^1(G^{\mathrm{ab}}, \mathbb{Z}_p)$. Let $H = G^{\mathrm{ab}}/U$ for U open. Then inflation-restriction gives

$$1 \to H^1(H, \mathbb{Z}_p) \to H^1(G^{\mathrm{ab}}, \mathbb{Z}_p) \to H^1(U, \mathbb{Z}_p)$$

so it suffices to show that $\operatorname{rank}_{\mathbb{Z}_p} H^1(U, \mathbb{Z}_p) = 0$. Now let $V = U/N$ be the maximal pro-p quotient of U, in which case V is torsion (by choice of U) and every finite quotient of N will have cardinality coprime to p. Again inflation-restriction gives

$$1 \to H^1(V, \mathbb{Z}_p) \to H^1(U, \mathbb{Z}_p) \to H^1(N, \mathbb{Z}_p)$$

The group V is finite so $H^1(V, \mathbb{Z}_p)$ is torsion and so $\operatorname{rank}_{\mathbb{Z}_p} H^1(V, \mathbb{Z}_p) = 0$ which implies that $\operatorname{rank}_{\mathbb{Z}_p} H^1(U, \mathbb{Z}_p) = \operatorname{rank}_{\mathbb{Z}_p} H^1(N, \mathbb{Z}_p)$ so it suffices to show that $\operatorname{rank}_{\mathbb{Z}_p} H^1(N, \mathbb{Z}_p) = 0$. But

$$H^1(N, \mathbb{Z}_p) = \varprojlim_{M \subset N} \left(\varinjlim_{p^n \mathbb{Z}_p \subset \mathbb{Z}_p} H^1(N/M, \mathbb{Z}/p^n\mathbb{Z}) \right)$$

where M is open normal in N. But N/M will be finite with cardinality invertible in $\mathbb{Z}/p^n\mathbb{Z}$ and so $H^1(N, \mathbb{Z}_p) = 0$. □

Proposition 7.5. *Let M be a finitely generated $\mathbb{Z}_p$-module.*

1. *If $K/\mathbb{Q}_p$ is a finite extension and M carries an action of G_K then*

   $$\chi(G_K, M) = \operatorname{rank}_{\mathbb{Z}_p} H^0(G_K, M) - \operatorname{rank}_{\mathbb{Z}_p} H^1(G_K, M) + \operatorname{rank}_{\mathbb{Z}_p} H^2(G_K, M) = -[K : \mathbb{Q}_p] \operatorname{rank}_{\mathbb{Z}_p} M$$

   Moreover, $\operatorname{rank}_{\mathbb{Z}_p} H^i(G_K, M) = \operatorname{rank}_{\mathbb{Z}_p} H^{2-i}(G_K, M^*(1))$.

2. *If $K/\mathbb{Q}$ is a number field, S is a finite set of places which includes the infinite places, the places where M is ramified and the places above p, and M carries an action of $G_{K,S}$, then*

   $$\begin{aligned} \chi(G_{K,S}, M) &= \operatorname{rank}_{\mathbb{Z}_p} H^0(G_{K,S}, M) - \operatorname{rank}_{\mathbb{Z}_p} H^1(G_K, M) + \operatorname{rank}_{\mathbb{Z}_p} H^2(G_K, M) \\ &= \sum_{v|\infty} \operatorname{rank}_{\mathbb{Z}_p} M^{G_{K_v}} - [K : \mathbb{Q}] \operatorname{rank}_{\mathbb{Z}_p} M \end{aligned}$$

Proof. First note that if M is a finitely generated $\mathbb{Z}_p$-module and G is one of G_K and $G_{K,S}$ then Propositions 3.6 and 3.8 imply that $H^i(G, M)$ is a finitely generated $\mathbb{Z}_p$-module. Next one may write $M = M_{\mathrm{tors}} \oplus M_{\mathrm{TF}}$ where M_{tors} (the finite torsion) is stable under G and M_{TF} is torsion-free. As $H^i(G, M_{\mathrm{tors}})$ is finite it follows that $\operatorname{rank}_{\mathbb{Z}_p} H^i(G, M_{\mathrm{tors}}) = 0$. Using the exact sequence $H^i(G, M_{\mathrm{tors}}) \to H^i(G, M) \to H^i(G, M_{\mathrm{TF}}) \to H^{i+1}(G, M_{\mathrm{tors}})$ we deduce that $\operatorname{rank}_{\mathbb{Z}_p} H^i(G, M) = \operatorname{rank}_{\mathbb{Z}_p} H^i(G, M_{\mathrm{TF}})$ so for the rest of the argument we may assume that M is in fact torsion-free.

For any finitely generated $\mathbb{Z}_p$ module X one has that $\operatorname{rank}_{\mathbb{Z}_p} X = \dim_{\mathbb{F}_p}(X/pX) - \dim_{\mathbb{F}_p} X[p]$. Applying this observation to $X = H^i(G, M)$ get that

$$\operatorname{rank}_{\mathbb{Z}_p} H^i(G, M) = \dim_{\mathbb{F}_p} H^i(G, M)/pH^1(G, M) - \dim_{\mathbb{F}_p} H^1(G, M)[p]$$

Since M is a free $\mathbb{Z}_p$ module get an exact sequence $0 \to M \xrightarrow{p} M \to M/pM \to 0$ which gives the exact sequence

$$0 \to H^i(G,M)/pH^i(G,M) \to H^i(G,M/pM) \to H^{i+1}(G,M)[p] \to 0$$

We deduce that

$$\begin{aligned}
\chi(G,M) &= \operatorname{rank}_{\mathbb{Z}_p} H^0(G,M) - \operatorname{rank}_{\mathbb{Z}_p} H^1(G,M) + \operatorname{rank}_{\mathbb{Z}_p} H^2(G,M) \\
&= \dim_{\mathbb{F}_p} H^0(G,M)/pH^0(G,M) - \dim_{\mathbb{F}_p} H^0(G,M)[p] \\
&\quad - (\dim_{\mathbb{F}_p} H^1(G,M)/pH^1(G,M) - \dim_{\mathbb{F}_p} H^1(G,M)[p]) \\
&\quad + \dim_{\mathbb{F}_p} H^2(G,M)/pH^2(G,M) - \dim_{\mathbb{F}_p} H^2(G,M)[p] \\
&= \dim_{\mathbb{F}_p} H^0(G,M/pM) - \dim_{\mathbb{F}_p} H^1(G,M/pM) + \dim_{\mathbb{F}_p} H^2(G,M/pM) \\
&\quad - \dim_{\mathbb{F}_p} H^0(G,M)[p] - \dim_{\mathbb{F}_p} H^3(G,M)[p] \\
&= \dim_{\mathbb{F}_p} \chi(G,M/pM) - \dim_{\mathbb{F}_p} H^0(G,M)[p] - \dim_{\mathbb{F}_p} H^3(G,M)[p] \\
&= \dim_{\mathbb{F}_p} \chi(G,M/pM) - \dim_{\mathbb{F}_p} H^3(G,M)[p]
\end{aligned}$$

where for the last equality note that $H^0(G,M) \subset M$ is torsion-free and so $H^0(G,M)[p] = 0$.

If $G = G_K$ for $K/\mathbb{Q}_p$ then $\dim_{\mathbb{F}_p} \chi(G,M/pM) = -[K:\mathbb{Q}_p] \dim_{\mathbb{F}_p}(M/pM) = -[K:\mathbb{Q}_p] \operatorname{rank}_{\mathbb{Z}_p} M$ by Theorem 3.7 and $H^3(G_K,M) = 0$. This concludes the proof of the first part.

If $G = G_{K,S}$ then by Theorem 3.9

$$\begin{aligned}
\dim_{\mathbb{F}_p} \chi(G,M/pM) &= \sum_{v|\infty} \dim_{\mathbb{F}_p}(M/pM)^{G_{K_v}} - [K:\mathbb{Q}] \dim_{\mathbb{F}_p}(M/pM) \\
\dim_{\mathbb{F}_p} H^3(G_{K,S},M)[p] &= \sum_{v \in \infty} \dim_{\mathbb{F}_p} H^3(G_{K_v},M)[p]
\end{aligned}$$

It therefore suffices to show that for $v \mid \infty$ one has

$$\dim_{\mathbb{F}_p}(M/pM)^{G_{K_v}} - \dim_{\mathbb{F}_p} H^3(G_{K_v},M)[p] = \operatorname{rank}_{\mathbb{Z}_p} M^{G_{K_v}}$$

If $v \mid \mathbb{R}$ then

$$\begin{aligned}
H^3(G_{\mathbb{C}/\mathbb{R}},M)[p] &= H^1(G_{\mathbb{C}/\mathbb{R}},M)[p] \\
&= M[2][p] = 0
\end{aligned}$$

where the last line comes from $H^{\mathrm{odd}}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}) = 0$. If $v \mid \mathbb{C}$ then trivially $H^3(G_{K_v},M) = 0$.

When $v \mid \infty$ then G_{K_v} is cyclic and so $H^1(G_{K_v},M) = 0$. But from the exact sequence $0 \to M^{G_{K_v}}/pM^{G_{K_v}} \to (M/pM)^{G_{K_v}} \to H^1(G_{K_v},M)[p] \to 0$ we deduce that $\dim_{\mathbb{F}_p}(M/pM)^{G_{K_v}} = \dim_{\mathbb{F}_p} M^{G_{K_v}}/pM^{G_{K_v}} = \operatorname{rank}_{\mathbb{Z}_p} M^{G_{K_v}}$ as desired. □

Proposition 7.6. *Let $K/\mathbb{Q}_\ell$ be a finite extension and K_∞/K be a $\mathbb{Z}_p$-extension. If $p \neq \ell$ then K_∞/K is the unique unramified extension with Galois group $\mathbb{Z}_p$. If $p = \ell$ there are exactly $[K:\mathbb{Q}_\ell]+1$ independent such extensions K_∞/K.*

Proof. Certainly $G_{K^{\mathrm{ur}}/K} \cong \widehat{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}_p$ and so there exists a unique unramified $\mathbb{Z}_p$-extension. Let K^p/K be the composite of all $\mathbb{Z}_p$ extensions, which will then be the maximal abelian pro-p extension of K with torsion-free Galois group over K. The number of independent $\mathbb{Z}_p$ extensions is equal to the $\mathbb{Z}_p$ rank of the abelian pro-p group $G_{K^p/K}$.

If $p \neq \ell$ then $K^p \subset K^t$ the maximal tamely ramified extension of K since $P_K = G_{\overline{K}/K^t}$ is pro-ℓ. But recall from local class field theory that $G^{\mathrm{ab}}_{K^t/K} \cong G^{\mathrm{ab}}_K/P^{\mathrm{ab}}_K \cong \widehat{K^\times}/(1+\mathfrak{m}_K) \cong \mathrm{Frob}_K^{\widehat{\mathbb{Z}}} \times \mathcal{O}_K^\times/(1+\mathfrak{m}_K) \cong \mathrm{Frob}_K^{\widehat{\mathbb{Z}}} \times k_K^\times$. The largest torsion-free pro-p subquotient of this is $\mathrm{Frob}_K^{\mathbb{Z}_p}$ corresponding to the unique unramified $\mathbb{Z}_p$

extension. Another way of seeing this is by recalling from local class field theory that $t : G_{K^t/K^{\mathrm{ur}}} = I_K/P_K \xrightarrow{\cong} \prod_{q\neq\ell}\mathbb{Z}_q(1)$ and $G_{K^{\mathrm{ur}}/K} \cong \widehat{\mathbb{Z}}$. If $\sigma \in G_{K^t/K}$ and $\tau \in I_K/P_K$ then $\sigma\tau\sigma^{-1} \in I_K/P_K$ since I_K is normal in G_K and $t(\sigma\tau\sigma^{-1}) = \sigma(t(\tau))$ where σ acts on $\prod_{q\neq\ell}\mathbb{Z}_q(1)$ via the Tate twist. Now G_{K^t/K^p} contains the commutant $[G_{K^t/K}, G_{K^t/K}]$. Let $\sigma \in G_{K^t/K}$ and $\tau \in G_{K^t/K^{\mathrm{ur}}}$ in which case $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{K^t/K^p}$. But then $t(\sigma\tau\sigma^{-1}\tau^{-1}) = \sigma(t(\tau))t(\tau)^{-1}$ has to be trivial in $G_{K^p/K}$ the maximal abelian torsion-free pro-p subquotient of $G_{K^t/K}$ and so $\sigma(t(\tau)) = t(\tau)$ in this quotient which, since no nontrivial element of $G_{K^t/K}$ acts trivially on nontrivial Tate twists, implies that $t(\tau) = 0$ in the quotient. But then I_K/P_K projects to 0 and so the maximal abelian torsion-free pro-p subquotient of $G_{K^t/K}$ is also the maximal abelian torsion-free pro-p subquotient of $G_{K^{\mathrm{ur}}/K} \cong \widehat{\mathbb{Z}}$, i.e., $\mathbb{Z}_p$ as desired.

Now suppose that $p = \ell$. The number of independent $\mathbb{Z}_p$ extensions, by Lemma 7.3, is $\mathrm{rank}_{\mathbb{Z}_p} H^1(G_{K^p/K}, \mathbb{Z}_p)$. The group $G_{K^p/K}$ is the maximal abelian pro-p torsion-free subquotient of G_K and so Lemma 7.4 implies that $\mathrm{rank}_{\mathbb{Z}_p} H^1(G_{K^p/K}, \mathbb{Z}_p) = \mathrm{rank}_{\mathbb{Z}_p} H^1(G_K, \mathbb{Z}_p)$.

Finally, Proposition 7.5 gives that $\mathrm{rank}_{\mathbb{Z}_p} H^2(G_K, \mathbb{Z}_p) = \mathrm{rank}_{\mathbb{Z}_p} H^0(G_K, \mathbb{Z}_p(1)) = 0$ and

$$\mathrm{rank}_{\mathbb{Z}_p} H^0(G_K, \mathbb{Z}_p) - \mathrm{rank}_{\mathbb{Z}_p} H^0(G_K, \mathbb{Z}_p) + \mathrm{rank}_{\mathbb{Z}_p} H^0(G_K, \mathbb{Z}_p) = -[K : \mathbb{Q}_p]$$

from where immediately we get that $\mathrm{rank}_{\mathbb{Z}_p} H^1(G_K, \mathbb{Z}_p) = [K : \mathbb{Q}_p] + 1$.

□

Lecture 15
2013-05-03

Lemma 7.7. *1. If $K/\mathbb{Q}_p$ is a finite extension then $\varprojlim K^\times \otimes \mathbb{Z}/p^n\mathbb{Z} \cong K^\times \otimes \mathbb{Z}_p$.*

2. If K is a number field and S is the set of places containing the infinite places and the places above p then

$$\varprojlim \mathcal{O}_{K,S}^\times \otimes \mathbb{Z}/p^n\mathbb{Z} \cong \mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p$$

Proof. For the first part write $K^\times \cong \varpi_K^{\mathbb{Z}} \times k_K^\times \times \mu_{p^\infty}(K) \times (1+\mathfrak{m}_K)^{\mathrm{TF}}$. It suffices to show that $\varprojlim M \otimes \mathbb{Z}/p^n\mathbb{Z} \cong M \otimes \mathbb{Z}_p$ for each part separately. This is clear for $\varpi_K^{\mathbb{Z}}$, $k_K^\times$ and $\mu_{p^\infty}(K)$ which is a finite group. The group $(1+\mathfrak{m}_K)^{\mathrm{TF}}$ is a finitely generated torsion-free $\mathbb{Z}_p$-module ($1+p^2\mathcal{O}_K \cong p^2\mathcal{O}_K$ under the logarithm map and the latter is a finitely generated $\mathbb{Z}_p$-module; $1+p^2\mathcal{O}_K$ is finite index in $(1+\mathfrak{m}_K)^{\mathrm{TF}}$ and so the latter is also finitely generated) and therefore it is of the form $\mathbb{Z}_p^r$. Finally the result is true for $\mathbb{Z}_p$ and thus also for $K^\times$.

For the second part suppose M is a finitely presented abelian group with presentation $\mathbb{Z}^r \to \mathbb{Z}^s \to M \to 0$. Let $K \subset \mathbb{Z}^r$ be the kernel of $\mathbb{Z}^r \to \mathbb{Z}^s$ in which case $(\mathbb{Z}^r/K) \otimes (\mathbb{Z}/p^n\mathbb{Z})$ satisfies the Mittag-Leffler condition and so $R^1\varprojlim((\mathbb{Z}^r/K) \otimes (\mathbb{Z}/p^n\mathbb{Z})) = 0$. But then we deduce that $\varprojlim M \otimes \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p^s/\mathbb{Z}_p^r \cong M \otimes \mathbb{Z}_p$. From Theorem 2.1 it follows that $\mathcal{O}_{K,S}^\times$ is a finitely generated abelian group with rank $|S|-1$. The group $\mathcal{O}_{K,S}^\times$ is therefore finitely presented and the second part follows. □

Proposition 7.8. *Let K be a number field with r_1 real places and r_2 complex places. Let p be a prime. Then the number of independent $\mathbb{Z}_p$ extensions is $1 + r_2 + \delta_K$ where δ_K, called the Leopoldt defect, satisfies $0 \leq \delta_K \leq r_1 + r_2 - 1$. If K_∞/K is a $\mathbb{Z}_p$-extension then K_∞/K is unramified outside of places above p.*

Remark 1. One of the many equivalent formulations of Leopoldt's conjecture is that always $\delta_K = 0$. In particular, if $K = \mathbb{Q}$ or $K/\mathbb{Q}$ is quadratic imaginary then Leopoldt's conjecture is true. In the case of $K = \mathbb{Q}$ the unique $\mathbb{Z}_p$ extension is the cyclotomic one while in the case of quadratic imaginary fields one has an additional $\mathbb{Z}_p$ extension called the anticyclotomic extension.

Proof of Proposition 7.8. First, let $v \mid \ell \neq p$ and let w be a place of K_∞ above v. Then $K_{\infty,w}/K_v$ is abelian with Galois group a subgroup of $\mathbb{Z}_p$ and so is a $\mathbb{Z}_p$ extension as well. Thus $K_{\infty,w}/K_v$ is unramified by Proposition 7.6.

Let K^p/K be as before the composite of all the $\mathbb{Z}_p$ extensions in which case K^p/K is the maximal abelian pro-p torsion-free extension of K which is unramified outside of p. Let S be the finite set of places containing the infinite places and the places above p. Then $K^p \subset K_S$ and $G_{K^p/K}$ is a quotient of $G_{K,S}$. As before the number Z of independent $\mathbb{Z}_p$ extensions is $Z = \operatorname{rank}_{\mathbb{Z}_p} H^1(G_{K^p/K}, \mathbb{Z}_p)$.

The group $G_{K^p/K}$ is the maximal abelian pro-p torsion-free subquotient of $G_{K,S}$ and so by Lemma 7.4 it follows that

$$Z = \operatorname{rank}_{\mathbb{Z}_p} H^1(G_{K^p/K}, \mathbb{Z}_p) = \operatorname{rank}_{\mathbb{Z}_p} H^1(G_{K,S}, \mathbb{Z}_p)$$

The set S contains the infinite places and the places above p ($\mathbb{Z}_p$ is everywhere unramified as it carries the trivial G_K-action) and so Proposition 7.5 implies that

$$\operatorname{rank}_{\mathbb{Z}_p} H^0(G_{K,S}, \mathbb{Z}_p) - \operatorname{rank}_{\mathbb{Z}_p} H^1(G_{K,S}, \mathbb{Z}_p) + \operatorname{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p) = (r_1 + r_2) - [K : \mathbb{Q}] = -r_2$$

giving

$$Z = \operatorname{rank}_{\mathbb{Z}_p} H^1(G_{K,S}, \mathbb{Z}_p) = \operatorname{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p) + r_2 + 1$$

Let $\delta_K = \operatorname{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p) \geq 0$ in which case $Z = 1 + r_2 + \delta_K$. To prove the inequality $\delta_K \leq r_1 + r_2 - 1$ we need to show that $\operatorname{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p) \leq r_1 + r_2 - 1 = \operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K^\times$.

The Poitou-Tate sequence (Theorem 3.4) applied to $\mathbb{Z}/p^n\mathbb{Z}$ gives an exact sequence

$$H^1(G_{K,S}, \mathbb{Z}/p^n\mathbb{Z}) \to \oplus_{v \in S} H^1(K_v, \mathbb{Z}/p^n\mathbb{Z}) \to H^1(G_{K,S}, \mu_{p^n})^\vee \to$$

$$\to H^2(G_{K,S}, \mathbb{Z}/p^n\mathbb{Z}) \to \oplus_{v \in S} H^2(K_v, \mathbb{Z}/p^n\mathbb{Z}) \to H^0(G_{K,S}, \mu_{p^n})^\vee \to 0$$

Dualizing and using Tate duality to write $H^i(K_v, \mathbb{Z}/p^n\mathbb{Z})^\vee \cong H^{2-i}(K_v, \mu_{p^n})$ we get

$$\oplus_{v \in S} H^0(K_v, \mu_{p^n}) \to H^2(G_{K,S}, \mathbb{Z}/p^n\mathbb{Z})^\vee \to H^1(G_{K,S}, \mu_{p^n}) \to \oplus_{v \in S} H^1(K_v, \mu_{p^n})$$

Kummer theory gives $H^1(K_v, \mu_{p^n}) = K_v^\times/(K_v^\times)^{p^n}$ and taking projective limits one gets

$$\oplus_{v \in S} \varprojlim \mu_{p^n}(K_v) \to \varprojlim H^2(G_{K,S}, \mathbb{Z}/p^n\mathbb{Z})^\vee \to \varprojlim H^1(G_{K,S}, \mu_{p^n}) \to \oplus_{v \in S} \varprojlim H^1(K_v, \mu_{p^n})$$

The projective maps in $\oplus_{v \in S} \mu_{p^n}(K_v)$ are $x \mapsto x^p$ and since $\mu_{p^\infty}(K_v)$ is finite ($e_{K_v/\mathbb{Q}_p}$ is finite whereas $e_{\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p}$ is infinite) it follows that $\varprojlim \mu_{p^n}(K_v) = 0$. Using $A/A^n \cong A \otimes \mathbb{Z}/n\mathbb{Z}$ and Lemma 7.7 we obtain

$$0 \to \varprojlim H^2(G_{K,S}, \mathbb{Z}/p^n\mathbb{Z})^\vee \to \varprojlim H^1(G_{K,S}, \mu_{p^n}) \to \oplus_{v \in S} K_v^\times \otimes \mathbb{Z}_p$$

First, note that

$$\varprojlim H^2(G_{K,S}, \mathbb{Z}/p^n\mathbb{Z})^\vee = (\varinjlim H^2(G_{K,S}, \mathbb{Z}/p^n\mathbb{Z}))^\vee = H^2(G_{K,S}, \varinjlim \mathbb{Z}/p^n\mathbb{Z})^\vee = H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee$$

and so

$$0 \to H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \to \varprojlim H^1(G_{K,S}, \mu_{p^n}) \to \oplus_{v \in S} K_v^\times \otimes \mathbb{Z}_p$$

For the next step, we need a little notation. Let $E_S = \varinjlim_{L \subset K_S} \mathcal{O}_{L,S}^\times$, $J_S = \varinjlim_{L \subset K_S} \prod_{v|S} L_v^\times$ and let $C_S = \varinjlim_{L \subset K_S} \prod_{v|S} L_v^\times/\mathcal{O}_{L,S}^\times$. It is a classical computation in global class field theory (see [NSW08, 8.3.8] or [Mil13, Theorem 5.1]) that $H^0(G_{K,S}, C_S) = \mathbb{A}_K^\times/K^\times \prod_{v \notin S} \mathcal{O}_{K_v}^\times$. The $G_{K,S}$ cohomology sequence for $1 \to E_S \to J_S \to C_S \to 1$ gives

$$H^0(G_{K,S}, J_S) \to H^0(G_{K,S}, C_S) \to H^1(G_{K,S}, E_S) \to H^1(G_{K,S}, J_S)$$

Hilbert 90 gives $H^1(G_{K,S}, J_S) = 0$ and so

$$H^1(G_{K,S}, E_S) \cong \mathbb{A}_K^\times/K^\times \prod_{v \in S} K_v^\times \prod_{v \notin S} \mathcal{O}_{K_v}^\times \cong \mathrm{Cl}_S(K)$$

Since S contains the places of K above p the sequence

$$1 \to \mu_{p^n} \to E_S \to E_S \to 1$$

is exact. Indeed, if $\alpha \in E_S$ then $\alpha \in \mathcal{O}_{L,S}^\times$ for some $L \subset K_S$ and $K(\sqrt[p^n]{\alpha})/K$ will be unramified at places away from S and so $M = K(\sqrt[p^n]{\alpha}) \subset K_S$. Necessarily then $\sqrt[p^n]{\alpha} \in \mathcal{O}_{M,S}^\times$ where $M \subset K_S$.

Now Kummer theory gives

$$0 \to \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^{p^n} \to H^1(G_{K,S}, \mu_{p^n}) \to H^1(G_{K,S}, E_S)[p^n] \to 0$$

where $H^1(G_{K,S}, E_S)[p^n] = \mathrm{Cl}_S(K)[p^n]$. Taking projective limits as $n \to \infty$ one gets

$$0 \to \varprojlim \mathcal{O}_{K,S}^\times \otimes \mathbb{Z}/p^n\mathbb{Z} \to \varprojlim H^1(G_{K,S}, \mu_{p^n}) \to \varprojlim \mathrm{Cl}_S(K)[p^n]$$

and since $\varprojlim A[p^n] = 0$ for any finite group A it follows that, using Lemma 7.7,

$$\mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p \cong \varprojlim H^1(G_{K,S}, \mu_{p^n})$$

Plugging this back into the exact sequence above yields

$$0 \to H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \to \mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p \to \oplus_{v \in S} K_v^\times \otimes \mathbb{Z}_p$$

Consider the exact sequence

$$0 \to \mathcal{O}_K^\times \to \mathcal{O}_{K,S}^\times \to \oplus_{v \in S - \infty} K_v^\times/\mathcal{O}_v^\times \to \mathrm{Cl}(K) \to \mathrm{Cl}_S(K) \to 0$$

Since $\mathbb{Z}_p$ is flat over $\mathbb{Z}$ we get after tensoring

$$0 \to \mathcal{O}_K^\times \otimes \mathbb{Z}_p \to \mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p \to \oplus_{v \in S - \infty} K_v^\times/\mathcal{O}_v^\times \otimes \mathbb{Z}_p$$

Now $c \in H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ maps via $\mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p$ to 0 in $\oplus_{v \in S} K_v^\times \otimes \mathbb{Z}_p$ and so to 0 in $\oplus_{v \in S - \infty} K_v^\times/\mathcal{O}_v^\times \otimes \mathbb{Z}_p$. But then the image of c in $\mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p$ lies in fact in $\mathcal{O}_K^\times \otimes \mathbb{Z}_p$.

Now

$$\begin{aligned} \mathrm{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee &\leq \mathrm{rank}_{\mathbb{Z}_p} \mathcal{O}_K^\times \otimes \mathbb{Z}_p \\ &\leq \mathrm{rank}_{\mathbb{Z}} \mathcal{O}_K^\times \\ &= r_1 + r_2 - 1 \end{aligned}$$

but at the same time if we write $H^2(G_{K,S}, \mathbb{Z}_p) = \mathbb{Z}_p^r \oplus X$ where X is finite torsion and $r = \mathrm{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p)$ then

$$\begin{aligned} \mathrm{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee &= \mathrm{rank}_{\mathbb{Z}_p}(H^2(G_K, \mathbb{Z}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \\ &= \mathrm{rank}_{\mathbb{Z}_p}((\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus (X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p))^\vee \\ &= \mathrm{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p) \end{aligned}$$

since $X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p = 0$ and $(\mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \mathbb{Z}_p$. Therefore $\mathrm{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p) \leq r_1 + r_2 - 1$ as desired. □

Remark 2. Given that $\delta_K = \mathrm{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p)$ another formulation of Leopoldt's conjecture is that $\mathrm{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p) = 0$.

Lecture 16
2013-05-08

7.2 Class groups and Galois modules

Lemma 7.9. *Let K_∞/K be a $\mathbb{Z}_p$ extension of a number field. There exists $m \geq 0$ such that K_∞/K_m is totally ramified at all places of ramification.*

Proof. We already know from Proposition 7.8 that K_∞/K can ramify only at the places $v_1, \ldots, v_r$ of K above p. Fixing a place w_i of K_∞ above v_i (since K_∞/K is Galois any will do) let $I_i = I_{K_{\infty,w_i}/K_{v_i}}$. Now $\cap I_i$ is an open subgroup of $G_{K_\infty/K} \cong \mathbb{Z}_p$ and so is of the form $p^m\mathbb{Z}_p \cong G_{K_\infty/K_m}$ for some m. Suppose that $w \mid t \mid v$ are places of K_∞, K_m, K. Then $G_{K_{\infty,w}/K_{m,t}} \subset G_{K_\infty/K_m} \subset I_v$. But then Herbrandt's theorem gives $I_{K_{\infty,w}/K_{m,t}} = I_v \cap G_{K_{\infty,w}/K_{m,t}} = G_{K_{\infty,w}/K_{m,t}}$ and so $K_{\infty,w}/K_{m,t}$ is totally ramified. □

Remark 3. If $K_0 = \mathbb{Q}(\sqrt{-6})$ and $K_1 \subset K_\infty$, the $\mathbb{Z}_2$-extension, with $G_{K_1/K_0} \cong \mathbb{Z}/2\mathbb{Z}$ then $K_1 = K_0(\sqrt{2})$ is unramified over K_0. (This is [Was97, Exercise 13.3].)

Definition 7.10. Let L_n/K_n be the maximal abelian extension of K_n which is unramified at all finite places and has p-power order. This is a subextension of the Hilbert class field fixed by the prime to p part of $\mathrm{Cl}(K_n)$. Let $L_\infty = \cup L_n$. In this case

$$v_p(h_{K_n}) = v_p([L_n : K_n]) = \log_p[L_n : K_n]$$

Lemma 7.11. *The Galois group $X_n = G_{L_n/K_n} \cong \mathrm{Cl}(K_n)$ carries an action of $G_{K_n/K}$ by letting $g \cdot \sigma = \widetilde{g}\sigma\widetilde{g}^{-1}$ for $g \in G_{K_n/K}$, $\sigma \in X_n$ and $\widetilde{g}$ any lift of g to $G_{L_n/K}$.*

Proof. First, any other lift of g to $G_{L_n/K}$ is of the form $\widetilde{g}h$ for $h \in G_{L_n/K_n} \subset G_{L_n/K}$. Then

$$\begin{aligned}\widetilde{g}h\sigma(\widetilde{g}h)^{-1} &= \widetilde{g}h\sigma h^{-1}\widetilde{g}^{-1} \\ &= \widetilde{g}\sigma\widetilde{g}^{-1}\end{aligned}$$

since $h, \sigma \in X_n$ which is an abelian group by definition. Therefore the action is independent of the choice of lift. Finally, if $g, h \in G_{K_n/K}$ then $\widetilde{g}\widetilde{h}$ is a choice of lift of gh and so

$$\begin{aligned}g \cdot (h \cdot \sigma) &= \widetilde{g}\widetilde{h}\sigma\widetilde{h}^{-1}\widetilde{g}^{-1} \\ &= \widetilde{g}\widetilde{h}\sigma(\widetilde{g}\widetilde{h})^{-1} \\ &= \widetilde{gh}\sigma\widetilde{gh}^{-1} \\ &= (gh) \cdot \sigma\end{aligned}$$

and so this is indeed a group action. □

Lemma 7.12. *Let $v_1, \ldots, v_s$ be the places of K_m above p that ramify (necessarily totally) in K_∞ and let $w_i \mid v_i$ be any place of L_∞. If $I_{m,i} = I_{L_{\infty,w_i}/K_{m,v_i}}$ then $G_{L_\infty/K_m} \cong X_\infty I_{m,i}$ for all i.*

Proof. Since L_∞/K_∞ is unramified it follows that $I_{m,i} \cap X_\infty = 1$. Therefore $I_{m,i} \hookrightarrow G_{L_\infty/K_m}/X_\infty \cong G_{K_\infty/K_m}$. Denote by $I_{m,i}$ as well the image of $I_{m,i}$ in G_{K_∞/K_m}. The subextension K_m was chosen such that $I_{K_{\infty,u_i}/K_{m,v_i}} = G_{K_{\infty,u_i}/K_{m,v_i}}$ where u_i is the place of K_∞ below w_i. The decomposition group $G_{K_{\infty,u_i}/K_{m,v_i}} \subset G_{K_\infty/K_m}$ is an open subgroup and so it is of the form $G_{K_\infty/K_{n_i}}$ for some $n_i \geq m$. But by choice of K_m, $G_{K_\infty/K_m} = \cap I_{m,i}$ and so $G_{K_\infty,K_m} = \cap G_{K_\infty/K_{n_i}}$ which implies that $\min n_i = m$. But G_{K_∞/K_m} acts transitively on the places v_i and so $n_i = m$ for all i proving that $I_{m,i} \cong G_{K_\infty/K_m}$. Finally this implies that $G_{L_\infty/K_m} \cong X_\infty I_{m,i}$. □

Lemma 7.13. *Let γ_0 be a topological generator of $G_{K_\infty/K} \cong \mathbb{Z}_p$ in which case $\gamma_m = \gamma_0^{p^m}$ is a topological generator of $G_{K_\infty/K_m} \cong p^m\mathbb{Z}_p$. Then*

$$[G_{L_\infty/K_m}, G_{L_\infty/K_m}] = (\gamma_m - 1) \cdot X_\infty$$

where the action of G_{K_∞/K_m} on $X_\infty = \varprojlim X_n = G_{L_\infty/K_\infty}$ is defined in Lemma 7.11.

Proof. Identify $I_{m,1} \cong G_{K_\infty/K_m}$ in which case we denote by γ_m the lift to $I_{m,1}$ as well. Then $\gamma_m \cdot x = \gamma_m x \gamma_m^{-1}$. If $g_1, g_2 \in G_{L_\infty/K_m} = I_{m,1}X_\infty$ then may write $g_i = h_i x_i$ for $h_i \in G_{K_\infty/K_m}$ and $x_i \in X_\infty$ and it is easy to check (using that $I_{m,1}$ and X_∞ are abelian) that

$$g_1 g_2 g_1^{-1} g_2^{-1} = ((1-h_2)h_1 \cdot x_1)((h_1 - 1)h_2 \cdot x_2)$$

Taking $h_1 = \gamma_m$ and $h_2 = 1$ gives $(\gamma_m - 1) \cdot x_2 = g_1 g_2 g_1^{-1} g_2^{-1}$ and so $(\gamma_m - 1) \cdot X_\infty \subset [G_{L_\infty/K_m}, G_{L_\infty/K_m}]$.

Going in the other direction, if $\gamma \in G_{K_\infty/K_m}$ then $\gamma = \gamma_m^\alpha$ for some $\alpha \in \mathbb{Z}_p$. Then

$$\gamma - 1 = ((\gamma_m - 1) + 1)^\alpha - 1 = \sum_{n \geq 1} \binom{\alpha}{n} (\gamma_m - 1)^n$$

and so $(1-h_2)h_1 \cdot x_1, (1-h_1)h_2 \cdot x_2 \in (\gamma_m - 1) \cdot X_\infty$. We deduce that $[G_{L_\infty/K_m}, G_{L_\infty/K_m}] \subset (\gamma_m - 1) \cdot X_\infty$ and equality follows. □

Lemma 7.14. *Let $\sigma_{m,i} \in I_{m,i}$ be the image of $\gamma_m \in G_{K_\infty/K_m} \cong I_{m,i}$. Since $I_{m,i} \subset G_{L_\infty/K_m} = X_\infty I_{m,i}$ there exists $g_{m,i} \in X_\infty$ such that $\sigma_{m,i} = g_{m,i}\sigma_{m,1}$. Let $Y_m \subset X_\infty$ be the $\mathbb{Z}_p$-submodule generated by $g_{m,2}, \ldots, g_{m,s}$ and $(\gamma_m - 1)X_\infty$. Then*

$$X_n = X_\infty / \nu_{n,m} \cdot Y_m$$

where $\nu_{n,m} = 1 + \gamma_m^2 + \cdots + \gamma_m^{p^{n-m}-1}$. (Here the action of $\nu_{n,m}$ on $Y_m \subset X_\infty$ is that defined in Lemma 7.11.)

Proof. By definition L_n is the maximal abelian unramified p-extension of K_n while L_∞ is some p-extension of K_n. Therefore L_n is the maximal abelian unramified subextension of L_∞. Translating to Galois groups, G_{L_∞/L_n} is generated by the commutant $[G_{L_\infty,K_n}, G_{L_\infty/K_n}]$ (to make L_n/K_n abelian) and $I_{n,i}$ (to make L_n/K_n unramified).

Note that $\sigma_{n,i} = \sigma_{m,i}^{p^{n-m}}$ so

$$\begin{aligned}
\sigma_{n,i} &= \sigma_{m,i}^{p^{n-m}} \\
&= (g_{m,i}\sigma_{m,1})^{p^{n-m}} \\
&= \prod_{k=0}^{p^{n-m}-1} (\sigma_{m,1}^k g_{m,i} \sigma_{m,1}^{-k}) \sigma_{m,1}^{p^{n-m}} \\
&= \prod_{k=0}^{p^{n-m}-1} (\gamma_m^k \cdot g_{m,i}) \sigma_{m,1}^{p^{n-m}} \\
&= (\nu_{n,m} \cdot g_{m,i}) \sigma_{n,1}
\end{aligned}$$

where the fourth equality is by definition of the action $\gamma_m \cdot -$ since $\sigma_{m,1}$ is a lift of γ_m to $G_{L_\infty/K}$. We conclude that $g_{n,i} = \nu_{n,m} \cdot g_{m,i}$.

Now

$$\begin{aligned}
X_n &= G_{L_n/K_n} \\
&= G_{L_\infty/K_n}/G_{L_\infty/L_n} \\
&= X_\infty I_{n,1} / \langle [G_{L_\infty/K_n}, G_{L_\infty/K_n}], I_{n,1}, \ldots, I_{n,s} \rangle \\
&= X_\infty I_{n,1} / \langle [G_{L_\infty/K_n}, G_{L_\infty/K_n}], I_{n,1}, g_{n,2}, \ldots, g_{n,s} \rangle \\
&= X_\infty / \langle [G_{L_\infty/K_n}, G_{L_\infty/K_n}], g_{n,2}, \ldots, g_{n,s} \rangle \\
&= X_\infty / \langle (\gamma_n - 1) \cdot X_\infty, g_{n,2}, \ldots, g_{n,s} \rangle
\end{aligned}$$

where the third equality uses Lemma 7.12 and the sixth equality uses Lemma 7.13. Finally, Y_n is generated by $(\gamma_n - 1) \cdot X_\infty = \nu_{n,m}(\gamma_m - 1) \cdot X_\infty$ and $g_{n,i} = \nu_{n,m} \cdot g_{m,i}$ and so $Y_n = \nu_{n,m} \cdot Y_m$ giving

$$X_n = X_\infty / \nu_{n,m} \cdot Y_m$$

□

7.3 The Iwasawa algebra

Recall that our goal is Theorem 7.1 where we study $v_p(|X_n|)$ where X_n is a quotient of X_∞. To study the cardinality of X_n as $n \to \infty$ we need to study X_∞ as a module over $G_{K_\infty/K}$. In fact we will show that X_∞ is a module over $\mathbb{Z}_p[\![T]\!]$, we will study finitely generated modules over $\mathbb{Z}_p[\![T]\!]$ and we will deduce the theorem from a structure theorem.

We begin by collecting some facts, with brief sketches of proofs, about power series rings. Throughout $L/\mathbb{Q}_p$ is a finite extension.

Lemma 7.15 (Division with remainder)**.** *If $f, g \in \mathcal{O}_L[\![T]\!]$ such that $f(T) = a_0 + a_1 T + \cdots$ with $a_i \in \mathfrak{m}_L$ for $0 \leq i \leq n-1$ and $a_n \in \mathcal{O}_L^\times$ then one may uniquely write*

$$g = qf + r$$

for a power series $q \in \mathcal{O}_L[\![T]\!]$ and a polynomial $r \in \mathcal{O}_L[T]$ of degree $< n$.

Proof. Write $U(T) = a_n + a_{n+1}T + \cdots$ and for a uniformizer ϖ_L of L, let $P = \varpi_L^{-1}(f - UT^n)$, a polynomial of degree $< n$. Consider the linear operator

$$\tau(\sum_{i=0}^{\infty} b_i T^i) = \sum_{i=n}^{\infty} a_i T^{i-n}$$

and the multiplication by P/U operator $m_{P/U}$. If

$$q(T) = U(T)^{-1} \sum_{i=0}^{\infty} (-1)^i \varpi_L^i (\tau \circ m_{P/U})^i \circ \tau(g)$$

then one may check that this series converges and that $g = qf + r$ for a polynomial r of degree $< n$. For details see [Was97, Proposition 7.2]. □

Definition 7.16. A polynomial $P \in \mathcal{O}_L[T]$ is said to be distinguished if it is of the form $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ with $a_i \in \mathfrak{m}_L$.

Lemma 7.17 (Weierstrass preparation)**.** *Let $f \in \mathcal{O}_L[\![T]\!]$ such that $f(T) = a_0 + a_1 T + \cdots$ with $a_i \in \mathfrak{m}_L$ for $0 \leq i \leq n-1$ and $a_n \in \mathcal{O}_L^\times$. Then one may write f uniquely as $f(T) = P(T)U(T)$ where $U \in (\mathcal{O}_L[\![T]\!])^\times$ and $P \in \mathcal{O}_L[T]$ is a distinguished polynomial of degree n.*

Proof. By Lemma 7.15 it follows that $T^n = q(T)f(T) + r(T)$ for a polynomial r of degree $< n$. Modulo $\mathfrak{m}_L$ have $f(T) \equiv a_n T^n + O(T^{n+1})$ and so

$$T^n - r(T) = q(T)f(T) \equiv q(T)(a_n T^n + O(T^{n+1})) \pmod{\mathfrak{m}_L}$$

which implies that $r(T) \equiv 0 \pmod{\mathfrak{m}_L}$. Let $P(T) = T^n - r(T)$ of degree n and distinguished. Reducing modulo the ideal $(\mathfrak{m}_L, T^{n+1})$ the above equation becomes $T^n \equiv a_n q(0) T^n$ and so $q(0) \neq 0$ which means that $q \in (\mathcal{O}_L[\![T]\!])^\times$ and let $U(T) = q(T)^{-1}$. Finally $f(T) = P(T)U(T)$.

If $f = PU$ then $T^n = U(T)^{-1}f(T) + r(T)$ and uniqueness of P and U follows from the uniqueness statement of Lemma 7.15. □

Corollary 7.18. *If $f \in \mathcal{O}_L[\![T]\!]$ then $(f) = (\varpi_L^n P)$ for a distinguished polynomial P.*

Proof. Let n be the largest exponent such that $f \equiv 0 \pmod{\mathfrak{m}_L^n}$. Then $P = f\varpi_L^{-n}$ will satisfy the hypothesis of Lemma 7.17 and so $f = \varpi_L^n PU$ for a unit U. □

Definition 7.19. If G is a profinite group and $L/\mathbb{Q}_p$ a finite extension then the completed group ring $\mathcal{O}_L[\![G]\!]$ is defined as

$$\mathcal{O}_L[\![G]\!] = \varprojlim \mathcal{O}_L[G/H]$$

where $H \subset G$ runs through the open normal subgroups of G. The ring $\mathcal{O}_L[\![G]\!]$ is called the Iwasawa algebra of G.

Proposition 7.20. *Let $G \cong \mathbb{Z}_p$ be topologically generated by γ and let $L/\mathbb{Q}_p$ be a finite extension. Then $\gamma \mapsto 1+T$ yields an isomorphism*

$$\mathcal{O}_L[\![G]\!] \cong \mathcal{O}_L[\![T]\!]$$

Proof. The open normal subgroups of G are of the form $H = p^n\mathbb{Z}_p$ so we have $\mathcal{O}_L[G/H] = \mathcal{O}_L[\mathbb{Z}/p^n\mathbb{Z}] \cong \mathcal{O}_L[T]/((1+T)^{p^n}-1)$ by sending the generator of $\mathbb{Z}/p^n\mathbb{Z}$ to $1+T$. Therefore

$$\mathcal{O}_L[\![G]\!] \cong \varprojlim \mathcal{O}_L[T]/((1+T)^{p^n}-1)$$

It suffices to show that

$$\mathcal{O}_L[\![T]\!] \cong \varprojlim \mathcal{O}_L[T]/((1+T)^{p^n}-1)$$

Let $P_n(T) = (1+T)^{p^n}-1$. It is easy to see that $P_{n+1}/P_n \in (\mathfrak{m}_L, T)$ and so $P_n \in (\mathfrak{m}_L, T)^{n+1}$ by induction. Let $f \in \mathcal{O}_L[\![T]\!]$. Lemma 7.15 produces a power series q_n and a polynomial f_n of degree $< p^n$ such that

$$f(T) = q_n(T)P_n(T) + f_n(T)$$

in which case $f_m \equiv f_n \pmod{P_n}$ for all $m \geq n$. This provides a map $f \mapsto (f_n)$ from $\mathcal{O}_L[\![T]\!]$ to $\varprojlim \mathcal{O}_L[T]/(P_n(T))$. Finally, $\cap(P_n(T)) \subset \cap(\mathfrak{m}_L, T)^{n+1} = 0$ and so this map is injective.

Now for surjectivity, suppose that $(f_n) \in \varprojlim \mathcal{O}_L[T]/(P_n(T))$. Since $(P_n(T)) \subset (\mathfrak{m}_L, T)^{n+1}$, it follows that for $m \geq n$ we have $f_m \equiv f_n \pmod{(\mathfrak{m}_L, T)^{n+1}}$. But $\mathcal{O}_L[\![T]\!]$ is complete for the $(\mathfrak{m}_L, T)$-adic topology and so there exists $f \in \mathcal{O}_L[\![T]\!]$ such that $f \equiv f_n \pmod{(\mathfrak{m}_L, T)^{n+1}}$. It remains to show that in fact $f \equiv f_n \pmod{P_n(T)}$. By definition there exists $q_{m,n} \in \mathcal{O}_L[T]$ such that $f_m - f_n = q_{m,n}P_n$. In the $(\mathfrak{m}_L, T)$-adic topology of $\mathcal{O}_L[\![T]\!]$ we have

$$\frac{f-f_n}{P_n} = \lim_m \frac{f_m - f_n}{P_n} = \lim_m q_{m,n}$$

which, being a limit of polynomials, must be a power series in $\mathcal{O}_L[\![T]\!]$ if the sequence converges. (Here we may use that $\mathcal{O}_L[\![T]\!]$ is closed in its fraction field. Writing $q_n = \lim_m q_{m,n}$ get $f = q_nP_n + f_n$ as desired. □

Lecture 18
2013-05-13

7.4 Modules over the Iwasawa algebra

Definition 7.21. The Iwasawa algebra is $\Lambda = \mathcal{O}_L[\![T]\!]$.

Lemma 7.22 (Nakayama)**.** *Suppose X is a compact topological Λ-module. Then X is finitely generated if and only if $X/(\mathfrak{m}_L, T)X$ is finite.*

Proof. See for instance [Was97, Lemma 13.16]. □

Definition 7.23. Let M, N be two Λ-modules. Say $M \sim N$ if there exists a morphism of modules $M \to N$ with finite kernel and cokernel.

Lemma 7.24. *Let $L/\mathbb{Q}_p$ be a finite extension.*

1. *If $f, g \in \Lambda$ are coprime then (f, g) is finite index in Λ.*
2. *The prime ideals of Λ are 0, $\mathfrak{m}_L$, $(\mathfrak{m}_L, T)$ and $(P(T))$ where $P \in \mathcal{O}_L[T]$ is irreducible and distinguished. The prime ideal $(\mathfrak{m}_L, T)$ is the unique maximal ideal.*

3. *If $f \in \Lambda$ such that f is not a unit then $\Lambda/(f)$ is infinite.*

4. *If M is a finitely generated Λ module then*

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(\varpi_L^{n_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\right)$$

for distinguished irreducible polynomials f_j.

Proof. The first part. Corollary 7.18 implies that we may choose f, g to be products of powers of ϖ_L and distinguished polynomials or else $(f, g) = \Lambda$. Since f, g are coprime, without loss of generality assume $\varpi_L \nmid f$. Let $h \in (f, g)$ be a polynomial of minimal degree. Write $h = \varpi_L^n \ell$ with ℓ either 1 or a distinguished polynomial. If $\ell \neq 1$ then $f = q\ell + r$ for $\deg r < \deg \ell = \deg h$ gives $\varpi_L^n r \in (f, g)$ a polynomial of smaller degree than h. Thus $h = \varpi_L^n \in (f, g)$. Now $(\varpi_L^n, f) = (h, f) \subset (f, g)$ and so $\Lambda/(f, h) \twoheadrightarrow \Lambda/(f, g)$. But $\Lambda/(f, h) = \Lambda/(\varpi_L^n, f) \cong (\mathcal{O}_L/\mathfrak{m}_L^n)[\![T]\!]/(f)$ which consists of polynomials of degree $< \deg f$ and coefficients in $\mathcal{O}_L/\mathfrak{m}_L^n$ and therefore is finite.

The second part. The ideals listed are prime. Suppose $\mathfrak{p}$ is a proper prime ideal. By Corollary 7.18 every non-unit in $\mathfrak{p}$ is a polynomial. Let $f \in \mathfrak{p}$ be a polynomial of minimal degree. If $\varpi_L \in \mathfrak{p}$ then $\mathfrak{p}/\varpi_L$ is a prime ideal of $k_L[\![T]\!]$ which is a PID with maximal ideal T and so $\mathfrak{p} = (\varpi_L)$ or $\mathfrak{p} = (\varpi_L, T)$. Suppose $\varpi_L \notin \mathfrak{p}$. If $\mathfrak{p} \neq (f)$ then there exists $g \in \mathfrak{p} - (f)$ necessarily coprime to f. Then $\mathfrak{p} \supset (f, g)$ will have finite index in Λ by the first part. But then $\varpi_L^n \in \mathfrak{p}$ for some n contradicting the assumption that $\varpi_L \notin \mathfrak{p}$.

The third part. Since we care about the ideal (f), by Corollary 7.18, $(f) = (\varpi_L^n g)$ where $g = 1$ or g is a distinguished polynomial. If $n > 0$ then $(f) \subset (\varpi_L)$ and so $\Lambda/(f) \twoheadrightarrow k_L[\![T]\!]$ which is infinite. If $n = 0$ then $g \neq 1$ is a distinguished polynomial and no two elements in $\mathcal{O}_L$ can be equal in $\Lambda/(f)$ so the quotient is infinite.

The fourth part is a big exercise in linear algebra in the style of the classification of finitely generated modules over PIDs. See for instance [Was97, Theorem 13.12]. □

Lemma 7.25. *Let $M \sim N$ as Λ-modules and let $f_n \in \Lambda$ such that each $M/f_n M$ is finite. Then each $N/f_n N$ is finite and*

$$v_p(|M/f_n M|) = v_p(|N/f_n N|) + C(1)$$

where the notation $C(1)$ is taken to mean constant for $n >> 0$.

Proof. Unenlightening exercise in using the snake lemma. See [Was97, Lemma 13.21]. □

7.5 Class numbers in $\mathbb{Z}_p$-extensions

Lemma 7.26. *Let K_∞/K be a $\mathbb{Z}_p$ extension of a number field K. Let X_∞ be as defined in Lemma 7.13. Then Y_m and X_∞ are finitely generated $\mathbb{Z}_p[\![T]\!]$-modules.*

Proof. The group X_n carries an action of $\mathbb{Z}_p[G_{K_n/K}]$ and thus $X_\infty = \varprojlim X_n$ carries an action of $\varprojlim \mathbb{Z}_p[G_{K_n/K}] = \mathbb{Z}_p[\![G_{K_\infty/K}]\!] \cong \mathbb{Z}_p[\![T]\!]$ by Proposition 7.20.

Recall that $\mathbb{Z}_p[\![G_{K_\infty/K}]\!] \cong \mathbb{Z}_p[\![T]\!]$ sending $\gamma_0 \mapsto T + 1$. Let m be as in Lemma 7.9. By definition for $n > m$ we have

$$\nu_{n,m} = \frac{\gamma_n - 1}{\gamma_m - 1} = \sum_{i=0}^{p^{n-m}-1} (1+T)^{ip^m} \in (p, T) \subset \Lambda$$

and so by Lemma 7.14

$$Y_m/(p, T)Y_m \cong Y_m/\nu_{n,m} \cdot Y_m \subset X_\infty/\nu_{n,m} \cdot Y_m \cong X_n$$

is finite. By Lemma 7.22 we deduce that Y_m is finitely generated. Finally, $X_\infty/Y_m \cong X_m$ is finite and so X_∞ is finitely generated. □

Proof of Theorem 7.1. We will show that there exist nonnegative integers μ, λ, ν such that for $n >> 0$

$$v_p(h_{K_n}) = v_p(|X_n|) = \lambda n + \mu p^n + \nu$$

in other words that

$$v_p(|X_n|) = \lambda n + \mu p^n + C(1)$$

Note that $0 \to Y_m \to X_\infty \to X_\infty/Y_m \to 0$ where $X_\infty/Y_m \cong X_m$ is finite; therefore $Y_m \sim X_\infty$ which shows that $Y_m/\nu_{n,m} \cdot Y_m \sim X_\infty/\nu_{n,m} \cdot Y_m \cong X_n$. By Lemma 7.25 it suffices to show that

$$v_p(|Y_m/\nu_{n,m}Y_m|) = \lambda n + \mu p^n + C(1)$$

Lemma 7.26 shows that Y_m is a finitely generated Λ-module and so by Lemma 7.24 implies that

$$Y_m \cong \Lambda^r \oplus \left(\bigoplus \Lambda/(p^{n_i})\right) \oplus \left(\bigoplus \Lambda/(f_j^{m_j})\right)$$

First, note that $Y_m/\nu_{n,m}Y_m$ is finite but $\nu_{n,m} \in (p, T)$ it is not a unit and therefore $\Lambda/\nu_{n,m}$ is infinite by Lemma 7.24. This implies that $r = 0$.

Now

$$v_p(|Y_m/\nu_{n,m}Y_m|) = \sum v_p(|\Lambda/(p^{n_i}, \nu_{n,m})|) + \sum v_p(|\Lambda/(f_j^{m_j}, \nu_{n,m})|)$$

is a finite sum so it is enough to show that for each direct summand M of Y_m one has

$$v_p(|M/\nu_{n,m}M|) = \lambda_M n + \mu_M p^n + C(1)$$

where $\lambda_M, \mu_M \in \mathbb{Z}_{\geq 0}$.

Suppose $M = \Lambda/(p^k)$. Then $M/\nu_{n,m}M = \Lambda/(p^k, \nu_{n,m})$ consists, using the division algorithm of Lemma 7.15 as $\deg \nu_{n,m} = p^n - p^m$, of polynomials of degree $< p^n - p^m$ with coefficients in $\mathbb{Z}/p^k\mathbb{Z}$. Therefore $|M/\nu_{n,m}M| = p^{k(p^n - p^m)}$ and so $v_p(|M/\nu_{n,m}M|) = kp^n + C(1)$ as desired.

Now suppose that $M = \Lambda/(f^r)$ where f is distinguished and therefore $g = f^r$ of degree d is also distinguished. If $k \geq d$, the division algorithm gives $T^k = q(T)g(T) + r(T)$ with $\deg r < d$. Modulo p, $g =\equiv T^d$ and so $T^k \equiv qT^d + r$ which implies that $r \equiv 0 \pmod p$ and so $T^k \equiv p\mathbb{Z}_p[T] \pmod g$. If $p^n > d$ then $(1+T)^{p^n} \equiv 1 + p\mathbb{Z}_p[T] \pmod g$ and so by induction $(1+T)^{p^{n+k}} \equiv 1 + p^k\mathbb{Z}_p[T] \pmod g$. Let $n_0 \geq m$ such that $p^n > d$. If $n \geq n_0$, $p^n > d$ and $k \geq 1$ then

$$P_{n+k+1} = P_{n+k}\left(\sum_{i=0}^{p-1}(1+T)^{p^{n+k}i}\right) \equiv P_{n+k}\sum_{i=0}^{p-1}(1+p^k\mathbb{Z}_p[T])^i \pmod g \equiv P_{n+k}p(1+p\mathbb{Z}_p[T]) \pmod g$$

where recall that $P_k(T) = (1+T)^{p^k} - 1$. But $1 + p\mathbb{Z}_p[T]$ is invertible in Λ and so in $\Lambda/(g)$, $\nu_{n+k+1,n+k} = P_{n+k+1}/P_{n+k}$ acts (up to a unit) by multiplication by p.

Now g is distinguished so $p \nmid g$ and therefore multiplication by p is injective on $M = \Lambda/(g)$. Therefore

$$\begin{aligned}
|M/\nu_{n,m}M| &= |M/\nu_{n,n-1}\cdots\nu_{n_0+2,n_0+1}\nu_{n_0+1,m}M| \\
&= |M/p^{n-n_0-1}\nu_{n_0+1,m}M| \\
&= |M/p^{n-n_0-1}M||p^{n-n_0-1}M/p^{n-n_0-1}\nu_{n_0+1,m}M| \\
&= |M/p^{n-n_0-1}M||M/\nu_{n_0+1,m}M| \\
&= |\Lambda/(p^{n-n_0-1}, g)||M/\nu_{n_0+1,m}M| \\
&= |(\mathbb{Z}/p^{n-n_0-1}\mathbb{Z})[T]/(g)||M/\nu_{n_0+1,m}M| \\
&= p^{d(n-n_0-1)}|M/\nu_{n_0+1,m}M|
\end{aligned}$$

This implies that

$$v_p(|M/\nu_{n,m}M|) = d(n - n_0 - 1) + v_p(|M/\nu_{n_0+1,m}M|) = dn + C(1)$$

□

Remark 4. It is a theorem of Ferrero and Washington that if $K/\mathbb{Q}$ is abelian Galois then $\mu = 0$. In general, if K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension then it is expected that $\mu = 0$.

Lecture 19
2013-05-15

---

8 Hecke theory for GL(1)

Hecke theory refers to the study of L-functions attached to various arithmetic or analytic objects and their functional equations. It is worth spending a little time understanding what the point is, as the results are fairly technical.

Suppose K is a number field and $\rho : G_K \to \mathrm{GL}(n, \mathbb{C})$ be a continuous Galois representation. One defines the L-function of ρ as

$$L(\rho, s) = \prod_{v \nmid \infty} \det(1 - \rho(\mathrm{Frob}_v) q_v^{-s} | \rho^{I_{K_v}})^{-1}$$

which is an analytic function for $\mathrm{Re}\, s >> 0$. However, a priori, it is not known what kind of behavior L has on $\mathbb{C}$. Is it meromorphic? Analytic? Does it have a functional equation?

The strategy for tackling these questions is to find an analytic construction of the L-function in a context where these questions can be answered naturally using Fourier transforms. Hecke theory for GL(1) is the topic of Tate's thesis, whose main results we explain, without detailed proofs.

8.1 Fourier analysis

8.1.1 Measures

Let G be a locally compact topological abelian group and let μ_G be a Haar measure. Let $\widehat{G} = \mathrm{Hom}(G, S^1)$ be the space of continuous characters. Then G is compact if and only if $\widehat{G}$ is discrete and $\widehat{\widehat{G}} \cong G$. If $H \subset G$ is a closed subgroup then $\widehat{G/H} \cong H^\perp = \{\phi \in \widehat{G} | \phi(H) = 1\}$ and $\widehat{G}/H^\perp \cong \widehat{H}$. There exists a unique Haar measure μ_G/μ_H on G/H such that for every $\phi \in C_c(G)$ with compact support

$$\int_G \phi(g) d\mu_{G,g} = \int_{G/H} \left(\int_H \phi(gh) d\mu_{H,h} \right) d(\mu_G/\mu_H)_g$$

If $G = \prod'_{\{U_v\}} G_v$ is a restricted product with respect to the open subgroups $U_v \subset G_v$ then $\widehat{G} \cong \prod'_{\{U_v^\perp\}} \widehat{G}_v$. If μ_v is a Haar measure for U_v such that for almost all v, $\mu_v(U_v) = 1$ then $\mu = \otimes \mu_v$ is a Haar measure for $\prod'_{\{U_v\}} G_v$.

8.1.2 Fourier transforms for abelian groups

For a Haar measure μ on G the Fourier transform $\mathcal{F}_\mu : L^1(G, \mu) \to C(\widehat{G})$ defined by

$$\mathcal{F}_\mu(\phi)(\chi) = \int_G \phi(g) \chi(g) d\mu_g$$

extends by continuity to $\mathcal{F}_\mu : L^2(G, \mu) \to L^2(\widehat{G}, \widehat{\mu})$ for the unique (dual) Haar measure $\widehat{\mu}$ on $\widehat{G}$ such that for every $\phi \in C_c(G)$,

$$\int_G |\phi|^2 d\mu = \int_{\widehat{G}} |\mathcal{F}_\mu(\phi)|^2 d\widehat{\mu}$$

Then $\mathcal{F}_{\widehat{\mu}} \mathcal{F}_\mu \phi = \phi$ under the canonical identification $\widehat{\widehat{G}} \cong G$.

Suppose $\Gamma \subset G$ is a discrete subgroup such that G/Γ is compact. Poisson summation states that

$$\sum_{\gamma \in \Gamma} \phi(\gamma) = \sum_{\gamma^\perp \in \Gamma^\perp} \mathcal{F}_\mu(\phi)(\gamma^\perp)$$

8.1.3 Fourier transforms for vector spaces

If G is $\mathbb{R}$, $\mathbb{C}$, a finite extension of $\mathbb{Q}_p$ or $\mathbb{A}_K/K$ where K is a number field and $\psi \in \widehat{G}$ is nontrivial then $a \mapsto (x \mapsto \psi(ax))$ gives a noncanonical identification $G \cong \widehat{G}$. Write $\mathcal{S}(G)$ for the space of Schwarz functions: when $G = \mathbb{R}$ or $\mathbb{C}$ these are functions all of whose derivatives decay faster than polynomials, when $G = K/\mathbb{Q}_p$ is a finite extension then these are locally constant functions with compact support.

Choosing $\phi \in \widehat{G}$ as above gives a Fourier transform $\mathcal{F}_{\mu,\psi} : \mathcal{S}(G) \to \mathcal{S}(G)$. Via the identification $G \cong \widehat{G}$, the explicit formula is

$$\mathcal{F}_{\mu,\psi}(\phi)(h) = \int_G \phi(g)\psi(hg)d\mu_g$$

Write μ_ψ^* for the transfer of the dual measure $\widehat{\mu}$ from $\widehat{G}$ to G using ψ.

Lemma 8.1. *If $K = \mathbb{R}$ let $\psi(x) = \exp(2\pi i x)$ and $\mu([0,1]) = 1$. If $K = \mathbb{C}$ let $\psi(x) = \exp(2\pi i \operatorname{Re} x)$ and $\mu([0,1] \times [0,i]) = 2$. If $K/\mathbb{Q}_p$ is a finite extension let $\lambda : \mathbb{Q}_p \to \mathbb{Z}[1/p]$ be such that $\lambda(x) + x \in \mathbb{Z}_p$. Then $\lambda(x)$ is well-defined up to $\mathbb{Z}$ and $\psi(x) = \exp(2\pi i \lambda(\operatorname{Tr}_{K/\mathbb{Q}_p}(x))$ is a well-defined character. Suppose $\mu(\mathcal{O}_K) = [\mathcal{D}_{K/\mathbb{Q}_p}^{-1} : \mathcal{O}_K]^{-1/2}$.*

In all three cases, $\mu_\psi^* = \mu$.

Proof. [Tat67, Theorem 2.2.2]. □

Let K be a number field. For each place v fix $\psi_v \in \widehat{K}_v$ such that for almost all v, $\ker \psi_v = \mathcal{O}_v$. Then $\psi = \otimes \psi_v \in \widehat{\mathbb{A}_K} = \prod'_{\{\mathcal{O}_v^\perp\}} \widehat{K_v}$. Using ψ_v to identify $K_v \cong \widehat{K}_v$ get $\mathcal{O}_v \cong \mathcal{O}_v^\perp$. Thus $\mathbb{A}_K \cong \widehat{\mathbb{A}}_K$ via $a \mapsto (x \mapsto \psi(ax))$. Under this identification $K^\perp \subset \widehat{\mathbb{A}_K}$ is simply $K \subset \mathbb{A}_K$ and $\widehat{\mathbb{A}_K/K} \cong K$.

If μ is the Haar measure on $\mathbb{A}_K$ inducing the discrete measure on the discrete subgroup $K \subset \mathbb{A}_K/K$ and inducing $\mu(\mathbb{A}_K/K) = 1$ on the compact group $\mathbb{A}_K/K$ then $\mu_\psi^* = \mu$.

Let $\mathcal{S}(\mathbb{A}_K) = \otimes'_v \mathcal{S}(K_v)$ consist of $\phi = \otimes \phi_v$ where $\phi_v = \operatorname{char}_{\mathcal{O}_v}$ for almost all v. If $\phi = \otimes \phi_v \in \mathcal{S}(\mathbb{A}_K)$ then

$$\mathcal{F}_{\mu,\psi}\phi = \otimes \mathcal{F}_{\mu_v,\psi_v}\phi_v$$

with Fourier inversion $\mathcal{F}_{\mu,\psi^{-1}}\mathcal{F}_{\mu,\psi}\phi = \phi$.

The Poisson summation formula for $K \subset \mathbb{A}_K$ states that

$$|a|_{\mathbb{A}_K} \sum_{\alpha \in K} \phi(a\alpha) = \sum_{\alpha \in K} \mathcal{F}_{\mu,\psi}(\phi)(a^{-1}\alpha)$$

8.2 Local zeta integrals

Suppose $K = \mathbb{R}, \mathbb{C}$ or a finite extension of $\mathbb{Q}_p$. For a continuous character $\chi : K^\times \to \mathbb{C}^\times$ we would like to define "analytically" an L-function. The idea is to define for each test function $\phi \in \mathcal{S}(K)$ and Haar measure ν on $K^\times$

$$\zeta(\phi, \chi, \nu, s) = \int_{K^\times} \phi(x)\chi(x)|x|_K^s d\nu_x$$

and recover the L-function as a common denominator as the test function ϕ varies.

If $K = \mathbb{R}$ and $\chi(x) = (x/|x|)^\varepsilon |x|_{\mathbb{R}}^t$ define

$$L(\chi, s) = \pi^{-(s+t+\varepsilon)/2}\Gamma((s+t+\varepsilon)/2)$$

If $K = \mathbb{C}$ and $\chi(x) = (x/|x|)^m |x|_{\mathbb{C}}^t$ define

$$L(\chi, s) = 2(2\pi)^{-(s+t+|m|/2)}\Gamma(s+t+|m|/2)$$

If $K/\mathbb{Q}_p$ then

$$L(\chi, s) = \begin{cases} 1 & \chi(\mathcal{O}_K^\times) \neq 1 \\ (1 - \chi(\varpi_K)q_K^{-s})^{-1} & \chi(\mathcal{O}_K^\times) = 1 \end{cases}$$

Proposition 8.2. *There exists a test function ϕ_χ such that $\zeta(\phi, \chi_\chi, \nu, s) = L(\chi, s)$. For every test function $\phi \in \mathcal{S}(K)$, $\dfrac{\zeta(\phi, \chi, \nu, s)}{L(\chi, s)}$ is holomorphic.*

1. *If $K = \mathbb{R}$, $\nu = dx/|x|$ and $\chi = (x/|x|)^\varepsilon |x|_{\mathbb{R}}^t$ then $\phi_\chi = x^\varepsilon e^{-\pi x^2}$.*
2. *If $K = \mathbb{C}$, $\nu = \frac{2dxdy}{\pi(x^2+y^2)}$ and $\chi(x) = (x/|x|)^m |x|_{\mathbb{C}}^t$ then $\phi_\chi = \overline{x}^n e^{-2\pi|x|_{\mathbb{C}}}$ if $n \geq 0$ and $\phi_\chi = x^{-n} e^{-2\pi|x|_{\mathbb{C}}}$ if $n < 0$.*
3. *If $K/\mathbb{Q}_p$ is a finite extension, $\nu(\mathcal{O}_K^\times) = 1$ and χ is unramified then $\phi_\chi = \mathrm{char}_{\mathcal{O}_K}$; if χ is ramified of conductor $f \geq 1$ then $\phi_\chi = \nu(1 + \mathfrak{m}_K^f)^{-1} \mathrm{char}_{1+\mathfrak{m}_K^f}$.*

Proof. See [Tat67, §2.5] "the corresponding functions of $\mathfrak{z}$" on page 316 for $K = \mathbb{R}$, on page 318 for $K = \mathbb{C}$ and on page 320 for $K/\mathbb{Q}_p$. □

Lecture 20
2013-05-17

8.3 Local functional equation and local ε-factors

Now that we have defined L-functions analytically we should remark that they do not contain much information about the characters. In fact, for every ramified character χ, one has $L(\chi, s) = 1$, and more generally the L-function of a Galois representation does not take into account the ramified part of the representation. To study the ramified part one needs the ε-factor which arise naturally in the context of functional equations.

Suppose $K = \mathbb{R}, \mathbb{C}$ or a finite extension of $\mathbb{Q}_p$ and $\chi : K^\times \to \mathbb{C}^\times$. Let $\psi \in \widehat{K}$ nontrivial identifying $\widehat{K}$ with K, μ a Haar measure on K and ν a Haar measure on $K^\times$.

Proposition 8.3. *For every $\phi \in \mathcal{S}(K)$*

$$\zeta(\phi, \chi, \nu, s)\gamma(\chi, \psi, \mu, s) = \zeta(\mathcal{F}_{\mu,\psi}\phi, \chi^{-1}, \nu, 1 - s)$$

for $\gamma(\chi, \psi, \mu, s)$ not depending on ϕ and ν.

Proof. [Tat67, Theorem 2.4.1]. □

Theorem 8.4. *The function*

$$\varepsilon(\chi, \psi, \mu, s) = \gamma(\chi, \psi, \mu, s) \frac{L(\chi, s)}{L(\chi^{-1}, 1 - s)}$$

is of the form $A \cdot B^s$ where $A, B \in K$.

Let ψ and μ as in Lemma 8.1. If $K = \mathbb{R}$ and $\chi(x) = (x/|x|)^\varepsilon |x|_{\mathbb{R}}^t$ then $\varepsilon(\chi, \psi, \mu, s) = i^\varepsilon$. If $K = \mathbb{C}$ and $\chi(x) = (x/|x|)^m |x|_{\mathbb{C}}^t$ then $\varepsilon(\chi, \psi, \mu, s) = i^{|m|}$.

Finally suppose $K/\mathbb{Q}_p$ is a finite extension and ψ is any nontrivial character of K. Let f be the conductor of χ, i.e., the smallest integer such that $\chi(\mathcal{U}_K^f) = 1$ and let $-d$ be the conductor of ψ, i.e., the smallest integer such that $\psi(\mathfrak{m}_K^{-d}) = 1$. (For example if ψ is as in Lemma 8.1 then $d = v_K(\mathcal{D}_{K/\mathbb{Q}_p})$.) Then

$$\varepsilon(\chi, \psi, \mu, s) = \left(\mu(\mathfrak{m}_K^{-d}) \sum_{x \in \mathcal{O}_K^\times / \mathcal{U}_K^f} \psi\left(\frac{x}{\varpi_K^{d+f}}\right) \chi^{-1}\left(\frac{x}{\varpi_K^{d+f}}\right) \right) q_K^{-(d+f)s}$$

Proof. See [CF86, §2.5] "explicit expressions for $\rho(c)$" on page 317 for $K = \mathbb{R}$, on page 319 for $K = \mathbb{C}$ and on page 322 for $K/\mathbb{Q}_p$. □

Corollary 8.5. *Have*

$$\varepsilon(\chi,\psi(a\cdot-),\mu,s)=\chi(a)|a|_K^{s-1}\varepsilon(\chi,\psi,\mu,s)$$
$$\varepsilon(\chi,\psi,r\mu,s)=r\varepsilon(\chi,\psi,\mu,s)$$

Proof. The second equality is immediate. For the first equality note that the conductor of $\psi(a\cdot-)$ is equal to $-d-v_K(a)$ and so

$$\begin{aligned}\varepsilon(\chi,\mu,\psi(a\cdot-),s)&=\left(\mu(\mathfrak{m}_K^{-d-v_K(a)})\sum_{x\in\mathcal{O}_K^\times/\mathcal{U}_K^f}\psi\left(\frac{ax}{\varpi_K^{d+v_K(a)+f}}\right)\chi^{-1}\left(\frac{x}{\varpi_K^{d+v_K(a)+f}}\right)\right)q_K^{-(d+v_K(a)+f)s}\\&=\left(\chi(a)|a|_K^{-1}\mu(\mathfrak{m}_K^{-d})\sum_{x\in\mathcal{O}_K^\times/\mathcal{U}_K^f}\psi\left(\frac{ax}{\varpi_K^{d+v_K(a)+f}}\right)\chi^{-1}\left(\frac{ax}{\varpi_K^{d+v_K(a)+f}}\right)\right)q_K^{-(d+v_K(a)+f)s}\\&=\chi(a)|a|_K^{s-1}\left(\mu(\mathfrak{m}_K^{-d})\sum_{y\in\mathcal{O}_K^\times/\mathcal{U}_K^f}\psi\left(\frac{y}{\varpi_K^{d+f}}\right)\chi^{-1}\left(\frac{y}{\varpi_K^{d+f}}\right)\right)q_K^{-(d+f)s}\\&=\chi(a)|a|_K^{s-1}\varepsilon(\chi,\psi,\mu,s)\end{aligned}$$

where we used that $\mu(\mathfrak{m}_K^{-d-v_K(a)})/\mu(\mathfrak{m}_K^{-d})=[\mathfrak{m}_K^{-d-v_K(a)}:\mathfrak{m}_K^{-d}]=q_K^{v_K(a)}=|a|_K^{-1}$ as μ is a Haar measure and we denoted $y=xa\varpi_K^{-v_K(a)}$. □

Proposition 8.6. *Let $K/\mathbb{Q}_p$ be a finite extension, ψ a nontrivial character of K and $\eta:K^\times\to\mathbb{C}^\times$ a continuous character of conductor $f\geq 1$.*

1. *For $0\leq a\leq f/2$ there exists $c_a\in K$ such that $\eta(1+x)=\psi(c_ax)$ for $v_K(x)\geq f-a$.*
2. *If $\chi_1,\chi_2:K^\times\to\mathbb{C}^\times$ are continuous characters of conductors f_1 and f_2 such that $f_1,f_2\leq a$ then*

$$\varepsilon(\chi_1\eta,\psi,\mu,s)\chi_1(c_a)=\varepsilon(\chi_2\eta,\psi,\mu,s)\chi_2(c_a)$$

Proof. Let $\chi:K^\times\to\mathbb{C}^\times$ be any continuous character of conductor $f\geq 1$. First, if $v_K(x),v_K(y)\geq f-a$ then $(1+x)(1+y)=(1+x+y)(1+\frac{xy}{1+x+y})$ where $1+\frac{xy}{1+x+y}\in\mathcal{U}_K^{2f-2a}\subset\mathcal{U}_K^f=\ker\chi$. Therefore $\chi((1+x)(1+y))=\chi(1+x+y)$ and so $x\mapsto\chi(1+x)$ is an additive character which case then be recovered as $\psi(c_ax)$ for some $c_a\in K$. Applying this to $\chi=\eta$ yields the first result.

Recall that $\ker(\psi(c_a\cdot-))=c_a^{-1}\ker(\psi)=\mathfrak{m}_K^f$ as χ has conductor f. But then $v_K(c_a)=-d-f$. In particular, in the formula of Theorem 8.4

$$\varepsilon(\chi,\psi,\mu,s)=\left(\mu(\mathfrak{m}_K^{-d})\sum_{\mathcal{O}_K^\times/\mathcal{U}_K^f}\psi(xc_a)\chi^{-1}(xc_a)\right)q_K^{-(d+f)s}$$

where we replace the sum over x with a sum over $xc_a\varpi_K^{d+f}$.

Writing $x=y(1+z)$ gives

$$\begin{aligned}\sum_{x\in\mathcal{O}_K^\times/\mathcal{U}_K^f}\psi_K(c_ax)\chi^{-1}(c_ax)&=\sum_{y\in\mathcal{O}_K^\times/\mathcal{U}_K^{f-a}}\sum_{z\in\mathfrak{m}_K^{f-a}/\mathfrak{m}_K^f}\psi(c_ay(z+1))\chi^{-1}(c_ay(z+1))\\&=\sum_{y\in\mathcal{O}_K^\times/\mathcal{U}_K^{f-a}}\psi(c_ay)\chi^{-1}(c_ay)\sum_{z\in\mathfrak{m}_K^{f-a}/\mathfrak{m}_K^f}\psi(c_ayz)\chi^{-1}(1+z)\\&=\sum_{y\in\mathcal{O}_K^\times/\mathcal{U}_K^{f-a}}\psi(c_ay)\chi^{-1}(c_ay)\sum_{z\in\mathfrak{m}_K^{f-a}/\mathfrak{m}_K^f}\psi(c_az(y-1))\end{aligned}$$

where the last line follows from the fact that $\chi(1+z)=\psi(c_a z)$ as $v_K(z)\geq f-a$.

If $u=\varpi_K^{f-a}$ then

$$\begin{aligned}\sum_{z\in\wp_K^{f-a}/\wp_K^f}\psi(c_a z(y-1)) &= \sum_{z\in\mathfrak{m}_K^{f-a}/\mathfrak{m}_K^f}\psi(c_a(z+u)(y-1))\\ &= \psi(c_a u(y-1))\sum_{z\in\mathfrak{m}_K^{f-a}/\mathfrak{m}_K^f}\psi(c_a z(y-1))\end{aligned}$$

and therefore $\sum_{z\in\mathfrak{m}_K^{f-a}/\mathfrak{m}_K^f}\psi(c_a z(y-1))=0$ unless $\psi(c_a u(y-1))=1$, which can only happen if $v_K(c_a u(y-1))\geq -d$. But $v_K(c)=-d-f$ and $v_K(u)=f-a$ and therefore the sum vanishes unless $y\in\mathcal{U}_K^a$. If $y\in\mathcal{U}_K^a$ then $\psi(c_a z(y-1))=1$ and so

$$\sum_{z\in\mathfrak{m}_K^{f-a}/\mathfrak{m}_K^f}\psi(c_a z(y-1))=|\mathfrak{m}_K^{f-a}/\mathfrak{m}_K^f|=q_K^a$$

We get

$$\sum_{x\in\mathcal{O}_K^\times/\mathcal{U}_K^f}\psi_K(c_a x)\chi^{-1}(c_a x)=q_K^a\sum_{y\in\mathcal{U}_K^a/\mathcal{U}_K^{f-a}}\psi(c_a y)\chi^{-1}(c_a y)$$

which gives

$$\varepsilon(\chi,\psi,\mu,s)=q_K^{-(d+f)s}\mu_K(\mathfrak{m}_K^{-d})q_K^a\left(\sum_{y\in\mathcal{U}_K^a/\mathcal{U}_K^{f-a}}\psi(c_a y)\chi^{-1}(c_a y)\right)$$

We now apply the above to $\chi=\chi_1\eta$ and $\chi_2\eta$. Suppose for instance that $\chi=\chi_1\eta$. Then χ has conductor f and $\chi(1+x)=\chi_1(1+x)\eta(1+x)=\eta(1+x)=\psi(c_a x)$ for every $x\in\mathcal{U}_K^{f-a}$ as $f_1\leq a\leq f-a$. Therefore

$$\begin{aligned}\varepsilon(\chi_1\eta,\psi,\mu,s) &= q_K^{a-(d+f)s}\mu_K(\mathfrak{m}_K^{-d})\left(\sum_{y\in\mathcal{U}_K^a/\mathcal{U}_K^{f-a}}\psi(c_a y)(\chi_1\eta)^{-1}(c_a y)\right)\\ &= \chi_1^{-1}(c_a)q_K^{a-(d+f)s}\mu_K(\mathfrak{m}_K^{-d})\left(\sum_{y\in\mathcal{U}_K^a/\mathcal{U}_K^{f-a}}\psi(c_a y)\eta^{-1}(c_a y)\right)\end{aligned}$$

because if $y\in\mathcal{U}_K^a\subset\ker\chi_1$ then $\chi_1^{-1}(c_a y)=\chi_1^{-1}(c_a)$.

The conclusion follows from the fact that $\varepsilon(\chi_1\eta,\psi,\mu,s)\chi_1(c_a)$ does not depend on χ_1. □

Lecture 21
2013-05-20

8.4 Global zeta integrals

Suppose $\chi:\mathbb{A}_K^\times/K^\times\to\mathbb{C}^\times$ is a continuous Hecke character, ν is a Haar measure on $\mathbb{A}_K^\times$ and $\phi\in\mathcal{S}(\mathbb{A}_K)$. Define

$$\zeta(\phi,\chi,\nu,s)=\int_{\mathbb{A}_K^\times}\phi(x)\chi(x)|x|_{\mathbb{A}_K}^s d\nu_x$$

Since $\widehat{\mathbb{A}^\times}\cong\prod'_{\{\mathcal{O}_v^\times,^\perp\}}\widehat{K_v^\times}$ we may write $\chi=\otimes\chi_v$ where $\chi_v:K_v^\times\to\mathbb{C}^\times$ is unramified at all but finitely many v. By definition $\phi=\otimes\phi_v$ and write $\nu=\otimes\nu_v$ where ν_v is a Haar measure on $K_v^\times$ with the property that $\nu_x(\mathcal{O}_v^\times)=1$ for almost all v. Then

$$\zeta(\phi,\chi,\nu,s)=\prod\zeta(\phi_v,\chi_v,\nu_v,s)$$

which converges for $\operatorname{Re} s > t+1$ where $|\chi_v| = |x|_{K_v}^{t_v}$ for $t_v \leq t$ a real number. Such a t can always be found if $\chi(K^\times) = 1$, i.e., $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$ is a continuous Hecke character.

Theorem 8.7. *The integral $\zeta(\phi, \chi, \nu, s)$ satisfies the functional equation*

$$\zeta(\phi, \chi, \nu, s) = \zeta(\mathcal{F}_{\mu,\psi}\phi, \chi^{-1}, \nu, 1-s)$$

It has analytic continuation to $\mathbb{C}$ unless $\chi = |\cdot|_{\mathbb{A}_K}^{s_0}$ in which case it has a simple pole at $s = -s_0$ with residue $-\nu^1(\mathbb{A}_K^1/K^\times)\phi(0)$ and a simple pole at $s = 1 - s_0$ with residue $\nu^1(\mathbb{A}_K^1/K)\mathcal{F}_{\mu,\psi}(\phi)(0)$. Here ν^1 on $\mathbb{A}_K^1$ is the Haar measure such that the quotient measure on $\mathbb{A}_K^\times/\mathbb{A}_K^1 \cong (0,\infty)$ is the measure dt/t, while the Haar measure on $\mathbb{A}_K^1/K^\times$ is the quotient measure by the discrete Haar measure on $K^\times$.

Proof. See [Tat67, Main Theorem 4.4.1]. □

Corollary 8.8. *If K is a number field and $\chi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ is a continuous Hecke character then $\prod_v \gamma(\chi_v, \psi_v, \mu_v, s) = 1$.*

Proof. This is immediate from Theorem 8.7 and Proposition 8.3. □

8.5 Global L-functions and ε-factors

Let $\chi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ be a continuous Hecke character and write $\chi = \otimes\chi_v$. Define

$$L(\chi, s) = \prod_v L(\chi_v, s)$$

Write

$$\varepsilon(\chi, s) = \prod \varepsilon(\chi_v, \psi_v, \mu_v, s)$$

which does not depend on ψ or μ. Choose ν such that $\nu_v = \frac{dx}{|x|}$ if $v \mid \mathbb{R}$, $\nu_v = \frac{2dxdy}{\pi\sqrt{x^2+y^2}}$ for $v \mid \mathbb{C}$ and $\nu_v(\mathcal{O}_v^\times) = 1$ for $v \nmid \infty$. Choose μ_v as in Lemma 8.1.

Theorem 8.9. *The function $L(\chi, s)$ has analytic continuation to $\mathbb{C}$ unless $\chi = |\cdot|_{\mathbb{A}_K}^{s_0}$ in which case it has a simple pole at $s = -s_0$ with residue $-\nu^1(\mathbb{A}_K^1/K^\times)$ and a simple pole at $s = 1 - s_0$ with residue $\nu^1(\mathbb{A}_K^1/K^\times)\sqrt{|D_K|}^{-1}$ where D_K is the discriminant of $K/\mathbb{Q}$. Moreover*

$$L(\chi, s) = \varepsilon(\chi, s)L(\chi^{-1}, 1-s)$$

Proof. Let S be the finite set of places such that $v \mid \infty$ or χ_v is ramified or $\ker\psi_v \neq \mathcal{O}_v$ or $\mu_v(\mathcal{O}_v) \neq 1$ or $\nu(\mathcal{O}_v^\times) \neq 1$. For every place v choose ϕ_v such that $\zeta(\phi_v, \chi_v, \nu_v, s) = L(\chi_v, s)$. In particular, for $v \notin S$, $\phi_v = \operatorname{char}_{\mathcal{O}_v}$ by Proposition 8.2 and in this case we compute

$$\begin{aligned}(\mathcal{F}_{\psi_v,\mu_v}\phi_v)(x) &= \int_{K_v} \operatorname{char}_{\mathcal{O}_v}(y)\psi_v(xy)d\mu_{v,y} = \int_{\mathcal{O}_v} \psi_v(xy)d\mu_{v,y} \\ &= \begin{cases}\mu_v(\mathcal{O}_v) & \psi_v(x) = 1 \\ 0 & \psi_v(x) \neq 1\end{cases}\end{aligned}$$

where $\ker\psi_v = \mathcal{O}_v$ since ψ_v is unramified for $v \notin S$ by choice of S. Therefore $\mathcal{F}_{\psi_v,\mu_v}\phi_v = \mu_v(\mathcal{O}_v)\phi_v = \phi_v$.

Then for $v \notin S$, $\mathcal{F}_{\mu_v,\psi_v}\phi_v = \operatorname{char}_{\mathcal{O}_v}$, $\zeta(\mathcal{F}_{\mu_v,\psi_v}\phi_v, \chi_v^{-1}, \nu_v, 1-s) = L(\chi_v^{-1}, 1-s)$ and $\varepsilon(\chi_v, \psi_v, \mu_v, s) = 1$. Thus

$$1 = \frac{\zeta(\phi, \chi, \nu, s)}{L(\chi, s)} = \prod_{v\in S} \frac{\zeta(\phi_v, \chi_v, \nu_v, s)}{L(\chi_v, s)}$$

$$\frac{\zeta(\mathcal{F}_{\mu,\psi}\phi, \chi^{-1}, \nu, 1-s)}{L(\chi^{-1}, 1-s)} = \prod_{v\in S} \frac{\zeta(\mathcal{F}_{\psi_v,\mu_v}\phi_v, \chi_v^{-1}, \nu_v, 1-s)}{L(\chi_v^{-1}, 1-s)}$$

and so

$$\begin{aligned}\frac{L(\chi^{-1},1-s)\varepsilon(\chi,s)}{L(\chi,s)} &= \frac{\zeta(\mathcal{F}_{\mu,\psi}\phi,\chi^{-1},\nu,1-s)\prod_{v\in S}\frac{L(\chi_v^{-1},1-s)}{\zeta(\mathcal{F}_{\mu_v,\psi_v}\phi_v,\chi_v^{-1},1-s)}\prod_{v\in S}\varepsilon(\chi_v,\psi_v,\mu_v,s)}{\zeta(\phi,\chi,\nu,s)\prod_{v\in S}\frac{L(\chi_v,s)}{\zeta(\phi_v,\chi_v,\nu_v,s)}} \\ &= \frac{\zeta(\mathcal{F}_{\mu,\psi}\phi,\chi^{-1},\nu,1-s)}{\zeta(\phi,\chi,\nu,s)}\prod_{v\in S}\frac{\zeta(\phi_v,\chi_v,\nu_v,s)}{\zeta(\mathcal{F}_{\mu_v,\psi_v}\phi_v,\chi_v^{-1},1-s)}\frac{\varepsilon(\chi_v,\psi_v,\mu_v,s)L(\chi_v^{-1},1-s)}{L(\chi_v,s)} \\ &= 1\end{aligned}$$

Since $L(\chi,s)=\zeta(\phi,\chi,\nu,s)$, $L(\chi,s)$ is analytic unless $\chi=|\cdot|_{\mathbb{A}_K}^{s_0}$ for some s_0 in which case it has simple poles at $s=-s_0$ and $s=1-s_0$.

It remains to compute the residues. By Theorem 8.7 the residue at $-s_0$ is $-\nu^1(\mathbb{A}_K^1/K^\times)\phi(0)$ and the residue at $1-s_0$ is $\nu^1(\mathbb{A}_K^1/K^\times)\mathcal{F}_{\mu,\psi}(\phi)(0)$ so it suffices to compute $\phi(0)$ and $\mathcal{F}_{\mu,\psi}(\phi)(0)$. Recall from Proposition 8.2 that for $\chi_v=1$ which is unramified we can choose $\phi_v=\mathrm{char}_{\mathcal{O}_v}$ for all $v\nmid\infty$. When $v\mid\mathbb{R}$ then $\phi_v(x)=e^{-\pi x^2}$ and when $v\mid\mathbb{C}$ then $\phi_v(x+iy)=e^{-\pi(x^2+y^2)}$. In particular $\phi(0)=\prod\phi_v(0)=1$ as desired.

It remains to show that $\mathcal{F}_{\mu,\psi}(\phi)(0)=\sqrt{|D_K|}^{-1}$. But for $v\mid\mathbb{R}$ we have chosen $\phi_v(x)=e^{-\pi x^2}$, $\psi_v(x)=e^{2\pi ix}$ and $\mu_v=dx$ for which

$$\mathcal{F}_{\mu_v,\psi_v}\phi_v(0)=\int_{\mathbb{R}}e^{-\pi x^2}dx=1$$

For $v\mid\mathbb{C}$ we have chosen $\phi_v(x+iy)=e^{-2\pi(x^2+y^2)}$, $\psi_v(x+iy)=e^{4\pi ix}$ and $\mu_v=2dxdy$ for which

$$\mathcal{F}_{\mu_v,\psi_v}\phi_v(0)=\int_{\mathbb{C}}e^{-2\pi(x^2+y^2)}2dxdy=1$$

For $v\nmid\infty$ we only need to look at $\chi_v(x)=|x|_v^{s_0}$ which is unramified and since $\nu(\mathcal{O}_v^\times)=1$ we have $\phi_v=\mathrm{char}_{\mathcal{O}_v}$ and we have already computed the Fourier transform

$$\mathcal{F}_{\mu_v,\psi_v}\phi_v(0)=\mu_v(\mathcal{O}_v)=[\mathcal{D}_{K_v/\mathbb{Q}_p}^{-1}:\mathcal{O}_v]^{-1/2}$$

where the last equality follows from Lemma 8.1. Therefore

$$\begin{aligned}\mathcal{F}_{\mu,\psi}(\phi)(0) &= \prod_{v\nmid\infty}[\mathcal{D}_{K_v/\mathbb{Q}_p}^{-1}:\mathcal{O}_v]^{-1/2} \\ &= \prod_{v\nmid\infty}(N_{K_v/\mathbb{Q}_p}\mathcal{D}_{K_v/\mathbb{Q}_p})^{-1/2} \\ &= \sqrt{|D_K|}^{-1}\end{aligned}$$

as desired. □

8.6 Applications

Theorem 8.10 (Analytic class number formula)**.** *Let K be a number field and let 1 denote the trivial Hecke character of K. Show that $L(1,s)$ has a simple pole at $s=1$ with residue*

$$\lim_{s\to1}(s-1)L(1,s)=\frac{2^nh_KR_K}{w_K\sqrt{|D_K|}}$$

where n is the number of infinite places of K, $h_K=|\mathrm{Cl}(K)|$, R_K is the regulator of K (defined as the absolute value of the rank of the matrix $(\log(|u_i|_v))_{i,v}$ as u_i ranges through a set of generators of $\mathcal{O}_K^\times$ and $v\mid\infty$), $w_K=|\mu_\infty(K)|$ and D_K is the discriminant of $K/\mathbb{Q}$.

Proof. Theorem 8.9 shows that $L(1,s)$ has a simple pole with residue $\nu^1(\mathbb{A}_K^1/K^\times)\sqrt{|D_K|}^{-1}$ so we just need to compute this volume. Recall from Theorem 2.1 the exact sequence

$$0 \to K_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times/\mathcal{O}_K^\times \to \mathbb{A}_K^1/K^\times \to \mathrm{Cl}(K) \to 0$$

and that ν^1 is the quotient measure on $\mathbb{A}_K^1/K^\times$ induced from the Haar measure on $\mathbb{A}_K^1$ coming from ν on $\mathbb{A}_K^\times$ by the discrete measure on $K^\times \subset \mathbb{A}_K^1$. This gives

$$\nu^1(\mathbb{A}_K^1/K^\times) = \nu^1(K_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times/\mathcal{O}_K^\times)\nu^1(\mathrm{Cl}(K)) = h_K \nu^1(K_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times/\mathcal{O}_K^\times)$$

Also recall the exact sequence

$$0 \to \prod_{v|\mathbb{R}}\{\pm 1\} \prod_{v|\mathbb{C}} S^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times/\mu_\infty(K) \to K_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times/\mathcal{O}_K^\times \to \Delta_\infty/\log \mathcal{O}_K^\times \to 0$$

Writing ν^1 for the measure on

$$K_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times/\mathcal{O}_K^\times \subset \mathbb{A}_K^1/K^\times$$

and for the subset measure on $\prod_{v|\mathbb{R}}\{\pm 1\}\prod_{v|\mathbb{C}} S^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times/\mu_\infty(K)$ we get the quotient measure ν^1 on $\Delta_\infty/\log \mathcal{O}_K^\times$ which gives

$$\nu^1(K_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times/\mathcal{O}_K^\times) = \nu^1(\prod_{v|\mathbb{R}}\{\pm 1\} \prod_{v|\mathbb{C}} S^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times/\mu_\infty(K))\nu^1(\Delta_\infty/\log \mathcal{O}_K^\times)$$

What are the measures on the kernel and image? If $v \mid \mathbb{R}$ then we have

$$0 \to \{\pm 1\} \to \mathbb{R}^\times \to \mathbb{R} \to 0$$

via $x \mapsto \log|x|$. The measure on $\mathbb{R}^\times$ is $\nu_v = dx/|x| = d\log|x|$ and so the measure on the image $\mathbb{R}$ is dx. If $v \mid \mathbb{C}$ then

$$0 \to S^1 \to \mathbb{C}^\times \to \mathbb{R} \to 0$$

via $z \mapsto \log|z|_\mathbb{C}$. Recall that $\nu_v = \frac{2dxdy}{\pi(x^2+y^2)}$ which in polar coordinates $x = r\cos\theta$ and $y = r\sin\theta$ becomes $\nu_v = \frac{2rdrd\theta}{\pi r^2} = \frac{2drd\theta}{\pi r} = \frac{d\theta d\log r^2}{\pi}$ and so we can put the measure $d\theta/\pi$ on S^1 yielding the measure dx on the quotient $\mathbb{R}$.

This produces the standard Lebesgue measure on Δ_∞ and so the volume of $\Delta_\infty/\log \mathcal{O}_K^\times$ is precisely R_K. The volume of $\prod_{v|\mathbb{R}}\{\pm 1\}\prod_{v|\mathbb{C}} S^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times$ is 2^n where n is the number of infinite places. Putting everything together gives

$$\nu^1(\mathbb{A}_K^1/K^\times) = \frac{2^n h_K R_K}{w_K}$$

□

The following section was not covered in lecture

Corollary 8.11. *Let ζ_K be the Dedekind ζ-function of K. Show that*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^r(2\pi)^s h_K R_K}{w_K\sqrt{|D_K|}}$$

where r, h_K, R_K and w_K are as in Theorem 8.10, $2s$ is the number of non-real embeddings $K \hookrightarrow \mathbb{C}$, $h_K = |\mathrm{Cl}(K)|$ and D_K is the discriminant of $K/\mathbb{Q}$.

Proof. Note that if r_1 is the number of real places and r_2 is the number of complex places then

$$L(1,s) = \left(\pi^{-s/2}\Gamma(s/2)\right)^{r_1} \left(2(2\pi)^{-s}\Gamma(s)\right)^{r_2} \zeta_K(s)$$

and the result follows from Theorem 8.10 and the fact that

$$\operatorname{res}_{s=1} L(1,s) = \pi^{-r_2} \operatorname{res}_{s=1} \zeta_K(s)$$

□

Theorem 8.12 (Strong multiplicity one for characters)**.** *Let K be a number field and $\chi_1, \chi_2 : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$ be two continuous Hecke characters such that $\chi_{1,v} = \chi_{2,v}$ for almost all v. Then $\chi_1 = \chi_2$.*

Proof. Let $\chi = \chi_1 \chi_2^{-1}$ such that $\chi_v = 1$ for $v \notin S$ where S is a finite set of places which, by assumption, does not include the infinite places. Then

$$\begin{aligned} L(\chi, s) &= \prod_{v \in s} L(\chi_v, s) \prod_{v \notin S} L(1_v, s) \\ &= L(1,s) \prod_{v \in S} \frac{L(\chi_v, s)}{L(1_v, s)} \end{aligned}$$

If χ_v is unramified let $\alpha_v = \chi_v(\varpi_v)$ and otherwise let $\alpha_v = 0$. Then $L(\chi_v, s) = (1 - \alpha_v q_v^{-s})^{-1}$ and so

$$L(\chi, s) = L(1,s) \prod_{v \in S} \frac{1 - q_v^{-s}}{1 - \alpha_v q_v^{-s}}$$

But each $\frac{1-q_v^{-s}}{1-\alpha_v q_v^{-s}}$ is nonzero at $s = 0$ and $s = 1$. Thus $L(\chi, s)$ has a pole at $s = 0$ and $s = 1$ which implies, by Theorem 8.9, that $\chi = 1$. □

End of section not covered in lecture

Lecture 22
2013-05-22

9 Hecke theory for Galois representations

9.1 Global theory

Let $K/\mathbb{Q}$ be a finite extension and $\rho : G_K \to \mathrm{GL}(n, \mathbb{C})$ be a continuous Galois representation. We have already defined

$$L^\infty(\rho, s) = \prod_{v \nmid \infty} \det(1 - \rho(\mathrm{Frob}_v) q_v^{-s} | \rho^{I_{K_v}})^{-1}$$

Lemma 9.1. *Let K be a number field and L/K a finite extension.*

1. *The function $L^\infty(-, s)$ extends to virtual representations. In particular, if ρ is a virtual representation such that $\rho = 0$ then $L^\infty(\rho, s) = 1$.*
2. *If $\rho : G_L \to \mathrm{GL}(n, \mathbb{C})$ then*
$$L^\infty(\mathrm{Ind}_L^K \rho, s) = L^\infty(\rho, s)$$

Proof. For the first part, note that ρ being continuous will have open kernel of the form G_L for L/K finite Galois. Thus $\rho : G_{L/K} \to \mathrm{GL}(n,\mathbb{C})$. Maschke's theorem then implies that ρ is completely reducible and so we only need to check that $L^\infty(\rho_1 \oplus \rho_2, s) = L^\infty(\rho_1, s)L^\infty(\rho_2, s)$ which is immediate from the fact that $\det(1 - \rho_1 \oplus \rho_2(\mathrm{Frob}_v)X|(\rho_1 \oplus \rho_2)^{I_v}) = \det(1 - \rho_1(\mathrm{Frob}_v)X|\rho_1)\det(1 - \rho_1(\mathrm{Frob}_v)X|\rho_1)$.

The second part requires some work. See for example [Neu99, Chapter VII, Proposition 10.4 (iv)]. The idea is to use the decomposition $(\mathrm{Ind}_L^K \rho)|_{G_{K_v}} = \oplus_{w|v} \mathrm{Ind}_{L_w}^{K_v}(\rho|_{G_{L_w}})$ and then to express the action of Frob_v on the inertial invariants of this space as a matrix in terms of the action of Frob_w on the inertial invariants of the $\rho|_{G_{L_w}}$. □

Theorem 9.2. *There exists $L_\infty(\rho, s)$, and $\varepsilon(\rho, s)$ of the form $A \cdot B^s$ such that if $L(\rho, s) = L_\infty(\rho, s)L^\infty(\rho, s)$ then*

$$L(\rho, s) = \varepsilon(\rho, s)L(\rho^*, 1 - s)$$

where $\rho^* = \mathrm{Hom}(\rho, \mathbb{C})$ with action $(\rho^*(g)f)(v) = f(\rho(g^{-1})(v))$.

Proof. If $\chi : G_K \to \mathbb{C}^\times$ is a continuous character then χ factors through $G_K^{\mathrm{ab}} \cong \mathbb{A}_K^\times / \overline{K^\times K_\infty^{\times,0}}$ and therefore get $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$. It is easy to see that $L^\infty(\chi, s)$ with χ a Galois character is $L^\infty(\chi, s)$ with χ a Hecke character. By Theorem 8.9 $L(\chi, s) = \varepsilon(\chi, s)L(\chi^{-1}, 1 - s)$.

As ρ is continuous, there exists a finite Galois extension L/K such that $G_L \subset \ker \rho$ and so ρ factors through $G_{L/K} \to \mathrm{GL}(n,\mathbb{C})$. Brauer's theorem implies the existence of cyclic extensions $L/L_i/K$ and characters $\chi_i : G_{L/L_i} \to \mathbb{C}^\times$ such that $\rho = \sum m_i \mathrm{Ind}_{L_i}^K \chi_i$ in the Grothendieck group of continuous representations of G_K.

Let $L_\infty(\rho, s) = \prod L_\infty(\mathrm{Ind}_{L_i}^K \chi_i, s)^{m_i}$ in which case $L(\rho, s) = \prod L(\chi_i, s)^{m_i}$. Let $\varepsilon(\rho, s) = \prod \varepsilon(\chi_i, s)^{m_i}$. Then

$$\begin{aligned} L(\rho, s) &= \prod L(\chi_i, s)^{m_i} \\ &= \prod \varepsilon(\chi_i, s)^{m_i} L(\chi_i^{-1}, 1 - s)^{m_i} \\ &= \varepsilon(\rho, s)L(\rho^*, 1 - s) \end{aligned}$$

as desired.

It remains to show that $L(\rho, s)$ (and therefore $\varepsilon(\rho, s)$) is well-defined, i.e., if $\sum n_i \mathrm{Ind}_{L_i}^K \chi_i = 0$ as a virtual representation, then $\prod L(\chi_i, s)^{n_i} = 1$. By Lemma 9.1, $\prod L^\infty(\chi_i, s)^{n_i} = L^\infty(\sum n_i \mathrm{Ind}_{L_i}^K \chi_i, s) = 1$. Therefore it suffices to show that $\prod_i L_\infty(\chi_i, s)^{n_i} = 1$. We will, in fact, show that for each place $v \mid \infty$ of K, $\prod_i \prod_{w_i|v} L_\infty(\chi_{i,w_i}, s)^{n_i} = 1$ where w_i are places of L_i lying above v.

First, note that the characters χ_i are (finite order) characters of G_{L/L_i} and so $\chi_{i,w_i} = 1$ or σ where σ is the sign character for real places w_i. Next, from $\sum n_i \mathrm{Ind}_{L_i}^K \chi_i = 0$ restricting to G_{K_v} we get

$$\sum_i \sum_{w_i|v} n_i \mathrm{Ind}_{L_{i,w_i}}^{K_v} \chi_{i,w_i} = \sum_i \sum_{w_i|v} n_i \mathrm{Ind}_{L_{i,w_i}}^{K_v} 1 = 0$$

If $v \mid \mathbb{C}$ then $w_i \mid \mathbb{C}$ for all w_i and so we deduce that $\sum_i n_i \sum_{w_i|v} 1 = \sum_i n_i[L_i : K]1 = 0$ which is equivalent to $\sum n_i[L_i : K] = 0$. At the same time $L(\chi_{i,w_i}, s) = L(1, s) = 2(2\pi)^{-s}\Gamma(s)$ and we compute

$$\begin{aligned} \prod_i \prod_{w_i|v} L(\chi_{i,w_i}, s)^{n_i} &= \prod_i \prod_{w_i|v} (2(2\pi)^{-s}\Gamma(s))^{n_i} \\ &= (2(2\pi)^{-s}\Gamma(s))^{\sum_i n_i[L_i:K]} \\ &= 1 \end{aligned}$$

If $v \mid \mathbb{R}$ denote by I the set of (i, w_i) with $w_i \mid \mathbb{R}$ and $\chi_{i,w_i} = 1$, by J the set of (i, w_i) such that $w_i \mid \mathbb{R}$ and $\chi_{i,w_i} = \sigma$ and by H the set of (i, w_i) such that $w_i \mid \mathbb{C}$ and (necessarily) $\chi_{i,w_i} = 1$. Then the formula

$\sum_i \sum_{w_i|v} n_i \operatorname{Ind}_{L_{i,w_i}}^{K_v} 1 = 0$ becomes

$$\sum_{(i,w_i)\in I} n_i \cdot 1 + \sum_{(i,w_i)\in J} n_i \cdot \sigma + \sum_{(i,w_i)\in H} n_i(1+\sigma) = 0$$

as $\operatorname{Ind}_{\mathbb{C}}^{\mathbb{R}} 1 = 1 \oplus \sigma$. We deduce that $\sum_I n_i + \sum_H n_i = 0$ and $\sum_J n_i + \sum_H n_i = 0$. We compute

$$\begin{aligned}
\prod_i \prod_{w_i|v} L(\chi_{i,w_i}, s)^{n_i} &= \prod_{(i,w_i)\in I} L(1_{\mathbb{R}}, s)^{n_i} \prod_{(i,w_i)\in J} L(\sigma, s)^{n_i} \prod_{(i,w_i)\in H} L(1_{\mathbb{C}}, s)^{n_i} \\
&= L(1_{\mathbb{R}}, s)^{\sum_I n_i} L(\sigma, s)^{\sum_J n_i} L(1_{\mathbb{C}}, s)^{\sum_H n_i} \\
&= L(1_{\mathbb{R}}, s)^{-\sum_H n_i} L(\sigma, s)^{-\sum_H n_i} L(1_{\mathbb{C}}, s)^{\sum_H n_i} \\
&= \left(\frac{L(1_{\mathbb{C}}, s)}{L(1_{\mathbb{R}}, s) L(\sigma, s)} \right)^{\sum_H n_i} \\
&= 1
\end{aligned}$$

where we used the identity

$$\left(\pi^{-s/2}\Gamma(s/2)\right)\left(\pi^{-(s+1)/2}\Gamma((s+1)/2)\right) = 2(2\pi)^{-s}\Gamma(s)$$

in other words $L(1_{\mathbb{R}}, s)L(\sigma, s) = L(1_{\mathbb{C}}, s)$.

□

9.2 Deligne's local ε-factors

Having settled the issue of the existence of $\varepsilon(\rho, s)$ for a global $\rho : G_K \to \mathrm{GL}(n, \mathbb{C})$ one is left with the natural question of defining $\varepsilon(\rho_v, \psi, \mu, s)$ for $\rho_v : G_{K_v} \to \mathrm{GL}(n, \mathbb{C})$. Such an ε-factor would encode information about the ramification of ρ_v and appears naturally in the statement of the local Langlands correspondence.

Theorem 9.3. *Let $K/\mathbb{Q}_p$ be a finite extension, $\psi \in \widehat{K}$ nontrivial and μ a Haar measure on K. There exist $\varepsilon(\rho, \psi, \mu, s)$ (of the form $A \cdot B^s$) attached to finite dimensional continuous representations ρ of G_K such that:*

1. *If $\chi : G_K \to \mathbb{C}^\times$ is a character then $\varepsilon(\chi, \psi, \mu, s) = \varepsilon(\chi \circ r_K, \psi, \mu, s)$ as defined for characters of $K^\times$.*
2. *$\varepsilon(\rho_1 \oplus \rho_2, \psi, \mu, s) = \varepsilon(\rho_1, \psi, \mu, s)\varepsilon(\rho_2, \psi, \mu, s)$ so $\varepsilon(-, \psi, \mu, s)$ is multiplicative on the Grothendieck ring.*
3. *For $r \in (0, \infty)$, $\varepsilon(\rho, \psi, r\mu, s) = r^{\dim \rho}\varepsilon(\rho, \psi, \mu, s)$.*
4. *For $a \in K^\times$, $\varepsilon(\rho, \psi(a \cdot -), \mu, s) = \det \rho(r_K(a))|a|_K^{(s-1)\dim \rho}\varepsilon(\rho, \psi, \mu, s)$.*
5. *If L/K is a finite extension and ρ is a representation of virtual dimension 0 (i.e., $\rho = \sum m_i \rho_i$ in the Grothendieck ring with $\sum m_i \dim \rho_i = 0$) then $\varepsilon(\operatorname{Ind}_L^K \rho, \psi, \mu, s) = \varepsilon(\rho, \psi \circ \mathrm{Tr}_{L/K}, \mu', s)$ for any Haar measure μ' of L.*
6. *Have*
$$\varepsilon(\rho, \psi, \mu, s) = \varepsilon(\rho, \psi, \mu, 0) \cdot q_K^{-s(\operatorname{cond} \rho - \dim \rho \operatorname{cond} \psi)}$$
7. *There exists f_ρ such that if χ is a character of conductor $f \geq f_\rho$ then*
$$\varepsilon(\rho \otimes \chi, \psi, \mu, s) = \det \rho(c)^{-1} \varepsilon(\chi, \psi, \mu, s)^{\dim \rho}$$
where c is such that $\chi(1 + x) = \psi(cx)$ for $v_K(x) \geq \lceil f/2 \rceil$.

In principle this should follow from the Brauer induction theorem. Indeed ρ trivializes G_L for some finite Galois extension L/K and thus factors through $G_{L/K}$. There exist $L/M_i/K$ subextensions and character $\chi_i : G_{L/M_i} \to \mathbb{C}^\times$ such that in the Grothendieck ring

$$\rho - \dim \rho \cdot 1 = \sum n_i \operatorname{Ind}_{M_i}^L (\chi_i - 1)$$

where $n_i \in \mathbb{Z}$. Thus

$$\varepsilon(\rho - \dim \rho \cdot 1, \psi, \mu, s) = \prod \varepsilon(\chi_i - 1, \psi \circ \operatorname{Tr}_{M_i/K}, \mu_i, s)^{n_i}$$

giving $\varepsilon(\rho, \psi, \mu, s)$. However, the challenge is to show that this definition does not depend on M_i, χ_i and n_i. In fact there is no current local proof of this fact.

The actual proof will use the global ε-factors of Theorem 9.2 which are known to exist. To do this we need to go from the local to the global setting and in the process prove results that ensure that choices do not affect the outcome.

Lemma 9.4. *Let L/K be a finite Galois extension of p-adic fields. There exists a finite Galois extension of number fields E/F, a finite place v_0 of F and a unique place u_0 of E such that $F_{v_0} = K$ and $E_{u_0} = L$. Moreover, $G_{E/F} \cong G_{L/K}$.*

Proof. Since $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ one may choose a number field $E_0 \subset L$ which is dense in L. Let E be the composite of $\{\sigma(E_0) | \alpha \in G_{L/K}\}$ and let $F = E \cap K$. Since $E \subset L$ and $F \subset K$ are dense, $G_{E/F} = G_{L/K}$. The dense embedding $F \subset K$ defines a finite place v_0 of F with $F_{v_0} = K$ and the dense embedding $E \subset L$ defines a finite place u_0 of E with $E_{u_0} = L$. Now u_0 is fixed by $G_{L/K} = G_{E/F}$ and so u_0 is the only place of E above v_0. □

Lemma 9.5. *Let L/K be a finite Galois extension of p-adic fields and let $e = e_{L/K}$ be the ramification index. Then for $x \in \mathcal{O}_L$ one has*

$$N_{L/K}(1 + x) \equiv 1 + \operatorname{Tr}_{L/K}(x) \pmod{\mathfrak{m}_K^{\lceil 2v_L(x)/e \rceil}}$$

Proof. If $\sigma \in G_{L/K}$ then $v_K(\sigma(x)) = v_K(x) = e^{-1} v_L(x)$ and therefore if $I \subset G_{L/K}$ is a set of cardinality i then $v_K(\prod_{\sigma \in I} \sigma(x)) = \frac{i}{e} v_L(x)$. If $i \geq 2$ then

$$v_K\Big(\sum_{I \subset G_{L/K}, |I| = i} \prod_{\sigma \in I} \sigma(x)\Big) \geq \frac{i}{e} v_L(x) \geq \left\lceil \frac{2v_L(x)}{e} \right\rceil$$

and so

$$\begin{aligned} N_{L/K}(1 + x) &= \prod_{\sigma \in G_{L/K}} (1 + \sigma(x)) \\ &= 1 + \operatorname{Tr}_{L/K}(x) + \sum_{i=2}^{[L:K]} \sum_{I \subset G_{L/K}, |I| = i} \prod_{\sigma \in I} \sigma(x) \\ &\equiv 1 + \operatorname{Tr}_{L/K} \pmod{\mathfrak{m}_K^{\lceil 2v_L(x)/e \rceil}} \end{aligned}$$

□

Lecture 23
2013-05-24

Lemma 9.6. *Let $L/K/\mathbb{Q}_p$ be finite extensions. Let $\ell_{L/K}$ be the smallest integer such that $G_K^{\ell_{L/K}} \subset G_L$. Then for $y \geq \ell_{L/K}$,*

$$\phi_{L/K}^{-1}(y) = e_{L/K} y - v_L(\mathcal{D}_{L/K})$$

where recall that $\phi_{L/K}$ is the ramification function defined as $\phi_{L/K}(x) = \displaystyle\int_0^\infty [G_{L/K,0} : G_{L/K,u}]^{-1} du$ when L/K is Galois, and $\phi_{L/K} = \phi_{E/K} \circ \phi_{E/L}^{-1}$ where E is the Galois closure of L/K in the non-Galois case.

Proof. Start with L/K Galois. The graph of the function $\phi_{L/K}$ is piece-wise linear with inflection points at the jumps in the ramification filtration. In particular, for $x \geq \phi_{L/K}^{-1}(\ell_{L/K})$, the slope of the graph of $\phi_{L/K}$ is $e_{L/K}^{-1}$. This implies that for $y = \phi_{L/K}(x) \geq \ell_{L/K}$,

$$\phi_{L/K}^{-1}(y) = e_{L/K}y + \phi_{L/K}^{-1}(\ell_{L/K}) - e_{L/K}\ell_{L/K}$$

Let $k = \phi_{L/K}^{-1}(\ell_{L/K}) \in \mathbb{Z}$. The we need to show that $e_{L/K}\phi_{L/K}(k) - k = v_L(\mathcal{D}_{L/K})$. But

$$\begin{aligned} e_{L/K}\phi_{L/K}(k) - k &= \int_0^k \frac{e_{L/K}du}{[G_{L/K,0} : G_{L/K,u}]} - k \\ &= \int_0^k |G_{L/K,u}|du - k \\ &= \sum_{i=1}^{k}(|G_{L/K,i}| - 1) \\ &= v_L(\mathcal{D}_{L/K}) \end{aligned}$$

Now suppose L/K is not Galois and let E be the Galois closure. For $y >> 0$ one has

$$y = \phi_{E/L}^{-1}(\phi_{E/L}(y)) = e_{E/L}\phi_{E/L} - v_E(\mathcal{D}_{E/L})$$

and so

$$\begin{aligned} \phi_{L/K}^{-1}(y) &= \phi_{E/L}(\phi_{E/K}^{-1}(y)) \\ &= \frac{\phi_{E/K}^{-1}(y) + v_E(\mathcal{D}_{E/L})}{e_{E/L}} \\ &= \frac{e_{E/K}y - v_E(\mathcal{D}_{E/K}) + v_E(\mathcal{D}_{E/L})}{e_{E/L}} \\ &= e_{L/K}y - v_L(\mathcal{D}_{L/K}) \end{aligned}$$

where the last equality follows from $\mathcal{D}_{E/K} = \mathcal{D}_{E/L}\mathcal{D}_{L/K}$. To show that $\phi_{L/K}^{-1}(y) = e_{L/K}y - v_L(\mathcal{D}_{L/K})$ for $y \geq \ell_{L/K}$ it suffices to show that $(\phi_{L/K}^{-1})'(\ell_{L/K}) = e_{L/K}$ where $()'$ means right derivative. Using the chain rule we get

$$\begin{aligned} (\phi_{L/K}^{-1})'(\ell_{L/K}) &= (\phi_{E/L} \circ \phi_{E/K}^{-1})'(\ell_{L/K}) \\ &= \frac{\phi'_{E/L}(\phi_{E/K}^{-1}(\ell_{L/K}))}{\phi'_{E/K}(\phi_{E/K}^{-1}(\ell_{L/K}))} \\ &= \frac{[I_{E/K} : G_{E/K,\phi_{E/K}^{-1}(\ell_{L/K})}]}{[I_{E/L} : G_{E/L,\phi_{E/K}^{-1}(\ell_{L/K})}]} \\ &= \frac{e_{L/K}|G_{E/L,\phi_{E/K}^{-1}(\ell_{L/K})}|}{|G_{E/K,\phi_{E/K}^{-1}(\ell_{L/K})}|} \end{aligned}$$

as $\phi'_{L/K}(x) = 1/[I_{L/K} : G_{L/K,x}]$ by definition. Thus it is enough to show that

$$|G_{E/K,\phi_{E/K}^{-1}(\ell_{L/K})}| = |G_{E/L,\phi_{E/K}^{-1}(\ell_{L/K})}|$$

But $G_{E/K,\phi_{E/K}^{-1}(\ell_{L/K})} = G_{E/K}^{\ell_{L/K}}$ while $G_{E/L,\phi_{E/K}^{-1}(\ell_{L/K})} = G_{E/L}^{\phi_{E/L}(\phi_{E/K}^{-1}(\ell_{L/K}))} = G_{E/L}^{\phi_{L/K}^{-1}(\ell_{L/K})}$. But Herbrand implies that

$$G_{E/L}^{\phi_{L/K}^{-1}(\ell_{L/K})} = G_{E/K}^{\phi_{L/K}(\phi_{L/K}^{-1}(\ell_{L/K}))} \cap G_{E/L} = G_{E/K}^{\ell_{L/K}} \cap G_{E/L} = G_{E/K}^{\ell_{L/K}}$$

where the last equality follows from the fact that by definition of $\ell_{L/K}$ we have $G_{E/K}^{\ell_{L/K}} \subset G_{E/L}$. □

Lemma 9.7. *Let L/K be a finite extension of p-adic local fields and let $\alpha : K^\times \to \mathbb{C}^\times$ be a continuous character of conductor $\mathrm{cond}(\alpha) > \ell_{L/K}$. Then*

$$\mathrm{cond}(\alpha \circ N_{L/K}) = \phi_{L/K}^{-1}(\mathrm{cond}(\alpha))$$

Proof. Let $m = \mathrm{cond}(\alpha \circ N_{L/K})$ the smallest integer such that $\alpha \circ N_{L/K}$ vanishes on $\mathcal{U}_K^m$. Via the local Artin map m is the smallest integer such that $\alpha \circ N_{L/K} \circ r_L^{-1}$ vanishes on G_L^m. But $\alpha \circ N_{L/K} \circ r_L^{-1} = \alpha \circ r_K^{-1}$ which would then have to vanish on G_L^m with m smallest with this property. Herbrand's theorem says that $G_L^u = G_K^{\phi_{L/K}(u)} \cap G_L$ and so m is the smallest integer such that $\alpha \circ r_K^{-1}$ is trivial on $G_K^{\phi_{L/K}(m)} \cap G_L = G_K^{\phi_{L/K}(m)} \cap G_K^{\ell_{L/K}} = G_K^{\max(\phi_{L/K}(m),\ell_{L/K})}$. This implies that $\max(\phi_{L/K}(m), \ell_{L/K}) \geq \mathrm{cond}(\alpha)$. Since $\mathrm{cond}(\alpha) > \ell_{L/K}$ we get that $\phi_{L/K}(m) \geq \mathrm{cond}(\alpha)$ and m is minimal with this property. The result follows since $\phi_{L/K}^{-1}(\ell_{L/K}) \in \mathbb{Z}$ from the previous lemma. □

Lecture 24
2013-06-05

Lemma 9.8. *Let L/K be a finite Galois extension of p-adic fields. There exists an integer $n_{L/K}$ which depends only on L/K with the following property. Suppose $\alpha : K^\times \to \mathbb{C}^\times$ is a continuous character of conductor $n \geq n_{L/K}$ and $a = \lfloor n/2 \rfloor - v_L(\mathcal{D}_{L/K})$. Let ψ be a nontrivial additive character of K and let $c_a \in K$ from the proof of Proposition 8.6 such that $\alpha(1+x) = \psi(c_a x)$ for $x \in K$ with $v_K(x) \geq n - a$. If $L/M/K$ is a subextension and χ is any character of $G_{L/M}$ then*

$$\varepsilon(\chi \cdot \alpha \circ N_{M/K}, \psi \circ \mathrm{Tr}_{M/K}, \mu, s) = \chi(c_a)^{-1} \varepsilon(\alpha \circ N_{M/K}, \psi \circ \mathrm{Tr}_{M/K}, \mu, s)$$

for any Haar measure μ on M.

Proof. We will apply the stability Proposition 8.6 for $\chi_1 = \chi$, $\chi_2 = 1$ and $\eta = \alpha \circ N_{M/K}$. Denote by $c_{a,\eta,\psi}$ such that $\eta(1+x) = \psi(c_{a,\eta,\psi} x)$ for $v_K(x) \geq \mathrm{cond}(\eta) - a$ where $a \leq \mathrm{cond}(\eta)/2$.

Let

$$n_{L/K} \geq \max(\ell_{M/K}, 2(v_L(\mathcal{D}_{L/K}) + v_K(\mathcal{D}_{M/K}) + \ell_{L/M}/e_{M/K}))$$

as M varies among the subextensions $L/M/K$. We will show that if χ is a character of $G_{L/M}$ then for $b = e_{M/K} a - v_M(\mathcal{D}_{M/K})$ we have $\mathrm{cond}(\chi), \mathrm{cond}(1) \leq b \leq \mathrm{cond}(\alpha \circ N_{M/K})/2$. Then Proposition 8.6 would imply that

$$\varepsilon(\chi \cdot \alpha \circ N_{M/K}, \psi \circ \mathrm{Tr}_{M/K}, \mu, s) = \chi(c_{b,\alpha\circ N_{M/K},\psi\circ \mathrm{Tr}_{M/K}})^{-1} \varepsilon(\alpha \circ N_{M/K}, \psi \circ \mathrm{Tr}_{M/K}, \mu, s)$$

and the Lemma would follow if we could check that

$$c_{b,\alpha\circ N_{M/K},\psi\circ \mathrm{Tr}_{M/K}} = c_{a,\alpha,\psi}$$

From $n \geq n_{L/K} \geq 2(v_L(\mathcal{D}_{L/K}) + v_K(\mathcal{D}_{M/K}) + \ell_{L/M}/e_{M/K})$ we deduce that $b \geq \ell_{L/M}$. But if χ is a character of $G_{L/M}$ it will be trivial on $G_M^{\ell_{L/M}} \subset G_L$ and so $\mathrm{cond}(\chi) \leq \ell_{L/M} \leq b$ as desired. To check that $b \leq \mathrm{cond}(\alpha \circ N_{M/K})/2$ it suffices to check that

$$b = e_{M/K}(n/2 - v_L(\mathcal{D}_{L/K})) - v_M(\mathcal{D}_{M/K}) \leq \mathrm{cond}(\alpha \circ N_{M/K})/2 = \phi_{M/K}^{-1}(n)/2$$

where the last equality follows from Lemma 9.7 as $\mathrm{cond}(\alpha) = n \geq n_{L/K} \geq \ell_{M/K}$. This inequality is equivalent to

$$\begin{aligned} \phi_{M/K}^{-1}(n)/2 &\geq e_{M/K}(n/2 - v_L(\mathcal{D}_{L/K})) - v_M(\mathcal{D}_{M/K}) \\ (e_{M/K}n - v_M(\mathcal{D}_{M/K}))/2 &\geq e_{M/K}(n/2 - v_L(\mathcal{D}_{L/K})) - v_M(\mathcal{D}_{M/K}) \\ e_{M/K}v_L(\mathcal{D}_{L/K}) + v_M(\mathcal{D}_{M/K})/2 &\geq 0 \end{aligned}$$

which is clear.

It remains to show that $c_{b,\alpha\circ N_{M/K},\psi\circ \mathrm{Tr}_{M/K}} = c_{a,\alpha,\psi}$. Let $x \in M$ such that $v_M(x) \geq \mathrm{cond}(\alpha \circ N_{M/K}) - b$. Then $v_M(x) \geq e_{M/K}(n-a) + v_M(\mathcal{D}_{M/K})$ and so $v_K(\mathrm{Tr}_{M/K}(x)) \geq v_K(x) \geq n - a > 0$. By Lemma 9.5, $N_{M/K}(1+x) = 1 + \mathrm{Tr}_{M/K}(x) + y$ where $v_K(y) \geq 2v_M(x)/e_{M/K} \geq 2(n-a) \geq n$. Therefore

$$\begin{aligned} \alpha(N_{M/K}(1+x)) &= \alpha(1+\mathrm{Tr}_{M/K}(x))\alpha\left(1 + \frac{y}{1+\mathrm{Tr}_{M/K}(x)}\right) \\ &= \alpha(1+\mathrm{Tr}_{M/K}(x)) \\ &= \psi(c_{a,\alpha,\psi}\,\mathrm{Tr}_{M/K}(x)) \\ &= \psi(\mathrm{Tr}_{M/K}(c_{a,\alpha,\psi}x)) \end{aligned}$$

since $1+\frac{y}{1+\mathrm{Tr}_{M/K}(x)} \in \mathcal{U}_K^n \subset \ker\alpha$ and $v_K(\mathrm{Tr}_{M/K}(x)) \geq n-a$. By definition this implies that $c_{b,\alpha\circ N_{M/K},\psi\circ\mathrm{Tr}_{M/K}} = c_{a,\alpha,\psi}$ and the result of the lemma follows. □

Proof of Theorem 9.3. Any continuous Galois representation ρ will be trivial on G_L for some finite Galois extension L/K. For a fixed finite Galois extension L/K and any representation ρ of $G_{L/K}$ we will construct $\varepsilon(\rho,\psi,\mu,s)$.

Let E/F be the finite Galois extension from Lemma 9.4. Since $G_{L/K} \cong G_{E/F}$ every representation ρ of $G_{L/K}$ is also a representation $\widetilde{\rho}$ of $G_{E/F}$.

Let S be the finite set of places of F containing the places where E/F ramifies and the place v_0. For each $v \in S - v_0$ choose a finite order character α_v of $F_v^\times$ of conductor $n_v \geq n_{E_u/F_v}$ for a (any) place $u \mid v$ of E. For $v = v_0$ let $\alpha_v = 1$. By Theorem 5.5 there exists α a continuous character of $\mathbb{A}_F^\times/F^\times$ such that $\alpha|_{F_v} = \alpha_v$ for $v \in S$. Choose ψ_F a nontrivial character in $\widehat{\mathbb{A}_F}/F$ such that $\psi_{F,v_0} = \psi$ and μ_F a Haar measure on $\mathbb{A}_F$ such that $\mu_F(\mathbb{A}_F/F) = 1$, $\mu_{F,v_0} = \mu$ and $\mu_{F,v}(\mathcal{O}_v) = 1$ for $v \notin S$. When $v \in S - v_0$ let $c_v \in F_v^\times$ such that $\alpha_v(1+x) = \psi_v(c_v x)$ for $v(x) \geq \lceil n_v/2\rceil - v(\mathcal{D}_{E_u/F_v})$ (see Lemma 9.8). When $v \notin S - v_0$ choose $c_v = 1$ and let $c = (c_v) \in \mathbb{A}_F^\times$.

Suppose $L/M/K$ is a subextension with corresponding global subextension $E/H/F$ and ρ is a representation of $G_{L/M}$ giving $\widetilde{\rho}$ a representation of $G_{E/H}$. Let S_H be the places of H over places in S and again we denote by v_0 the unique place of H over v_0. Let μ_M be a Haar measure on M and let μ_H be a Haar measure on $\mathbb{A}_H$ giving volume 1 to $\mathbb{A}_H/H$ and such that $\mu_{H,v_0} = \mu_M$. We will define

$$\varepsilon(\rho,\psi\circ\mathrm{Tr}_{M/L},\mu_M,s) = \varepsilon(\widetilde{\rho}\cdot\alpha\circ N_{H/F},s)\det\widetilde{\rho}(r_H(c))\left(\prod_{w\in S_H - v_0}\varepsilon(\alpha_v\circ N_{H_w/F_v},\psi_{F,v}\circ\mathrm{Tr}_{H_w/F_v},\mu_{H,w},s)\right)^{-\dim\rho}$$

where v denotes the place of F under w. A priori $\varepsilon(\rho,\psi\circ\mathrm{Tr}_{M/K},\mu_M,s)$ depends on α. We will check the following four facts:

1. if χ is a character of $G_{L/M}$ then $\varepsilon(\chi,\psi\circ\mathrm{Tr}_{M/K},\mu_M,s) = \varepsilon(\chi\circ r_M,\mathrm{Tr}\circ\mathrm{Tr}_{M/K},\mu_M,s)$ as defined for characters,
2. $\varepsilon(-,\psi\circ\mathrm{Tr}_{M/K},\mu_M,s)$ extends to the Grothendieck group,
3. if ρ has virtual dimension 0 then $\varepsilon(\rho,\psi\circ\mathrm{Tr}_{M/L},\mu_M,s)$ does not depend on μ_M

4. if $L/M_1/M_2/K$ are subextensions and ρ is a virtual representation of G_{L/M_1} of virtual dimension 0 then for any choices of μ_{M_1} and μ_{M_2} have $\varepsilon(\mathrm{Ind}_{M_1}^{M_2}\rho, \psi\circ\mathrm{Tr}_{M_2/K}, \mu_{M_2}, s) = \varepsilon(\rho, \psi\circ\mathrm{Tr}_{M_1/K}, \mu_{M_1}, s)$.

Independence of α: Use Brauer induction to find $L/L_i/K$, characters χ_i of G_{L/L_i} and integers n_i such that $\rho - \dim\rho\cdot 1 = \sum n_i \mathrm{Ind}_{L_i}^K(\chi_i - 1)$. Using properties 2 and 5 we deduce

$$\frac{\varepsilon(\rho,\psi,\mu,s)}{\varepsilon(1,\psi,\mu,s)^{\dim\rho}} = \prod\left(\frac{\varepsilon(\chi_i,\psi\circ\mathrm{Tr}_{L_i/K},\mu_i,s)}{\varepsilon(1,\psi\circ\mathrm{Tr}_{L_i/K},\mu_i,s)}\right)^{n_i}$$

and independence of α is clear.

Lecture 25
2013-06-07

Property 1 and fact 1: We now check that if $L/M/K$ is a subextension and χ is a character of $G_{L/M}$ then $\varepsilon(\chi,\psi\circ\mathrm{Tr}_{M/K},\mu_M,s) = \varepsilon(\chi\circ r_M, \mathrm{Tr}\circ\mathrm{Tr}_{M/K},\mu_M,s)$. This implies property 1.

By construction

$$\varepsilon(\chi,\psi_M,\mu_M,s) = \varepsilon(\widetilde{\chi}\cdot\alpha\circ N_{H/F},s)\widetilde{\chi}(r_H(c))\prod_{w\in S_H - v_0}\varepsilon(\alpha_v\circ N_{H_w/F_v},\psi_{H,w},\mu_{H,w},s)$$

where S_H are the places of H over places in S and again we denote by v_0 the unique place of H over v_0; here v is the place of F under w, and $\psi_H = \psi_F\circ\mathrm{Tr}_{H/F}$. Now S_H contains all the places of ramification of E/H and $\widetilde{\chi}$, being a character of $G_{E/H}$, can only ramify at $w\in S_H$. Therefore by definition

$$\varepsilon(\widetilde{\chi}\cdot\alpha\circ N_{H/F},s) = \prod_{w\in S_H}\varepsilon(\widetilde{\chi}_w\cdot\alpha_v\circ N_{H_w/F_v},\psi_{H,w},\mu_{H,w},s)$$

where recall that $\alpha_{v_0}=1$ and so $\alpha_{v_0}\circ N_{H_{v_0}/F_{v_0}}=1$ and $c_{v_0}=1$ by choice. Since $\widetilde{\chi}(r_H(c)) = \prod_{w\in S_H}\widetilde{\chi}_w(r_{H_w}(c_v))$ we need to check that

$$\begin{aligned}\varepsilon(\widetilde{\chi}_{v_0},\psi_{H,v_0},\mu_{H,v_0},s) &= \varepsilon(\widetilde{\chi}_{v_0},\psi_{H,v_0},\mu_{H,v_0},s)\widetilde{\chi}_{v_0}(1)\\ &\quad\times\prod_{w\in S_H - v_0}\varepsilon(\widetilde{\chi}_w\alpha_v\circ N_{H_w/F_v},\psi_{H,w},\mu_{H,w},s)\widetilde{\chi}_w(c_v)\varepsilon(\alpha_v\circ N_{H_w/F_v},\psi_{H,w},\mu_{H,w},s)^{-1}\end{aligned}$$

for which is is enough to show that $\varepsilon(\widetilde{\chi}_w\alpha_v\circ N_{H_w/F_v},\psi_{H,w},\mu_{H,w},s)\widetilde{\chi}_w(c_v) = \varepsilon(\alpha_v\circ N_{H_w/F_v},\psi_{H,w},\mu_{H,w},s)$. Since $\mathrm{cond}(\alpha_v) = n_v \geq n_{E_w/L_v}$ this is implied by Lemma 9.8.

Property 2 and fact 2: The fact that $\varepsilon(\rho,\psi\circ\mathrm{Tr}_{M/K},\mu_M,s)$ extends to the Grothendieck group is automatic from the fact that $L(-,s)$, det and dim extend.

Property 3 and fact 3: We will show that $\varepsilon(\rho,\psi\circ\mathrm{Tr}_{M/K},r\mu_M,s) = r^{\dim\rho}\varepsilon(\rho,\psi\circ\mathrm{Tr}_{M/K},\mu_M,s)$ which also implies that if ρ has virtual dimension 0 then $\varepsilon(\rho,\psi\circ\mathrm{Tr}_{M/K},\mu_M,s)$ does not depend on μ_M.

Recall that $\mu_H = \otimes\mu_{H,v}$ gives volume 1 to $\mathbb{A}_H/H$. Let $r>0$ and $\mu_{H,r} = \otimes\mu_{H,r,w}$ with $\mu_{H,r,v_0} = r\mu_{H,v_0}$,

$\mu_{H,r,u} = r^{-1}\mu_{H,u}$ for some $u \in S_H - v_0$ above t and $\mu_{H,r,w} = \mu_{H,w}$ for $w \neq v_0, u$. Then

$$\begin{aligned}
\frac{\varepsilon(\rho, \psi \circ \mathrm{Tr}_{M/K}, r\mu_M, s)}{\varepsilon(\widetilde{\rho}\alpha \circ N_{H/F}, s) \det \rho(r_H(c))} &= \left(\prod_{w \in S_H - v_0} \varepsilon(\alpha_v \circ N_{H_w/F_v}, \psi_{F,v} \circ \mathrm{Tr}_{H_w/F_v}, \mu_{H,r,w}, s) \right)^{-\dim \rho} \\
&= \big(\varepsilon(\alpha_t \circ N_{H_u/F_t}, \psi_{F,t} \circ \mathrm{Tr}_{H_u/F_t}, r^{-1}\mu_{H,u}, s) \times \\
&\quad \times \prod_{w \in S_H - \{v_0, u\}} \varepsilon(\alpha_v \circ N_{H_w/F_v}, \psi_{F,v} \circ \mathrm{Tr}_{H_w/F_v}, \mu_{H,w}, s) \Big)^{-\dim \rho} \\
&= r^{\dim \rho} \left(\prod_{w \in S_H - v_0} \varepsilon(\alpha_v \circ N_{H_w/F_v}, \psi_{F,v} \circ \mathrm{Tr}_{H_w/F_v}, \mu_{H,w}, s) \right)^{-\dim \rho} \\
&= \frac{r^{\dim \rho} \varepsilon(\rho, \psi \circ \mathrm{Tr}_{M/K}, \mu_M, s)}{\varepsilon(\widetilde{\rho}\alpha \circ N_{H/F}, s) \det \rho(r_H(c))}
\end{aligned}$$

by Theorem 8.4.

Property 4: We have seen that

$$\begin{aligned}
\varepsilon(\rho, \psi(a \cdot -), \mu, s) &= \varepsilon(1, \psi(a \cdot -), \mu, s)^{\dim \rho} \prod \left(\frac{\varepsilon(\chi_i, \psi \circ \mathrm{Tr}_{L_i/K}(a \cdot -), \mu_i, s)}{\varepsilon(1, \psi \circ \mathrm{Tr}_{L_i/K}(a \cdot -), \mu_i, s)} \right)^{n_i} \\
&= (|a|_K^{(s-1)\dim \rho} \prod \chi_i(r_{L_i}(a))^{n_i}) \varepsilon(1, \psi, \mu, s)^{\dim \rho} \prod \left(\frac{\varepsilon(\chi_i, \psi \circ \mathrm{Tr}_{L_i/K}, \mu_i, s)}{\varepsilon(1, \psi \circ \mathrm{Tr}_{L_i/K}, \mu_i, s)} \right)^{n_i} \\
&= \det \rho(r_K(a)) |a|_K^{(s-1)\dim \rho} \varepsilon(\rho, \psi, \mu, s)
\end{aligned}$$

by Corollary 8.5 and the fact that if $\rho - \dim \rho \cdot 1 = \sum n_i \operatorname{Ind}_{L_i}^K(\chi_i - 1)$ then

$$\det \rho \circ r_K = \prod \chi_i (\mathrm{cor}_{L_i/K}^{\vee} \circ r_K)^{n_i} = \prod (\chi_i \circ r_{L_i})^{n_i}$$

Property 5 and fact 4: Suppose $L/M_1/M_2/K$ corresponds to $E/H_1/H_2/F$ and ρ is a virtual dimension 0 representation of G_{L/M_1} giving $\widetilde{\rho}$ of G_{E/H_1}. Then

$$\begin{aligned}
\varepsilon(\operatorname{Ind}_{M_1}^{M_2} \rho, \psi \circ \mathrm{Tr}_{M_2/K}, \mu, s) &= \varepsilon(\operatorname{Ind}_{H_1}^{H_2} \widetilde{\rho} \cdot \alpha \circ N_{H_2/F}, s) \det \operatorname{Ind}_{H_1}^{H_2} \widetilde{\rho}(r_{H_2}(c)) \\
&= \varepsilon(\operatorname{Ind}_{H_1}^{H_2}(\widetilde{\rho} \cdot \alpha \circ N_{H_1/F}), s) \det \widetilde{\rho}(\mathrm{cor}_{H_1/H_2}^{\vee} \circ r_{H_2}(c)) \\
&= \varepsilon(\widetilde{\rho} \cdot \alpha \circ N_{H_1/F}, s) \det \widetilde{\rho}(r_{H_1}(c)) \\
&= \varepsilon(\rho, \psi \circ \mathrm{Tr}_{M_1/K}, \mu_{M_1}, s)
\end{aligned}$$

since $\dim \operatorname{Ind}_{M_1}^{M_2} \rho = [M_1 : M_2] \dim \rho = 0$ and $\det \operatorname{Ind}_{H_1}^{H_2} \widetilde{\rho} = \widetilde{\rho} \circ \mathrm{cor}_{H_1/H_2}^{\vee}$ and $\mathrm{cor}_{H_1/H_2}^{\vee} \circ r_{H_2} = r_{H_1}$.

Certainly global L-functions are inductive in that if ρ is a representation of G_{E/H_1} then $L(\operatorname{Ind}_{H_1}^{H_2} \rho, s) = L(\rho, s)$ and therefore $\varepsilon(\operatorname{Ind}_{H_1}^{H_2} \rho, s) = \varepsilon(\rho, s)$. Moreover, $\det \operatorname{Ind}_{H_1}^{H_2} \rho =$ and $\dim \operatorname{Ind}_{H_1}^{H_2} \rho = [H_1 : H_2] \dim \rho$. Note that while the character ψ does not seem to appear in the formulae, it does as c is defined in terms of ψ.

Property 6: Let $n(\rho, \psi)$ be such that $\varepsilon(\rho, \psi, \mu, s) = \varepsilon(\rho, \psi, \mu, 0) q_K^{-n(\rho,\psi)s}$. We know from Theorem 8.4 that $n(\chi, \psi) = \mathrm{cond}(\chi) - \mathrm{cond}(\psi)$. Also property 2 implies that $n(\rho_1 \oplus \rho_2, \psi) = n(\rho_1, \psi) + n(\rho_2, \psi)$ and so $n(-, \psi)$ extends to the Grothendieck group. Now suppose L/K is a finite extension and χ is a character of $L^\times$. Then property 5 gives $n(\operatorname{Ind}_L^K(\chi - 1), \psi) = f_{L/K} n(\chi - 1, \psi \circ \mathrm{Tr}_{L/K})$ since $q_L = q_K^{f_{L/K}}$. Thus if

$\rho - \dim\rho\cdot 1 = \sum n_i \operatorname{Ind}_{L_i}^K(\chi_i - 1)$ then

$$\begin{aligned} n(\rho,\psi) &= (\dim\rho)n(1,\psi) + \sum n_i n(\operatorname{Ind}_{L_i}^K(\chi_i-1),\psi) \\ &= (\dim\rho)n(1,\psi) + \sum n_i f_{L_i/K} n(\chi_i - 1, \psi\circ\operatorname{Tr}_{L_i/K}) \\ &= -(\dim\rho)\operatorname{cond}(\psi) + \sum n_i f_{L_i/K}\operatorname{cond}(\chi_i) \end{aligned}$$

because $n(1,\psi) = -\operatorname{cond}(\psi) + \operatorname{cond}(1) = -\operatorname{cond}(\psi)$ and $n(\chi-1,\psi\circ\operatorname{Tr}_{L/K}) = \operatorname{cond}(\chi) - \operatorname{cond}(1) = \operatorname{cond}(\chi)$. The result now follows from the computation

$$\begin{aligned} \operatorname{cond}(\rho) &= \operatorname{cond}(\rho - \dim\rho\cdot 1) \\ &= \sum n_i \operatorname{cond}(\operatorname{Ind}_{L_i}^K(\chi_i - 1)) \\ &= \sum n_i f_{L_i/K}(\operatorname{cond}(\chi_i) + v_{L_i}(\mathcal{D}_{L_i/K}) - \operatorname{cond}(1) - v_{L_i}(\mathcal{D}_{L_i/K}) \\ &= \sum n_i f_{L_i/K}\operatorname{cond}(\chi_i) \end{aligned}$$

using the fact that $\operatorname{cond}(\operatorname{Ind}_L^K\rho) = f_{L/K}(\operatorname{cond}(\rho) + \dim\rho\, v_L(\mathcal{D}_{L/K}))$.

Property 7: As before if $\rho - \dim\rho\cdot 1 = \sum n_i \operatorname{Ind}_{L_i}^K(\chi_i - 1)$ then

$$\varepsilon(\rho\otimes\chi,\psi,\mu,s) = \varepsilon(\chi,\psi,\mu,s)^{\dim\rho}\prod\left(\frac{\varepsilon(\chi_i\cdot\chi\circ N_{L_i/K},\psi\circ\operatorname{Tr}_{L_i/K},\mu_i,s)}{\varepsilon(\chi\circ N_{L_i/K},\psi\circ\operatorname{Tr}_{L_i/K},\mu_i,s)}\right)^{n_i}$$

If $\operatorname{cond}(\chi) = f \geq n_{L/K}$ then Lemma 9.8 gives $\varepsilon(\chi_i\cdot\chi\circ N_{L_i/K},\psi\circ\operatorname{Tr}_{L_i/K},\mu_i,s) = \chi_i(c)^{-1}\varepsilon(\chi\circ N_{L_i/K},\psi\circ\operatorname{Tr}_{L_i/K},\mu_i,s)$. Thus

$$\begin{aligned} \varepsilon(\rho\otimes\chi,\psi,\mu,s) &= \varepsilon(\chi,\psi,\mu,s)^{\dim\rho}\prod\chi_i(r_{L_i}(c))^{-n_i} \\ &= \varepsilon(\chi,\psi,\mu,s)^{\dim\rho}\prod\chi_i(\operatorname{cor}_{L_i/K}^{\vee}\circ r_K(c))^{-n_i} \\ &= \varepsilon(\chi,\psi,\mu,s)^{\dim\rho}\det\rho(r_K(c))^{-1} \end{aligned}$$

as desired. □

References

[AT09] Emil Artin and John Tate, *Class field theory*, AMS Chelsea Publishing, Providence, RI, 2009, Reprinted with corrections from the 1967 original. MR 2467155 (2009k:11001)

[CF86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original. MR 911121 (88h:11073)

[Mil13] J.S. Milne, *Class field theory (v4.02)*, 2013, Available at www.jmilne.org/math/, pp. 281+viii.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859 (2000m:11104)

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR 2392026 (2008m:11223)

[Tat67] J. T. Tate, *Fourier analysis in number fields, and Hecke's zeta-functions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 305–347. MR 0217026 (36 #121)

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575 (97h:11130)