FALL 2022 LEARNING SEMINAR: EULER SYSTEM OF CYCLOTOMIC UNITS

MURILO CORATO ZANARELLA

October 3, 2022

1. Some history of class groups of cyclotomic fields

Let p be an odd prime and consider $K = \mathbb{Q}(\mu_p)$ the cyclotomic field of degree $p-1$. Denote $K^+ = K \cap \mathbb{R}$ its totally real subfield. We are interested in the class numbers $h := \#\mathrm{Cl}(K)$ and $h^+ := \#\mathrm{Cl}(K^+)$. Write also $h^- := h/h^+$ (which is an integer!).

A standard application Dirichlet's unit theorem and of Hilbert theorem 90 tells us that

$$\mathcal{O}_K^\times = \pm\mu_p \times \mathcal{O}_{K^+}^\times.$$

In particular, the regulators of K and K^+ are the same. Using the analytic class number formula

$$\zeta_K^{(r_1+r_2-1)}(0) = -\frac{h_K R_K}{w_K}$$

for both K and K^+, we obtain

$$\left|\prod_{\chi \text{ odd}} L(0,\chi)\right|_p^{-1} = \left|\frac{\zeta_K}{\zeta_{K^+}}(0)\right|_p^{-1} = \left|\frac{h^-}{p}\right|_p^{-1} = \frac{1}{p}\left|\prod_{\chi \text{ odd}} \mathrm{Cl}(K)^\chi\right|_p^{-1}$$

where the products are over characters[1] $\chi\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$. Explicitly, we have $L(0,\chi) = -\frac{1}{p}\sum_{a=1}^{p-1} a\chi(a)$. There is a distinguished character $\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$, called the *Teichmüller character* and characterized by $\omega(a) \equiv a \mod p$. We have $|L(0,\omega^{-1})|_p^{-1} = \frac{1}{p}$ but $L(0,\chi^{-1}) \in \mathbb{Z}_p$ if $\chi \neq \omega$. Using also that $\mathrm{Cl}(K)^\omega = 0$ by Stickelberger's theorem, we may write

$$(\star_{\text{odd}}) \qquad \prod_{\chi\neq\omega \text{ odd}} |L(0,\chi^{-1})|_p^{-1} = \prod_{\chi\neq\omega \text{ odd}} |\mathrm{Cl}(K)^\chi|_p^{-1}.$$

For the even part of the class group, Kummer observed that there is a very explicit subgroup of units $\mathcal{C} \subseteq \mathcal{O}_{K^+}^\times$, called *cyclotomic units*, which has finite index and whose regulator can be explicitly computed. Comparing with the class number formula, one can compute that $|\mathcal{O}_{K^+}^\times/\mathcal{C}|_p^{-1} = |\mathrm{Cl}(K^+)|_p^{-1}$. Thus

$$(\star_{\text{even}}) \qquad \prod_{\chi \text{ even}} |(\mathcal{O}_{K^+}^\times/\mathcal{C})^\chi|_p^{-1} = \prod_{\chi \text{ even}} |\mathrm{Cl}(K)^\chi|_p^{-1}.$$

Remark 1.1. Vandivier's conjecture predicts that $|h^+|_p^{-1} = 1$.

1.1. Pre-Euler-systems history.

(1) Kummer [Kum50]: $p \mid h_{K^+} \implies p \mid h^-$, and thus $p \mid \mathrm{Cl}(K)$ if and only if p divides $\prod_{\chi\neq\omega \text{ odd}} L(0,\chi^{-1})$. It is a simple computation that this happens if and only if p divides one of the Bernoulli numbers $B_3, \dots, B_{p-2}$.

[1] We are fixing an isomorphism $\mathbb{C} \simeq \overline{\mathbb{Q}_p}$ to compare $\mathbb{C}^\times$ valued characters to such χ.

This is called a *reflection theorem*, and we can give a modern proof as follows: let $G = \mathrm{Gal}(K/\mathbb{Q})$. As G-modules, we have

$$K^\times/(K^\times)^p \overset{\text{Kummer theory}}{=} H^1(K, \mu_p) = H^1(K, \mathbb{Z}/p\mathbb{Z}) \otimes \omega = \mathrm{Hom}(G_K, \mathbb{Z}/p\mathbb{Z}) \otimes \omega$$

and we have Selmer groups (more about this later)

$$\mathrm{Sel}(K, \mu_p) := \{\alpha \in K^\times : p \mid \nu_v(\alpha) \text{ for all } v\}/(K^\times)^p \supseteq \mathrm{Hom}(\mathrm{Gal}(H_K/K), \mathbb{Z}/p\mathbb{Z}) \otimes \omega =: \mathrm{Sel}(K, \mathbb{Z}/p\mathbb{Z}) \otimes \omega$$

One can check that

$$1 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p \to \mathrm{Sel}(K, \mu_p) \to \mathrm{Cl}(K)[p] \to 1 \quad \text{and} \quad \mathrm{Sel}(K, \mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{Hom}(\mathrm{Cl}(K), \mathbb{Z}/p\mathbb{Z}),$$

and thus

$$\dim \mathrm{Cl}(K)[p]^{\omega\chi^{-1}} \leq \dim \mathrm{Cl}(K)[p]^{\chi} + \begin{cases} 1 & \text{if } \chi = \omega \text{ or } \chi \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

(2) Herbrand [Her33]: for χ odd, $|L(0, \chi^{-1})|_p^{-1} = 1 \implies |\mathrm{Cl}(K)^\chi|_p^{-1} = 1$. This is a consequence of Stickelberger's theorem.

(3) Ribet [Rib76]: for $\chi \neq \omega$ odd, $|\mathrm{Cl}(K)^\chi|_p^{-1} = 1 \implies |L(0, \chi^{-1})|_p^{-1} = 1$.

Ribet's argument deserves its own notes, but the idea is roughly as follows. Assume $|L(0, \chi)|_p^{-1} > 1$. By congruences, this propagates to $|L(1-k, \chi)|_p^{-1} > 1$ for some other $k \equiv 1 \mod p$. This in turn means that the constant coefficient of the Eisenstein series $E_{k,\chi}$ is divisible by p. Ribet finds a *cuspidal* modular form g which is congruent to $E_{k,\chi}$ modulo p, and then shows that on the associated Galois representation $\rho_g \colon G_\mathbb{Q} \to \mathrm{GL}_2(F)$, for F a finite extension of $\mathbb{Q}_p$, we can find a stable lattice for which the reduction of the representation becomes a non-trivial extension

$$\widetilde{\rho_g} = \begin{pmatrix} \chi\chi_{cycl}^{1-k} & * \\ & 1 \end{pmatrix}.$$

Note that the diagonal terms are what the Galois representation of $E_{k,\chi}$ looks like. This produces a nontrivial element in

$$H^1(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}(\chi\chi_{cycl}^{1-k})) = H^1(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}(\chi))$$

which satisfies the appropriate local conditions. Thus

$$0 \neq \mathrm{Sel}(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}(\chi)) = \mathrm{Sel}(F, \mathbb{Z}/p\mathbb{Z})^\chi = \mathrm{Hom}(\mathrm{Cl}(K), \mathbb{Z}/p\mathbb{Z})^\chi = \mathrm{Hom}(\mathrm{Cl}(K)^{\chi^{-1}}, \mathbb{Z}/p\mathbb{Z}).$$

(4) Mazur–Wiles [MW84]: for $\chi \neq \omega$ odd, $|L(0, \chi^{-1})|_p^{-1}$ divides $|\mathrm{Cl}(K)^\chi|_p^{-1}$.

Of course, together with ($\star_{\text{odd}}$) this implies the equality for all such χ. In fact, Mazur–Wiles prove an "assymptotic" version of this divisibility in an Iwasawa family, following the above method of Ribet. Then one "controls" the result back to K. Moreover, a reflection theorem in the Iwasawa family also lets one deduce from their results that

$$|(\mathcal{O}_{K^+}^\times/\mathcal{C})^\chi|_p^{-1} \quad \text{divides} \quad |\mathrm{Cl}(K)^\chi|_p^{-1}$$

for χ even, which together with ($\star_{\text{even}}$) implies the equality for each χ.

In short, Mazur–Wiles's work proves the following theorem.

Theorem 1.2. *We have*

$$|\mathrm{Cl}(K)^\chi|_p^{-1} = \begin{cases} 0 & \text{if } \chi = \omega, \\ |L(0,\chi^{-1})|_p^{-1} & \text{if } \chi \text{ is odd and } \chi \neq \omega, \\ |(\mathcal{O}_{K^+}^\times/\mathcal{C})^\chi|_p^{-1} & \text{if } \chi \text{ is even.} \end{cases}$$

And in its essence, this is done by proving RHS | LHS in an Iwasawa family, and then deducing the equality from the class number formula.

1.2. **Post-Euler-systems.** Four years later[2] in 1988, Kolyvagin published his groundbreaking work [Kol88] on Heegner points. But shortly before that, the Bolivian/Brazilian mathematician Francisco Thaine was working on a method to bound exponents of class groups of real abelian extensions ([Tha88]). As an example, he proved for an even character χ that

$$\exp(\mathrm{Cl}(K)^\chi) \leq \exp((\mathcal{O}_{K^+}^\times/\mathcal{C})^\chi).$$

This was already known by the above work of Mazur–Wiles, but the proof here is of a different nature: it uses, in its core, an Euler system[3].

Shortly after, Kolyvagin became aware of Thaine's work. Introducing the name "Euler systems", Kolyvagin revisited Thaine's setting and his own setting, improving the above inequality to an equality about the *orders* of the groups ([Kol90]). That is, Kolyvagin proved the divisibility

$$|\mathrm{Cl}(K)^\chi|_p^{-1} \quad \text{divides} \quad |(\mathcal{O}_{K^+}^\times/\mathcal{C})^\chi|_p^{-1} \quad \text{for } \chi \text{ is even.}$$

Thaine and Kolyvagin's work used the Euler system of *cyclotomic units*, which we will discuss here. In the same paper, Kolyvagin produces an Euler system for the odd part, using certain twisted Gauss sums, and proves

$$|\mathrm{Cl}(K)^\chi|_p^{-1} \quad \text{divides} \quad |L(0,\chi^{-1})|_p^{-1} \quad \text{if } \chi \neq \omega \text{ is odd.}$$

As before, these divisibilities imply the equalities, and in fact such Euler systems can be used to give a simpler proof of the Iwasawa main conjecture proven by Mazur–Wiles.

Remark 1.3. The divisibilities obtained with Euler systems are the *opposite* of the one provided by the Ribet/Mazur–Wiles method. In the setting of cyclotomic fields, we only need one of them to conclude the equality, due to the class number formulas ($\star_{\text{odd}}$) and ($\star_{\text{even}}$). In other settings, however, the two methods are *complementary*. For elliptic curves over $\mathbb{Q}$, for example, the class number formula has as analogue the refined BSD conjecture. So one can hope that a combination of both methods above could lead to information about the refined BSD conjecture. This hope has seen the light of day in many different contexts[4].

2. Selmer groups of μ_M and $\mathbb{Z}/M\mathbb{Z}$

Let K be a number field, and let M be an odd[5] positive integer. We will usually use the notation v for a place of K.

[2]The interested reader should look at the introduction of Rubin's book [Rub00] for some words about this history.
[3]Thaine only used the classes in the first "level" of the Euler system: the classes $c(1)$ an $c(l)$ for certain primes l.
[4]See for example [SU14] for the setting of elliptic curves over $\mathbb{Q}$ of rank 0, or [JSW17] for rank 1.
[5]This is so that, among other things, we don't need to consider the archimedean places in our discussion.

2.1. **With μ_M coefficients.** Consider the exact sequence

$$1 \to \mu_M \to \mathbb{G}_m \xrightarrow{\cdot p} \mathbb{G}_m \to 1.$$

Hilbert 90 implies that the Kummer maps

$$\delta_M \colon K^\times/(K^\times)^M \xrightarrow{\sim} H^1(K, \mu_M), \quad \delta_{v,M} \colon K_v^\times/(K_v^\times)^M \xrightarrow{\sim} H^1(K_v, \mu_M)$$

are isomorphisms. For the local cohomology, we consider the exact sequence

$$1 \to \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^M \xrightarrow{\alpha_v} K_v^\times/(K_v^\times)^M \xrightarrow{\text{ord}} \mathbb{Z}/M\mathbb{Z} \to 1.$$

If $v \nmid M$, the first term correspond to the unramified cohomology $H^1_{unr}(K_v, \mu_M)$, as then the Teichmüller character induces an isomorphism $\mathbb{F}_v^\times/(\mathbb{F}_v^\times)^M \to \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^M$. If $v \mid M$, the first term at least contains $H^1_{unr}(K_v, \mu_M)$: for $\alpha \in K_v^\times/(K_v^\times)^M$, we have that $\delta_M(\alpha)$ is an unramified class exactly if $K_v(\alpha^{1/p})$ is an unramified extension, which implies (but is not equivalent to) $\alpha \in \mathcal{O}_{K_v}^\times \cdot (K_v^\times)^M$.

We form a Selmer group with the local conditions $\text{Sel}(K_v, \mu_M) = \text{im}(\alpha_v)$. That is,

$$\text{Sel}(K, \mu_M) = \{c \in K^\times/(K^\times)^M \colon c \in (K_v^\times)^M \text{ for all places } v\}.$$

From the extended Snake lemma[6] on the diagram obtained from

$$0 \to \mathcal{O}_K^\times \to K^\times \to \bigoplus_v K_v^\times/\mathcal{O}_{K_v}^\times \to \text{Cl}(K) \to 0$$

mapping to itself by multiplication by M, we obtain

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^M \to \text{Sel}(K, \mu_M) \to \text{Cl}(K)[M] \to 0.$$

2.2. **With $\mathbb{Z}/m\mathbb{Z}$ coefficients.** Since the coefficients have trivial action, we have

$$H^1(K, \mathbb{Z}/M\mathbb{Z}) = \text{Hom}(G_K, \mathbb{Z}/M\mathbb{Z}), \quad H^1(K_v, \mathbb{Z}/M\mathbb{Z}) = \text{Hom}(G_{K_v}, \mathbb{Z}/M\mathbb{Z}).$$

If K_v has residue field $\mathbb{F}_v$, we have the inflation-restriction exact sequence

$$0 \to H^1(\mathbb{F}_v, \mathbb{Z}/M\mathbb{Z}) \xrightarrow{\beta_v} H^1(K_v, \mathbb{Z}/M\mathbb{Z}) \to H^1(I_v, \mathbb{Z}/M\mathbb{Z}) \to 0.$$

We form the Selmer group with (everywhere unramified) local conditions $\text{Sel}(K_v, \mu_M) = \text{im}(\beta_v)$. That is, if H_K is the Hilbert class field of K, then

$$\text{Sel}_M(K, \mathbb{Z}/M\mathbb{Z}) = \text{Hom}(\text{Gal}(H_K/K), \mathbb{Z}/M\mathbb{Z}) = \text{Hom}(\text{Cl}(K), \mathbb{Z}/M\mathbb{Z}).$$

2.3. **Local comparison map.** Consider the case where $|\mathbb{F}_v| \equiv 1 \mod M$. Then $\mu_M \subseteq \mathcal{O}_{K_v}$ and thus

$$\begin{aligned} H^1_{unr}(K_v, \mu_M) &\xrightarrow{\sim} \mu_M, \\ c &\longmapsto c(\text{Frob}_v) \end{aligned} \qquad \begin{aligned} H^1_s(K_v, \mu_M) \otimes G_v &\xrightarrow{\sim} \mu_M, \\ c \otimes \sigma &\longmapsto c(\sigma) \end{aligned}$$

[6] That is, by comparing the horizontal and vertical spectral sequences of the diagram.

where G_v is the Galois group of the maximal tamely ramified extension of K_v. So we have a finite-singular comparison map

$$\phi^{fs}\colon H^1_{unr}(K_v, X) \xrightarrow{\sim} H^1_s(K_v, X) \otimes G_v.$$

2.4. **Local Tate pairings.** For K_v local we have the cup product pairing

$$H^1(K_v, \mu_M) \otimes H^1(K_v, \mathbb{Z}/M\mathbb{Z}) \to H^2(K_v, \mu_M).$$

If $v \nmid M$, the local conditions $\mathrm{Sel}(K_v, \mu_M)$ and $\mathrm{Sel}(K_v, \mathbb{Z}/M\mathbb{Z})$ are both unramified and thus annihilate each other[7]. In the later sections we will be in a situation where the local conditions at $v \mid M$ also annihilate each other.

Proposition 2.1. *Let $M = p^k$ for p an odd prime. Assume either $K_v \cap \mu_p = \{1\}$ or $\mu_M \subseteq K_v$. Then $\mathrm{Sel}(K_v, \mu_M)$ and $\mathrm{Sel}(K_v, \mathbb{Z}/M\mathbb{Z})$ annihilate each other.*

Proof. In the first case, one can check that $H^i(K_v(\mu_M)/K_v, \mu_M) = 0$ for $i > 0$,[8] and thus $H^1(K_v, \mu_M) \simeq H^1(K_v(\mu_M), \mu_M)^{G_{K_v}}$. This reduces the question to the second case. In the case $\mu_M \subseteq K_v$, such pairing can be interpreted with Hilbert symbols, and we are left to check that $(\alpha, \beta)_M := \mathrm{Art}(\alpha)(\beta^{1/M})/(\beta^{1/M})$ is trivial if $K_v(\beta^{1/M})/K_v$ is unramified and if α is a unit. This follows at once from the properties of the local Artin map. □

With all that, we conclude: an Euler/Kolyvagin system in $H^1(K, \mu_M)$ can be used to bound $\mathrm{Sel}(K, \mathbb{Z}/M\mathbb{Z})$.[9]

3. The Euler and Kolyvagin systems

Let $F = \mathbb{Q}(\zeta_p)^+$, and denote $F_n = \mathbb{Q}(\zeta_{np})^+$. Denote $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. Consider the following elements:

$$x_n := (1 - \zeta_{pn})(1 - \zeta_{pn}^{-1}) \in F_n.$$

Note that $(1 - \zeta_{pn})$ is a unit in $\mathbb{Q}(\zeta_{np})$ as long as $n > 1$ and $p \nmid n$. Indeed,

$$(1 - \zeta_n\zeta_p)(1 - \zeta_n\zeta_p^2) \cdots (1 - \zeta_n\zeta_p^{p-1}) = \frac{1 - \zeta_n^p}{1 - \zeta_n}$$

is a unit. But a warning: $x_1 = (1 - \zeta_p)(1 - \zeta_p^{-1})$ is *not* a unit. Note however that if $R \in \mathrm{aug}(\mathbb{Z}[\Delta])$, then $R \cdot x_1$ is a unit.

Definition 3.1. The *cyclotomic units* for F are $\mathcal{C} := \mathrm{aug}(\mathbb{Z}[\Delta]) \cdot x_1 \subseteq \mathcal{O}_F^\times$.

It is very easy to check the following Euler system relations.

Proposition 3.2. *If nl is square-free, then (i) $\mathrm{Nm}_{F_{nl}/F_n} x_{nl} = (\mathrm{Frob}_l - 1)x_n$, (ii) if λ is any prime above l, then $x_{nl} \equiv x_n$* mod λ.

Proof. Note that

$$\mathrm{Nm}_{F_{nl}/F_n} x_{nl} = \prod_{i=1}^{l-1}(1 - \zeta_{pn}\zeta_l^i)(1 - \zeta_{pn}^{-1}\zeta_l^{-i}) = \frac{1 - \zeta_{np}^l}{1 - \zeta_{np}} \cdot \frac{1 - \zeta_{np}^{-l}}{1 - \zeta_{np}^{-1}} = (\mathrm{Frob}_l - 1)x_n.$$

---

[7]As then the image of $\mathrm{Sel}(K_v, \mu_M) \otimes \mathrm{Sel}(K_v, \mathbb{Z}/M\mathbb{Z})$ is simply the image of $H^1(\mathbb{F}_v, \mu_M) \otimes H^1(\mathbb{F}_v, \mathbb{Z}/M\mathbb{Z}) \to H^2(\mathbb{F}_v, \mu_M) \xrightarrow{\mathrm{Inf}} H^2(K_v, \mu_M)$, and $H^2(\mathbb{F}_v, \mu_M) = 0$ as there is no nontrivial division algebra over a finite field.

[8]The Galois group $\mathrm{Gal}(K_v(\mu_M)/K_v)$ is cyclic and generated by $\sigma\colon \mu_M \mapsto \mu_M^a$ for some $a \not\equiv 1 \mod p$, and thus both $\mu_M^{\sigma=1}$ and $\mu_M/(\sigma - 1)$ are trivial.

[9]One can also produce Euler/Kolyvagin systems in $H^1(K, \mathbb{Z}/M\mathbb{Z})$ to bound $\mathrm{Sel}(K, \mu_M)$. The previously mentioned Euler system of twisted Gauss sums is of this form.

Moreover, since $\zeta_l \equiv 1$ modulo any prime λ above l, we also have

$$1 - \zeta_{nl} \equiv 1 - \zeta_n \mod \lambda. \qquad \square$$

Now denote $G_l = \mathrm{Gal}(F_l/F) = \mathrm{Gal}(F_{nl}/F_n)$. For a choice of generator σ_l of G_l, we consider an operator $D_l \in \mathbb{Z}[G_l]$ such that

$$(\sigma_l - 1)D_l = \mathrm{Tr}_l - (l-1).$$

Definition 3.3. We denote $\mathcal{N}$ to be the set of square-free products of primes $l \equiv 1 \mod pM$.

If $l \in \mathcal{N}$, this for instance implies that $\mathrm{Frob}_l|_F = \mathrm{id}$.

Proposition 3.4. *Assume that $n \in \mathcal{N}$. Then $\delta_M(D_n x_n) \in H^1(F_n, \mu_M)^{\mathrm{Gal}(F_n/F)} \xleftarrow{\sim} H^1(F, \mu_M)$. That is, there is $c(n) \in F^\times$ and $\beta_n \in F_n^\times$ such that $D_n x_n = c(n)\beta_n^M$.*

Proof. The isomorphism follows from inflation-restriction and the fact that $\mu_M^{G_{F_n}} = 1$, as $\mu_M \cap F = 1$ and $(n, M) = 1$. We prove by induction that $\delta_M(D_n x_n)$ is invariant. For the induction step,

$$(\sigma_l - 1)(D_{nl}x_{nl}) = (\mathrm{Tr}_l - (l-1))D_n x_{nl} = \frac{(\mathrm{Frob}_l - 1)(D_n x_n)}{\left((D_n x_{nl})^{(l-1)/M}\right)^M} = \left(\frac{(\mathrm{Frob}_l - 1)\beta_n}{(D_n x_{nl})^{(l-1)/M}}\right)^M. \qquad \square$$

Theorem 3.5. *Let $nl \in \mathcal{N}$ and λ be a prime above l. Denote $\partial_\lambda \colon H^1(F_\lambda, \mu_M) \twoheadrightarrow H^1_s(F_\lambda, \mu_M)$. We have*

$$\phi^{fs}(\mathrm{loc}_\lambda c(n)) = \partial_\lambda \mathrm{loc}_\lambda c(nl) \otimes \sigma_l.$$

Proof. This amounts to proving that

$$\delta_M(c(n))(\mathrm{Frob}_\lambda) = \delta_M(c(nl))(\sigma_l).$$

Let λ_n be a prime of F_n above λ. The identity we want to prove it between elements of $\mu_M \subseteq \mathcal{O}_{F_{n,\lambda_n}}^\times$, and thus it suffices to prove they are congruent modulo λ_n. Write $D_n x_n = c(n)\beta_n^M$ as above. Note that $(\sigma - 1)\beta_n$ is the unique M-th root of $(\sigma - 1)D_n x_n$ contained in F_n. As

$$(D_n x_{nl})^{l-1} = (\mathrm{Tr}_l - (\sigma_l - 1)D_l)(D_n x_{nl}) = \frac{(\mathrm{Frob}_l - 1)(D_n x_n)}{(\sigma_l - 1)(D_{nl}x_{nl})} = \left(\frac{(\mathrm{Frob}_l - 1)\beta_n}{(\sigma_l - 1)\beta_{nl}}\right)^M,$$

this means that we must have

$$(D_n x_{nl})^{(l-1)/M} = \frac{(\mathrm{Frob}_l - 1)\beta_n}{(\sigma_l - 1)\beta_{nl}}.$$

Note that we may take β_n to be a λ_n-adic unit, and thus

$$c(n)^{(l-1)/M} = \frac{(D_n x_n)^{(l-1)/M}}{\beta_n^{l-1}} \equiv_{\lambda_n} \frac{(D_n x_{nl})^{(l-1)/M}}{(\mathrm{Frob}_l - 1)\beta_n} = \frac{1}{(\sigma_l - 1)\beta_{nl}}.$$

Hence

$$\delta_M(c(n))(\mathrm{Frob}_\lambda) = (\mathrm{Frob}_\lambda - 1)c(n)^{1/M} \equiv_\lambda c(n)^{(l-1)/M} \equiv_{\lambda_n} \frac{1}{(\sigma_l - 1)\beta_{nl}}.$$

Finally, as $D_{nl}x_{nl} \in F_n^\times$ is a unit, we have

$$\delta_M(c(nl))(\sigma_l) = \frac{1}{\delta_M(\beta_{nl}^M)(\sigma_l)} = \frac{1}{(\sigma_l - 1)\beta_{nl}}. \qquad \square$$

4. The global duality argument

We keep the notation from the previous section.

Theorem 4.1. *Let M be a power of p and $c \in \mathrm{Cl}(F)[p^\infty]$. Suppose we are given a nonzero element $d \in H^1(F, \mu_M) = F^\times/(F^\times)^M$ which is not in $p \cdot H^1(F, \mu_M)$. Then there are infinitely many primes λ of F such that: (i) $\lambda \in c$, (ii) the rational prime l below λ is in $\mathcal{N}$, (iii) $\mathrm{loc}_\lambda(d)$ is a generator of $H^1_{unr}(F_\lambda, \mu_M)$.*

Proof. Under the hypothesis $l \equiv 1 \mod M$ and the identification $H^1_{unr}(F_\lambda, \mu_M) \simeq \mu_M$, the class $\mathrm{loc}_\lambda(d)$ correspond to the root of unity ζ such that $\mathrm{Frob}_\lambda d^{1/M} = \zeta \cdot d^{1/M}$. So (ii) and (iii) correspond to having Frob_l be a generator of the Galois group H as below. Note that $H \simeq \mu_M$ as $d \notin (F^\times)^p$.

$$\begin{array}{c} F(d^{1/M}, \mu_M) \\ {\scriptstyle H}\big| \\ F(\mu_M) \\ \big| \\ F \\ \big| \\ \mathbb{Q} \end{array}$$

To guarantee (i), we only need to prove that the maximal unramified p-extension of F is disjoint from $F(d^{1/M}, \mu_M)$. So assume $L \subsetneq F(d^{1/M}, \mu_M)$ is an unramified p-extension of F. We want to prove that $L = F$. Since L/F is unramified, the action of complex conjugation is trivial on $\mathrm{Gal}(L/F)$. Note also that $F(\mu_M)/F$ is totally ramified, and thus we have that $H \twoheadrightarrow \mathrm{Gal}(L/F)$. But complex conjugation acts by -1 in H, and hence in $\mathrm{Gal}(L/F)$. So complex conjugation acts on $\mathrm{Gal}(L/F)$ by both 1 and -1, and thus $L = F$ since p is odd. □

Definition 4.2. For an abelian p-group A and $a \in A$, we define

$$\mathrm{ord}(a,\ A) := \sup(\{m \in \mathbb{Z}_{\geq 0} \colon a \in p^m A\}).$$

Corollary 4.3. *Let M be a power of p and $c \in \mathrm{Cl}(F)[p^\infty]$. Suppose we are given $d \in H^1(F, \mu_M)$. Then there are infinitely many primes λ of F such that: (i) $\lambda \in c$, (ii) the rational prime l below λ is in $\mathcal{N}$, (iii) we have*

$$\mathrm{ord}(\mathrm{loc}_\lambda(d),\ H^1_{unr}(F_\lambda, \mu_M)) = \mathrm{ord}(d,\ H^1(F, \mu_M)).$$

Proof. If $d = p^e d_0$ where $e = \mathrm{ord}(d,\ H^1(F, \mu_M))$, apply the above for d_0. Then $\mathrm{loc}_\lambda(d_0) \notin p \cdot H^1_{unr}(F_\lambda, \mu_M) \simeq (\mu_M)^p$, and thus $\mathrm{ord}(\mathrm{loc}_\lambda(d),\ H^1(F_\lambda, \mu_M)) = e$. □

Theorem 4.4. *Let $\mathcal{E} = \mathcal{O}_F^\times$, and $\mathcal{C} \subseteq \mathcal{E}$ be the finite index subgroup of cyclotomic units. Then for every even character χ, we have*

$$|\mathrm{Cl}(F)^\chi|_p^{-1} \quad \textit{divides} \quad |(\mathcal{E}/\mathcal{C})^\chi|_p^{-1}.$$

Proof. Let M be a power of p such that

$$|\mathcal{E}/\mathcal{C}|_p^{-1},\ |\mathrm{Cl}(F)|_p^{-1} \quad \text{divide} \quad M.$$

We may assume χ is nontrivial[10]. Let $e_\chi = \frac{2}{p-1}\sum_{\gamma\in\Delta}\chi^{-1}(\gamma)\gamma \in \mathbb{Z}_{(p)}[\Delta]$ be the projector to the χ eigencomponent. We denote $c^\chi(n) := e_\chi c(n)$. Since χ is nontrivial, $\mathrm{aug}(e_\chi) = \frac{2}{p-1}\sum_{\gamma\in\Delta}\chi^{-1}(\gamma) = 0$, and thus $c^\chi(1) \in \mathcal{C}$. In fact, $\mathcal{C}^\chi$ is generated by $c^\chi(1)$, and thus $(\mathcal{E}/\mathcal{C})^\chi[p^\infty] \xrightarrow{\sim} \delta_M(\mathcal{E}^\chi)/\delta_M(c^\chi(1))$. Note that $\delta_M(\mathcal{E}^\chi) \simeq \mathbb{Z}/M\mathbb{Z}$ is cyclic, and hence $|(\mathcal{E}/\mathcal{C})^\chi|_p^{-1} = \mathrm{ord}(c^\chi(1),\ H^1(F,\mu_M))$.

We know we will bound $\mathrm{Sel}(F,\mathbb{Z}/M\mathbb{Z})$, but which eigenspace exactly? Let's think of $c^\chi(l)$ for some $l\in\mathcal{N}$, for example. Note that l split completely in $F/\mathbb{Q}$, and so if we fix a prime λ above l, all the other primes above l are $\gamma\lambda$ for $\gamma\in\Delta$. We have canonical isomorphisms

$$H^1(F_\lambda,\mu_M) \simeq H^1(F_{\gamma\lambda},\mu_M),$$

and under this we have

$$\mathrm{loc}_{\gamma\lambda}c^\chi(l) = \chi(\gamma)\cdot\mathrm{loc}_\lambda c^\chi(l)$$

So if we have a class $f\in\mathrm{Sel}(F,\mathbb{Z}/M\mathbb{Z})^{\chi_0}$, we will have

$$0 = \sum_{\gamma\in\Delta}\langle\mathrm{loc}_{\gamma\lambda}c(l),\mathrm{loc}_{\gamma\lambda}f\rangle = \sum_{\gamma\in\Delta}\chi(\gamma)\chi_0(\gamma)\langle\mathrm{loc}_\lambda c(l),\mathrm{loc}_\lambda f\rangle = \langle\mathrm{loc}_\lambda c(l),\mathrm{loc}_\lambda f\rangle\sum_{\gamma\in\Delta}(\chi\chi_0)(\gamma).$$

This is only nontrivial if $\chi_0 = \chi^{-1}$. This means that we will be able to bound $\mathrm{Sel}(F,\mathbb{Z}/M\mathbb{Z})^{\chi^{-1}}$. As $\mathrm{Sel}(F,\mathbb{Z}/M\mathbb{Z}) = \mathrm{Hom}(\mathrm{Cl}(F),\mathbb{Z}/M\mathbb{Z})$, we will indeed bound $\mathrm{Cl}(F)^\chi$.

Choose a decomposition

$$\mathrm{Cl}(F)[p^\infty]^\chi = \bigoplus_{i=1}^r[\mathfrak{a}_i]\cdot\mathbb{Z}/p^{a_i}\mathbb{Z}.$$

From this we get a corresponding decomposition of $\mathrm{Sel}(F,\mathbb{Z}/M\mathbb{Z})^{\chi^{-1}}$, namely

$$\mathrm{Sel}(F,\mathbb{Z}/M\mathbb{Z})^{\chi^{-1}} = \bigoplus_{i=1}^r f_i\cdot\mathbb{Z}/p^{a_i}\mathbb{Z},\quad\text{where}\quad f_i([\mathfrak{a}_j]) = \begin{cases} 0 & \text{if } i\neq j,\\ M/p^{a_i} & \text{if } i=j.\end{cases}$$

We choose a sequence of primes $\lambda_1,\dots,\lambda_r$ of F such that for all i we have (i) $[\lambda_i]=[\mathfrak{a}_i]$, (ii) the rational prime l_i below λ_i is in $\mathcal{N}$, (iii) we have

$$(\star)\qquad \mathrm{ord}(\mathrm{loc}_{\lambda_i}c^\chi(l_1\cdots l_{i-1}),\ H^1_{unr}(F_{\lambda_i},\mu_M)) = \mathrm{ord}(c^\chi(l_1\cdots l_{i-1}),\ H^1(F,\mu_M)).$$

We can do this inductively by the above corollary. Denote $b_i = \mathrm{ord}(c^\chi(l_1\cdots l_i),\ H^1(F,\mu_M))$, so we may write $c^\chi(l_1\cdots l_i) = p^{b_i}\cdot d(i)$. Note that $b_0 = \mathrm{ord}(c^\chi(1),\ H^1(F,\mu_M))$, and so $p^{b_0} = |(\mathcal{E}/\mathcal{C})^\chi|_p^{-1}$.

Global duality for $d(i)\in H^1(F,\mu_M)$ and $f_i\in H^1(F,\mathbb{Z}/M\mathbb{Z})$ tells us that

$$0 = \sum_v\langle\mathrm{loc}_v d(i),\ \mathrm{loc}_v f_i\rangle = \frac{(p-1)}{2}\sum_{j=1}^i\langle\mathrm{loc}_{\lambda_j}d(i),\ \mathrm{loc}_{\lambda_j}f_i\rangle = \frac{(p-1)}{2}\langle\mathrm{loc}_{\lambda_i}d(i),\ \mathrm{loc}_{\lambda_i}f_i\rangle.$$

The second equality is since $d(i), f_i$ are in the local Selmer groups outside $l_1,\dots l_i$, and the third as $\mathrm{loc}_{\lambda_j}f_i \leftrightarrow f_i([\lambda_j])$ is 0 for $j\neq i$. This gives us the upper bound $a_i \le \mathrm{ord}(\partial_{\lambda_i}\mathrm{loc}_{\lambda_i}d(i),\ H^1_s(F_{\lambda_i},\mu_M))$.

[10]As any element $c\in\mathrm{Cl}(F)^{\mathrm{id}}$ satisfies $c^{p-1} = \mathrm{Nm}_{F/\mathbb{Q}}c\in\mathrm{Cl}(\mathbb{Q}) = \{1\}$, and thus $\mathrm{Cl}(F)^{\mathrm{id}}\subseteq\mathrm{Cl}(F)[p-1]$.

We can compute the above order in terms of the b_i:

$$\begin{array}{ccccc} b_i + \mathrm{ord}(\partial_{\lambda_i}\mathrm{loc}_{\lambda_i} d(i)) & = & \mathrm{ord}(\partial_{\lambda_i}\mathrm{loc}_{\lambda_i} c^\chi(l_1\cdots l_i)) & & \\ & & \Big\| \text{Kolyvagin system} & & \\ & & \mathrm{ord}(\mathrm{loc}_{\lambda_i} c^\chi(l_1\cdots l_{i-1})) & \overset{}{\underset{(\star)}{=\!=}} & \mathrm{ord}(c^\chi(l_1\cdots l_{i-1})) = b_{i-1}. \end{array}$$

Hence

$$a_i \leq \mathrm{ord}(\partial_{\lambda_i}\mathrm{loc}_{\lambda_i} d(i)) = b_{i-1} - b_i,$$

and thus

$$\log_p |\mathrm{Cl}(F)^\chi|_p^{-1} = \sum_{i=1}^r a_i \leq \sum_{i=1}^r (b_{i-1} - b_i) = b_0 - b_r \leq b_0 = \log_p |(\mathcal{E}/\mathcal{C})^\chi|_p^{-1}. \qquad \square$$

References

[Her33] J. Herbrand. Sur les théorèmes du genre principal et des idéaux principaux. *Abh. Math. Sem. Univ. Hamburg*, 9(1):84–92, 1933.

[JSW17] Dimitar Jetchev, Christopher Skinner, and Xin Wan. The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one. *Camb. J. Math.*, 5(3):369–434, 2017.

[Kol88] V. A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[Kol90] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, Boston, MA, 1990.

[Kum50] E. E. Kummer. Allgemeiner Beweis des Fermatschen Satzes, daßdie Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ welche ungerade Primzahlen sind und in den Zählern der ersten $1/2(\lambda)$ Bernoullischen zahlen als Factoren nicht vorkommen. *J. Reine Angew. Math.*, 40:130–138, 1850.

[MW84] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[Rib76] Kenneth A. Ribet. A modular construction of unramified p-extensions of $Q(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[Rub00] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

[SU14] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[Tha88] Francisco Thaine. On the ideal class groups of real abelian number fields. *Ann. of Math. (2)*, 128(1):1–18, 1988.