

Galois Cohomology and Applications

Shiva Chidambaram, discussed with Prof. Frank Calegari

March 17, 2017

1 Notations and Preliminaries

We start with some notation. For any field extension $K|F$, $G_{K|F}$ denotes the Galois group $\text{Gal}(K|F)$. For any field K , $\bar{K}$ denotes the separable closure of K , and G_K denotes $\text{Gal}(\bar{K}|K)$. If K is a local field, I_K denotes the inertia subgroup $\text{Gal}(\bar{K}|K^{ur})$, where K^{ur} is the maximal unramified extension of K . If K is a number field and l is a prime in K , G_l denotes the absolute Galois group of the completion K_l , and if l is finite, I_l denotes the inertia subgroup. Depending on our choice of embedding $\bar{K} \hookrightarrow \bar{K}_l$, we can regard G_l as a subgroup of G_K in different ways. This choice doesn't affect any of our statements. Also, if S is a finite set of places of a number field K , K_S denotes the maximal extension of K unramified outside S , and $G_{K,S}$ denotes the corresponding Galois group $\text{Gal}(K_S|K)$.

For any finite group G and a G -module M , unless we are dealing with Global Euler Characteristic formula or Wiles-Greenberg formula, $H^0(G, M)$ will denote the modified Tate cohomology group $M^G/N_G(M)$ rather than the usual M^G . In the two exceptional cases, we will use $\hat{H}^0(G, M)$ to denote the modified Tate cohomology groups, distinguishing it from the normal cohomology groups $H^0(G, M)$.

The dual of an abelian group A is $A^\vee = \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$. For any two G -modules M and N , the abelian group $\text{Hom}(M, N)$ is a G -module with $(g \cdot f)(m) = g \cdot (f(g^{-1} \cdot m))$. We will talk exclusively about Galois modules. In that context, the notion of a dual module is as follows. If $K|F$ is a Galois extension, and M is a $G_{K|F}$ -module, then the dual module M^* is defined as $M^* = \text{Hom}(M, \mu)$, where μ is the $G_{K|F}$ -submodule of $K^\times$ consisting of the roots of unity. If M is finite, then $M^* = \text{Hom}(M, K^\times)$.

Let G be a group, and M, N, P be G -modules such that there is a G -module pairing

$$\phi : M \otimes N \longrightarrow P.$$

This induces a pairing between cohomology groups, called the cup product.

$$H^i(G, M) \times H^j(G, N) \longrightarrow H^{i+j}(G, P)$$

We will only be interested in the case $i+j=2$. If $x \in H^0(G, M)$ and $f \in H^2(G, N)$, then $x \cup f \in H^2(G, P)$ is represented by the cocycle $x \cup f : G \times G \rightarrow P; (g_1, g_2) \mapsto \phi(x \otimes f(g_1, g_2))$. The cup product pairing between $H^2(G, M)$ and $H^0(G, N)$ is defined similarly. If $f_1 \in H^1(G, M)$ and $f_2 \in H^1(G, N)$, then $f_1 \cup f_2 \in H^2(G, P)$ is represented by the cocycle $f_1 \cup f_2 : G \times G \rightarrow P; (g_1, g_2) \mapsto \phi(f_1(g_1) \otimes g_1 f_2(g_2))$.

2 Galois Cohomology

This treatment of Galois Cohomology follows [1] and [5]. The cohomology $H^*(G_F, M)$ of a module M for G_F , is sometimes denoted $H^*(F, M)$. This shouldn't be confusing because we will only have Galois groups acting on modules. We will start by stating some fundamental theorems in the subject. Proofs can be found in [3].

Theorem 1.

Local Tate duality: Let K be a p -adic local field and M be a finite G_K module. Then

1. *the groups $H^i(G_K, M)$ are finite for all i , and zero for all $i \geq 3$.*
2. *for $i = 0, 1, 2$, the cup product pairing*

$$H^i(G_K, M) \times H^{2-i}(G_K, M^*) \longrightarrow H^2(G_K, \mu) = \mathbb{Q}/\mathbb{Z}$$

induced by the natural pairing between M and M^* is non-degenerate. So, they are duals of each other.

3. *If p does not divide $\#M$, then $H^i(G_K/I_K, M^{I_K})$ and $H^{2-i}(G_K/I_K, M^{*I_K})$ are the exact annihilators of each other in the above pairing.*

If K is an Archimedean local field, 1 and 2 still hold. We note that since G_K is finite in this case, these are actually the modified Tate cohomology groups. $\square$

Theorem 2.

Local Euler Characteristic formula: Let K be a finite extension of $\mathbb{Q}_p$, and M be a finite G_K module. Then,

$$\frac{\#H^0(G_K, M)\#H^2(G_K, M)}{\#H^1(G_K, M)} = |\#M|_K = p^{-[K:\mathbb{Q}_p] \cdot \text{ord}_p(\#M)} \quad \square$$

Theorem 3.

Global Euler Characteristic formula: Let K be a number field and M be a finite G_K module. Let S be a finite set of places consisting of all infinite places, all places at which M is ramified, and all places at which $\#M$ has positive order. Then $G_{K,S}$ acts on M and we have

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

(We note that these are the unmodified cohomology groups.)

Let Σ be a finite set of primes in $\mathbb{Q}$ and X be a $G_\Sigma = G_{\mathbb{Q}, \Sigma}$ -module. This is the same as saying, X is a $G_{\mathbb{Q}}$ -module that is unramified outside Σ . It can be shown that the cohomology $H^1(G_\Sigma, X)$ is isomorphic to the subgroup of $H^1(G_{\mathbb{Q}}, X)$ consisting of classes that are unramified outside Σ , i.e.,

$$H^1(G_\Sigma, X) \simeq \ker \left(H^1(G_{\mathbb{Q}}, X) \longrightarrow \prod_{l \notin \Sigma} H^1(I_l, X) \right). \quad (2.1)$$

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

When X is a finite $G_{\mathbb{Q}}$ -module, the kernel of the Galois action is a finite index subgroup and hence is equal to G_L for some number field L . Hence, X is unramified at all primes unramified in L . So, if we let Σ to be the set consisting of all the infinite primes, primes dividing $\#X$, and primes at which X is ramified, then Σ is finite and X is a G_Σ -module. In this case, there is a nine-term exact sequence involving $H^i(G_\Sigma, X)$ and $H^i(G_\Sigma, X^*)^\vee$ called the Poitou Tate sequence, that we will study next. Though we state the theorems in the situation with base field $\mathbb{Q}$, all of it applies for any number field K . The general result will be used in the next section in an application to Iwasawa theory.

Let X and Σ be as above. Then, for each i , we have a map

$$\alpha_{i,X} : H^i(G_\Sigma, X) \longrightarrow \prod_{v \in \Sigma} H^i(G_v, X)$$

We can consider the corresponding map α_{i,X^*} for the module X^* . We remark here that X^* is also unramified at all $v \notin \Sigma$. Dualizing this map, and using Local Tate duality for each $v \in \Sigma$, we get the following map

$$\beta_{2-i} : \prod_{v \in \Sigma} H^{2-i}(G_v, X) \longrightarrow H^i(G_\Sigma, X^*)^\vee.$$

Proposition 1.

There is a non-degenerate pairing $\ker \alpha_{1,X^*} \times \ker \alpha_{2,X} \longrightarrow \mathbb{Q}/\mathbb{Z}$. □

Proposition 2.

$\alpha_{0,X}$ is injective, β_2 is surjective and $\ker \beta_r = \text{Im } \alpha_{r,X}$. □

The proofs of the above propositions can be found in [3]. Putting these together, we get the Poitou Tate exact sequence.

Theorem 4.

Poitou-Tate: The following nine term sequence is exact

$$\begin{aligned} 0 \longrightarrow H^0(G_\Sigma, X) &\xrightarrow{\alpha_{0,X}} \prod_{v \in \Sigma} H^0(G_v, X) \xrightarrow{\beta_0} H^2(G_\Sigma, X^*)^\vee \\ &\xrightarrow{\gamma_1} H^1(G_\Sigma, X) \xrightarrow{\alpha_{1,X}} \prod_{v \in \Sigma} H^1(G_v, X) \xrightarrow{\beta_1} H^1(G_\Sigma, X^*)^\vee \\ &\xrightarrow{\gamma_2} H^2(G_\Sigma, X) \xrightarrow{\alpha_{2,X}} \prod_{v \in \Sigma} H^2(G_v, X) \xrightarrow{\beta_2} H^0(G_\Sigma, X^*)^\vee \longrightarrow 0 \end{aligned}$$

where γ_1 and γ_2 are the following maps induced by the non-degenerate pairing in Proposition 1.

$$\begin{aligned} \gamma_1 : H^2(G_\Sigma, X^*)^\vee &\twoheadrightarrow (\ker \alpha_{2,X^*})^\vee \xrightarrow{\simeq} \ker \alpha_{1,X} \hookrightarrow H^1(G_\Sigma, X), \\ \gamma_2 : H^1(G_\Sigma, X^*)^\vee &\twoheadrightarrow (\ker \alpha_{1,X^*})^\vee \xrightarrow{\simeq} \ker \alpha_{2,X} \hookrightarrow H^2(G_\Sigma, X). \end{aligned}$$

□

Using the Poitou Tate exact sequence, one can deduce the Wiles-Greenberg formula for generalised Selmer groups. Let X be a finite $G_{\mathbb{Q}}$ -module. For each place v of $\mathbb{Q}$, let L_v be a given subgroup of $H^1(G_v, X)$ such that for all but finitely many places, L_v is the subgroup $H^1(G_v/I_v, X^{I_v})$ of unramified cohomology classes. The generalized Selmer group $H_{\mathcal{L}}^1(G_{\mathbb{Q}}, X)$ for the given set $\mathcal{L} = \{L_v\}$ of local conditions, is defined as

$$\begin{aligned} H_{\mathcal{L}}^1(G_{\mathbb{Q}}, X) &= \ker \left(H^1(G_{\mathbb{Q}}, X) \longrightarrow \prod_v H^1(G_v, X)/L_v \right) \\ &= \{x \in H^1(G_{\mathbb{Q}}, X) \mid \text{res}_v(x) \in L_v \text{ for all } v\} \end{aligned} \tag{2.2}$$

where $\text{res}_v : H^1(G_{\mathbb{Q}}, X) \rightarrow H^1(G_v, X)$ is the restriction map for each place v . We will also sometimes use $H_{\mathcal{L}}^1(\mathbb{Q}, X)$ to denote this Selmer group. For each v , let $L_v^\perp$ be the exact annihilator of L_v under the local Tate pairing. By part 3 of Theorem 1, we have $L_v^\perp = H^1(G_v/I_v, X^{*I_v})$ for all but finitely many v . The collection $\{L_v^\perp\}$ is called the dual set of local conditions, and denoted $\mathcal{L}^*$.

Theorem 5.

Wiles - Greenberg: The group $H_{\mathcal{L}}^1(G_{\mathbb{Q}}, X)$ is finite and we have the following formula relating the cardinality of $H_{\mathcal{L}}^1(G_{\mathbb{Q}}, X)$ and $H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, X^*)$.

$$\frac{\#H_{\mathcal{L}}^1(G_{\mathbb{Q}}, X)}{\#H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, X^*)} = \frac{\#H^0(G_{\mathbb{Q}}, X)}{\#H^0(G_{\mathbb{Q}}, X^*)} \prod_v \frac{\#L_v}{\#H^0(G_v, X)} \tag{2.3}$$

(Note that these are the unmodified cohomology groups. We use $\hat{H}$ to denote the Tate cohomology groups in this proof.)

Proof. Let Σ be the finite set consisting of all the infinite places, finite primes dividing $\#X$, primes at which X is ramified, and finite places at which $L_v \neq H^1(G_v/I_v, X)$. Then, by definitions 2.1 and 2.2, and exactness of inflation restriction sequence, we get that $H^1_{\mathcal{L}}(G_{\mathbb{Q}}, X)$ is a subgroup of $H^1(G_{\Sigma}, X)$ and hence it is finite. Furthermore, we have an exact sequence

$$0 \longrightarrow H^1_{\mathcal{L}^*}(G_{\mathbb{Q}}, X^*) \longrightarrow H^1(G_{\Sigma}, X^*) \longrightarrow \prod_{v \in \Sigma} H^1(G_v, X^*)/L_v^{\perp}$$

Taking the dual, and using part 3 of Theorem 1, we get the exact sequence

$$\prod_{v \in \Sigma} L_v \longrightarrow H^1(G_{\Sigma}, X^*)^{\vee} \longrightarrow H^1_{\mathcal{L}^*}(G_{\mathbb{Q}}, X^*)^{\vee} \longrightarrow 0 \quad (2.4)$$

Now, we observe that $\ker \alpha_{1,X}$, in the Poitou Tate sequence, is in fact a subgroup of $H^1_{\mathcal{L}}(G_{\mathbb{Q}}, X)$, and hence γ_1 maps in to the subgroup $H^1_{\mathcal{L}}(G_{\mathbb{Q}}, X)$ of $H^1(G_{\Sigma}, X)$. Thus, we can take an initial segment of the Poitou Tate sequence and combine it with the sequence 2.4 using the above observation to get the following exact sequence.

$$\begin{aligned} 0 \longrightarrow H^0(G_{\Sigma}, X) &\xrightarrow{\alpha_{0,X}} \prod_{v \in \Sigma} \hat{H}^0(G_v, X) \xrightarrow{\beta_0} H^2(G_{\Sigma}, X^*)^{\vee} \xrightarrow{\gamma_1} H^1_{\mathcal{L}}(G_{\mathbb{Q}}, X) \\ &\xrightarrow{\alpha_{1,X}} \prod_{v \in \Sigma} L_v \longrightarrow H^1(G_{\Sigma}, X^*)^{\vee} \longrightarrow H^1_{\mathcal{L}^*}(G_{\mathbb{Q}}, X^*)^{\vee} \longrightarrow 0 \end{aligned}$$

Noting that all the terms are finite groups, and the cardinality of a finite group is equal to that of its dual, we get

$$\begin{aligned} \frac{\#H^1_{\mathcal{L}}(G_{\mathbb{Q}}, X)}{\#H^1_{\mathcal{L}^*}(G_{\mathbb{Q}}, X^*)} &= \frac{\#H^0(G_{\Sigma}, X) \#H^2(G_{\Sigma}, X^*)}{\#H^1(G_{\Sigma}, X^*)} \prod_{v \in \Sigma} \frac{\#L_v}{\#\hat{H}^0(G_v, X)} \\ &= \frac{\#H^0(G_{\mathbb{Q}}, X)}{\#H^0(G_{\mathbb{Q}}, X^*)} \prod_{v \in \Sigma} \frac{\#L_v}{\#H^0(G_v, X)} \frac{\#H^0(G_{\Sigma}, X^*) \#H^2(G_{\Sigma}, X^*) \#N_{G_{\mathbb{R}}}(X)}{\#H^1(G_{\Sigma}, X^*)} \end{aligned}$$

where we have used $H^0(G_{\Sigma}, X) = H^0(G_{\mathbb{Q}}, X)$ and $H^0(G_{\Sigma}, X^*) = H^0(G_{\mathbb{Q}}, X^*)$. So, the proof reduces to showing that the last factor is equal to 1. This is obtained from the global Euler characteristic formula and the observation that $N_{G_{\mathbb{R}}}(X)$ and $H^0(G_{\mathbb{R}}, X^*)$ are the exact annihilators of each other in the non-degenerate pairing $X \times X^* \rightarrow \mu$. $\square$

3 Applications to Iwasawa Theory

The following is a basic theorem in Iwasawa Theory.

Theorem 6.

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 , the Leopold defect, satisfies $0 \leq \delta_K \leq r_1 + r_2 - 1$.

Leopold's conjecture says that $\delta_K = 0$ always. It has been proved for the cases $K = \mathbb{Q}$ and K is an imaginary quadratic field. In particular, this means that there is a unique $\mathbb{Z}_p$ extension of $\mathbb{Q}$. This is called the cyclotomic $\mathbb{Z}_p$ extension $\mathbb{Q}_{\infty}$ and is obtained as follows. For each $n \in \mathbb{N}$, $\mathbb{Q}(\zeta_{p^n})$ is an abelian extension of $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/(p-1) \times \mathbb{Z}/p^{n-1}$. If we let $\mathbb{Q}_n$ be the fixed

field of the subgroup $\mathbb{Z}/(p-1)$, then the sequence $\mathbb{Q}_n$ forms a tower of Galois field extensions of $\mathbb{Q}$ with $G_{\mathbb{Q}_n|\mathbb{Q}} \simeq \mathbb{Z}/p^n$. Then, $\mathbb{Q}_\infty = \bigcup_{n=1}^{\infty} \mathbb{Q}_n$. For any number field K , the compositum $K \cdot \mathbb{Q}_\infty$ is a $\mathbb{Z}_p$ extension of K . It is called the cyclotomic $\mathbb{Z}_p$ extension of K .

We give a proof of the above theorem using Galois cohomology. There are a few propositions that we will need, including the Global Euler Characteristic formula for finitely generated modules. We state these below. Proofs can be found in [5].

Proposition 3.

Let $K|\mathbb{Q}_l$ be a finite extension and $K_\infty|K$ be a $\mathbb{Z}_p$ extension. If $p \neq l$, then K_∞ is the unique unramified extension with Galois group isomorphic to $\mathbb{Z}_p$. If $p = l$, there are exactly $[K : \mathbb{Q}_l] + 1$ independent such extensions. $\square$

Proposition 4.

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

$$\text{rank}_{\mathbb{Z}_p} H^1(G, \mathbb{Z}_p) = \text{rank}_{\mathbb{Z}_p} H^1(H, \mathbb{Z}_p). \quad \square$$

Proposition 5.

Global Euler Characteristic formula: Let K be a number field, and M be a finitely generated $\mathbb{Z}_p$ -module with a G_K action. Let S be a finite set of places of K consisting of all infinite places, all places at which M is ramified and all places above p . Suppose $G_{K,S}$ acts on M . Then, we have

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

Proof. (of Theorem 6). Let K_∞ be a $\mathbb{Z}_p$ extension of K . Let v be any place of K above $l \neq p$, and w be a place of K_∞ above v . Then, $K_{\infty,w}|K_v$ is a $\mathbb{Z}_p$ extension, and by proposition 3, it is unramified. Let S be the set consisting of all infinite places of K , and all places of K lying above p . Then, any $\mathbb{Z}_p$ extension of K is unramified outside the set S . Let K^p be the compositum of all $\mathbb{Z}_p$ extensions of K . Then $K^p \subset K_S$ and $G_{K^p|K}$ is a quotient of $G_{K,S} = \text{Gal}(K_S|K)$. The number of independent $\mathbb{Z}_p$ extensions of K is given by $\text{rank}_{\mathbb{Z}_p} H^1(G_{K^p|K}, \mathbb{Z}_p)$.

The group $G_{K^p|K}$ is the maximal abelian pro- p torsion free subquotient of $G_{K,S}$. Hence, by proposition 4,

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

By Proposition 5, we get

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

So, $\delta_K = \text{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Z}_p)$ and we have to show $0 \leq \delta_K \leq r_1 + r_2 - 1$. If $\delta_K = r$, i.e., $H^2(G_{K,S}, \mathbb{Z}_p) \simeq \mathbb{Z}_p^r \oplus M$ where M is the torsion part, then

$$\begin{aligned} H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee &\simeq \left(H^2(G_{K,S}, \mathbb{Z}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^\vee \simeq \left((\mathbb{Z}_p \otimes \mathbb{Q}_p/\mathbb{Z}_p)^r \oplus (M \otimes \mathbb{Q}_p/\mathbb{Z}_p) \right)^\vee \\ &\simeq \left((\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus 0 \right)^\vee \\ &\simeq \left((\mathbb{Q}_p/\mathbb{Z}_p)^\vee \right)^r \simeq \mathbb{Z}_p^r \end{aligned}$$

Hence, we will show the necessary bound for $\text{rank}_{\mathbb{Z}_p} H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee$.

A part of the Tate Poitou exact sequence for the $G_{K,S}$ module $\mu_{p^n} \subset K_S^\times$ reads

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

We now take projective limit of the above sequence over the maps $\mu_{p^{n+1}} \rightarrow \mu_{p^n}; \zeta \mapsto \zeta^p$. For each finite place $v \in S$, since the ramification index $e_{K_v|\mathbb{Q}_p}$ is finite, we have $\mu_{p^\infty}(K_v)$ is finite. Remembering that, at the infinite places we are working with the modified Tate cohomology groups, we deduce that $\varprojlim H^0(G_{K_v}, \mu_{p^n}) = 0$ for all $v \in S$. We also have

$$\begin{aligned} \varprojlim H^2(G_{K,S}, \mathbb{Z}/p^n)^\vee &\simeq (\varprojlim H^2(G_{K,S}, \mathbb{Z}/p^n))^\vee \simeq (H^2(G_{K,S}, \varprojlim \mathbb{Z}/p^n))^\vee \\ &\simeq (H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p))^\vee. \end{aligned}$$

Finally, by Kummer theory, we get $H^1(G_{K_v}, \mu_{p^n}) \simeq K_v^\times / (K_v^\times)^{p^n} \simeq K_v^\times \otimes \mathbb{Z}/p^n$. Therefore $\varprojlim H^1(G_{K_v}, \mu_{p^n}) \simeq \varprojlim K_v^\times \otimes \mathbb{Z}/p^n \simeq K_v^\times \otimes \mathbb{Z}_p$. Putting everything together, we have

$$0 \rightarrow (H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p))^\vee \rightarrow \varprojlim H^1(G_{K,S}, \mu_{p^n}) \rightarrow \prod_{v \in S} K_v^\times \otimes \mathbb{Z}_p \quad (3.1)$$

By studying the cohomology of the following exact sequence of $G_{K,S}$ -modules

$$1 \rightarrow \varprojlim_{L \subseteq K_S} \mathcal{O}_{L,S}^\times \rightarrow \varprojlim_{L \subseteq K_S} \prod_{v|S} L_v^\times \rightarrow \varprojlim_{L \subseteq K_S} \prod_{v|S} L_v^\times / \mathcal{O}_{L,S}^\times \rightarrow 1$$

where L varies over all finite subextensions of $K_S|K$, and $\mathcal{O}_{L,S}^\times$ is the multiplicative group of units in the ring of S -integers of L , and using the relation between the S -idele class group and the S -ideal class group, one can show the following isomorphism. We refer to [5] and [6] for the computations.

$$\varprojlim H^1(G_{K,S}, \mu_{p^n}) \simeq \mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p \quad (3.2)$$

We can substitute this back into the exact sequence 3.1 to get

$$0 \rightarrow (H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p))^\vee \rightarrow \mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p \rightarrow \prod_{v \in S} K_v^\times \otimes \mathbb{Z}_p \quad (3.3)$$

We also have the exact sequence $0 \rightarrow \mathcal{O}_K^\times \rightarrow \mathcal{O}_{K,S}^\times \rightarrow \prod_{v \in S, v \nmid \infty} K_v^\times / \mathcal{O}_{K_v}^\times$, which after tensoring by the flat $\mathbb{Z}$ -module $\mathbb{Z}_p$, gives the exact sequence

$$0 \rightarrow \mathcal{O}_K^\times \otimes \mathbb{Z}_p \rightarrow \mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p \rightarrow \prod_{v \in S, v \nmid \infty} K_v^\times / \mathcal{O}_{K_v}^\times \otimes \mathbb{Z}_p$$

From the exactness of the above sequence at the second term, we can deduce that in the sequence 3.3, the image of the injective map $(H^2(G_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p))^\vee \rightarrow \mathcal{O}_{K,S}^\times \otimes \mathbb{Z}_p$ infact lands inside $\mathcal{O}_K^\times \otimes \mathbb{Z}_p$. Hence

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

□

4 Reflection theorems

A reflection theorem is one of a collection of theorems linking the sizes of different ideal class groups or different isotypic components of a class group. The first such theorem is due to Kummer and is stated below.

Theorem 7.

Kummer's reflection theorem: Let p be an odd prime, $F = \mathbb{Q}(\zeta_p)$ and let $F^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be the totally real subfield. If $h = \#Cl_F$, $h^+ = \#Cl_{F^+}$, then $h^+ | h$ and if we let $h^- = h/h^+$, then $p | h^+ \implies p | h^-$.

In this section we will prove a reflection theorem relating the sizes of different isotypic components of the class group of the p^{th} cyclotomic field $F = \mathbb{Q}(\zeta_p)$, where p is an odd prime. This is Theorem 10.9 of [2], and is a strengthening of Kummer's reflection theorem. Our proof of this theorem is different from that in [2], and involves interpreting the different isotypic components in terms of Selmer groups and using Wiles-Greenberg formula. The following theorem due to Scholz can also be proved using this method.

Theorem 8.

Scholz reflection theorem: Let d be a positive square-free natural number. Let $F^+ = \mathbb{Q}(\sqrt{d})$ and $F^- = \mathbb{Q}(\sqrt{-3d})$. Then,

$$\text{rank}_3 Cl_{F^+} \leq \text{rank}_3 Cl_{F^-} \leq \text{rank}_3 Cl_{F^+} + 1.$$

(The p -rank of a finite abelian group A , denoted $\text{rank}_p A$, is equal to $\dim_{\mathbb{F}_p} A/pA$.)

Let p be an odd prime, let $F = \mathbb{Q}(\zeta_p)$ be the p^{th} cyclotomic field, and let A be the p -Sylow subgroup of the class group Cl_F . Then, A is a $\mathbb{Z}_p$ -module with an action of $G_{F|\mathbb{Q}}$. Let $\epsilon : G_{F|\mathbb{Q}} \rightarrow \mathbb{Z}_p^\times$ be the cyclotomic character. Then, the elements

$$e_i = \frac{1}{p-1} \sum_{\sigma \in G_{F|\mathbb{Q}}} \epsilon^i(\sigma) \sigma^{-1}, \quad \text{for } 0 \leq i < p-1$$

are idempotents of the group ring $\mathbb{Z}_p[G_{F|\mathbb{Q}}]$, and give a decomposition of a $G_{F|\mathbb{Q}}$ -module into its various isotypic components. In our case, this gives us a decomposition

$$A = A(0) \oplus A(1) \oplus A(2) \oplus \cdots \oplus A(p-2),$$

where, for each $0 \leq i < p-1$, $A(i) = e_i \cdot A$ is the subgroup of A on which $G_{F|\mathbb{Q}}$ acts by the character ϵ^i . By class field theory, A is isomorphic to the Galois group over F of the maximal abelian unramified p -extension of F , and $A(i)$ is isomorphic to the Galois group of the maximal abelian unramified p -extension of F on which $G_{F|\mathbb{Q}}$ acts by the character ϵ^i . So, the p -rank of $A(i)$, which is equal to $\dim_{\mathbb{F}_p} A(i)/pA(i)$, is the maximum number of independent $\mathbb{Z}/p$ -extensions K of F , that are unramified and are such that $G_{K|F} \simeq \epsilon^i$ as $G_{F|\mathbb{Q}}$ -modules.

Now, consider the $G_{\mathbb{Q}}$ -module $\mathbb{Z}/p$ with the action given by ϵ^i thought of as taking values in $(\mathbb{Z}/p)^\times$. So, in particular, the action is through the quotient $G_{F|\mathbb{Q}}$. We will denote this module simply by ϵ^i . The dual module is $\mathbb{Z}/p$ with action given by ϵ^{1-i} , and we will denote it simply as ϵ^{1-i} . Let's look at the following set of local conditions $\mathcal{L}_i = \{L_{i,v}\}$.

$$L_{i,v} = \begin{cases} 0 & \text{if } v = p, \infty \\ H^1(G_v/I_v, (\epsilon^i)^{I_v}) & \text{otherwise} \end{cases}$$

The set $\mathcal{L}_i^* = \{L_{i,v}^\perp\}$ of dual local conditions is as follows.

$$L_{i,v}^\perp = \begin{cases} H^1(G_p, \epsilon^{1-i}) & \text{if } v = p \\ H^1(G_{\mathbb{R}}, \epsilon^{1-i}) = 0 & \text{if } v = \infty \\ H^1(G_v/I_v, (\epsilon^{1-i})^{I_v}) & \text{otherwise} \end{cases}$$

The corresponding Selmer groups are related to the isotypic components $A(i)$, which will be explained below. The inflation restriction exact sequence gives an isomorphism

$$H^1(G_{\mathbb{Q}}, \epsilon^i) \xrightarrow{\simeq} H^1(G_F, \epsilon^i)^{G_{F|\mathbb{Q}}} = \text{Hom}(G_F, \epsilon^i)^{G_{F|\mathbb{Q}}} = \text{Hom}_{G_{F|\mathbb{Q}}}(G_F, \epsilon^i) \quad (4.1)$$

Let f be a crossed homomorphism $G_{\mathbb{Q}} \rightarrow \epsilon^i$ representing a cohomology class in $H^1(G_{\mathbb{Q}}, \epsilon^i)$. Restricting to G_F gives a $G_{F|\mathbb{Q}}$ -module homomorphism $G_F \rightarrow \epsilon^i$. Assuming it is non-trivial, its kernel is an index p subgroup of G_F , and thus determines a $\mathbb{Z}/p$ -extension K_f of F , with $G_{K_f|F} \simeq \epsilon^i$ as a $G_{F|\mathbb{Q}}$ -module.

The cohomology class of f belongs to $H^1_{\mathcal{L}_i}(\mathbb{Q}, \epsilon^i)$ if and only if the extension $K_f|F$ is unramified at all places, and split at all primes above p and ∞ . There is no real prime above ∞ in $F|\mathbb{Q}$, and p is totally ramified in $F|\mathbb{Q}$ with the only prime ideal above p being the principal ideal generated by $1 - \zeta_p$. Therefore, by class field theory, in any finite unramified extension of F , all primes above p and ∞ are split. So, the latter two conditions are redundant. Hence, a non-trivial class $[f]$ in $H^1_{\mathcal{L}_i}(\mathbb{Q}, \epsilon^i)$ determines an unramified $\mathbb{Z}/p$ -extension $K_f|F$ such that $G_{K_f|F} \simeq \epsilon^i$ as a $G_{F|\mathbb{Q}}$ -module, and conversely every class in $H^1_{\mathcal{L}_i}(\mathbb{Q}, \epsilon^i)$ is determined up to a multiple, by such an extension. Therefore, we have

$$\text{rank}_p A(i) = \dim_{\mathbb{F}_p} H^1_{\mathcal{L}_i}(\mathbb{Q}, \epsilon^i) \quad (4.2)$$

With the above setup, we are now ready to state and prove the theorem we mentioned at the start of the section.

Theorem 9.

$A(0) = A(1) = 0$. Further if $i \neq 0$ is even and j is odd with $j \equiv 1 - i \pmod{p-1}$, then

$$\text{rank}_p A(i) \leq \text{rank}_p A(j) \leq \text{rank}_p A(i) + 1$$

Proof. We first consider the two easy cases $A(0)$ and $A(1)$. If $A(0) \neq 0$, then by class field theory, there exists an unramified $\mathbb{Z}/p$ extension K of $F = \mathbb{Q}(\zeta_p)$, such that $G_{K|F} \simeq \mathbb{Z}/p$ as a $G_{F|\mathbb{Q}}$ -module. Since $G_{F|\mathbb{Q}}$ acts trivially on $G_{K|F}$ and the two groups have coprime order, the exact sequence

$$0 \rightarrow G_{K|F} \rightarrow G_{K|\mathbb{Q}} \rightarrow G_{F|\mathbb{Q}} \rightarrow 0$$

is split, and moreover, $G_{K|\mathbb{Q}}$ is isomorphic to the direct product $G_{K|F} \times G_{F|\mathbb{Q}} \simeq \mathbb{Z}/p \times (\mathbb{Z}/p)^\times$. Hence, the subfield of K that is fixed by the subgroup $(\mathbb{Z}/p)^\times$ of $G_{K|\mathbb{Q}}$, is an unramified $\mathbb{Z}/p$ extension of $\mathbb{Q}$. But, there are no non-trivial unramified extensions of $\mathbb{Q}$, which tells us that this cannot happen. Hence, $A(0)$ must be 0. In the language of Selmer groups, the existence of the extension K above, gives a cohomology class in a Selmer subgroup of $H^1(F, \mathbb{Z}/p)^{G_{F|\mathbb{Q}}}$, which, by the isomorphism given by the inflation restriction sequence, gives a cohomology class in $H^1_{\mathcal{L}_0}(\mathbb{Q}, \mathbb{Z}/p)$, and thus an unramified $\mathbb{Z}/p$ extension of $\mathbb{Q}$, showing that $A(0) \neq 0$ is not possible.

If $A(1) \neq 0$, then there exists, by class field theory and Kummer theory, an unramified $\mathbb{Z}/p$ extension K of F , obtained by adjoining a p^{th} root of an element α in $F^\times / (F^\times)^p$. Requiring that the action of $G_{F|\mathbb{Q}}$ on $G_{K|F}$ by conjugation is through the cyclotomic character ϵ , further gives us that $\alpha \in \mathbb{Q}^\times / (\mathbb{Q}^\times)^p$, and the condition of $K|F$ being unramified then tells that $\alpha = p$. But, p is then totally ramified in the degree p sub-extension $\mathbb{Q}(p^{1/p})|\mathbb{Q}$, which cannot happen. Therefore, $A(1) = 0$.

Now, let $i \neq 0$ be even and $j \equiv 1 - i \pmod{p-1}$. By the Wiles-Greenberg formula, we have

$$\frac{\#H^1_{\mathcal{L}_i}(\mathbb{Q}, \epsilon^i)}{\#H^1_{\mathcal{L}_i^*}(\mathbb{Q}, \epsilon^j)} = \frac{\#H^0(\mathbb{Q}, \epsilon^i)}{\#H^0(\mathbb{Q}, \epsilon^j)} \frac{\#L_{i,p}}{\#H^0(G_p, \epsilon^i)} \frac{\#L_{i,\infty}}{\#H^0(G_{\mathbb{R}}, \epsilon^i)}$$

Each of the factors on the right are easy to compute. Since $i \not\equiv 0 \pmod{p-1}$ and j is odd, we get

$$\begin{aligned} \frac{\#H^0(\mathbb{Q}, \epsilon^i)}{\#H^0(\mathbb{Q}, \epsilon^j)} &= 1; & \frac{\#L_{i,p}}{\#H^0(G_p, \epsilon^i)} &= \frac{1}{\#H^0(G_p, \epsilon^i)} = 1 \\ \frac{\#L_{i,\infty}}{\#H^0(G_{\mathbb{R}}, \epsilon^i)} &= \frac{1}{\#H^0(G_{\mathbb{R}}, \epsilon^i)} = \frac{1}{p} \quad \text{since } i \text{ is even.} \end{aligned}$$

Therefore,

$$\frac{\#H_{\mathcal{L}_i}^1(\mathbb{Q}, \epsilon^i)}{\#H_{\mathcal{L}_i^*}^1(\mathbb{Q}, \epsilon^j)} = \frac{1}{p}$$

In other words, $\dim_{\mathbb{F}_p} H_{\mathcal{L}_i}^1(\mathbb{Q}, \epsilon^i) - \dim_{\mathbb{F}_p} H_{\mathcal{L}_i^*}^1(\mathbb{Q}, \epsilon^j) = -1$.

Now, we observe that $\mathcal{L}_i^*$ and $\mathcal{L}_j$ are local conditions for the module $\epsilon^{1-i} = \epsilon^j$, that differ only at the place p . Indeed, $L_{i,\infty}^\perp = H^1(G_{\mathbb{R}}, \epsilon^{1-i}) = 0 = L_{j,\infty}$, and at the place p , we have $L_{j,p} = 0 \subset H^1(G_p, \epsilon^j) = L_{i,p}^\perp$. Therefore, we have the inclusion $H_{\mathcal{L}_j}^1(\mathbb{Q}, \epsilon^j) \subseteq H_{\mathcal{L}_i^*}^1(\mathbb{Q}, \epsilon^j)$ and furthermore, we have

$$\frac{\#H_{\mathcal{L}_i^*}^1(\mathbb{Q}, \epsilon^j)}{\#H_{\mathcal{L}_j}^1(\mathbb{Q}, \epsilon^j)} \leq \#H^1(G_p, \epsilon^j) = p^{\text{ord}_p(\#\epsilon^j)} \cdot \#H^0(G_p, \epsilon^j) \cdot \#H^0(G_p, \epsilon^{1-j}) = p \cdot 1 \cdot 1 = p$$

where we have used the local Euler Characteristic formula. In other words, we have obtained that $0 \leq \dim_{\mathbb{F}_p} H_{\mathcal{L}_i^*}^1(\mathbb{Q}, \epsilon^j) - \dim_{\mathbb{F}_p} H_{\mathcal{L}_j}^1(\mathbb{Q}, \epsilon^j) \leq 1$.

Thus, we get $-1 \leq \dim_{\mathbb{F}_p} H_{\mathcal{L}_i}^1(\mathbb{Q}, \epsilon^i) - \dim_{\mathbb{F}_p} H_{\mathcal{L}_j}^1(\mathbb{Q}, \epsilon^j) \leq 0$ and hence by 4.2, we get what we want.

$$-1 \leq \text{rank}_p A(i) - \text{rank}_p A(j) \leq 0$$

□

References

- [1] Lawrence C. Washington. Galois Cohomology. Gary Connel, Joseph H. Silverman, Glenn Stevens, Editors, *Modular Forms and Fermat's Last Theorem*, pages 101-120. Springer 1997.
- [2] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag 1997.
- [3] J. S. Milne. *Arithmetic Duality Theorems*, Second Edition. Available at <http://www.jmilne.org/math/Books/ADTnot.pdf>
- [4] John Tate. *Galois Cohomology*, IAS/Park City Mathematics Series. Available at http://wstein.org/edu/2010/582e/refs/tate-galois_cohomology.pdf
- [5] Andrei Jorza. *Applications of Global Class Field Theory*. Available at <https://www3.nd.edu/~ajorza/courses/m160c-s2013/overview/m160c-s2013.pdf>
- [6] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*, Chapter VIII §3. Second Edition, Springer-Verlag. Corrected version 2.2, July 2015, available at <https://www.mathi.uni-heidelberg.de/~schmidt/NSW2e>