Bounding the ideal class group

$K(E[\mathfrak{p}])$

Setting: E/K with CM by $\mathcal{O}$

- Fix an ideal $\mathfrak{q}$ of K prime to $6N_E$ (N_E = conductor of E)
  - a prime $\mathfrak{p}$ of K ——— $6N_E$ $\mathfrak{q}$ above $\mathfrak{p}$ splits in K
- $F := K(E[\mathfrak{p}])$, $\mu_F :=$ roots of unity
- Fix $M = \mathfrak{p}^k$, denote $\mu_M :=$ M^{th} roots of unity
  $F_M := F(\mu_M)$
- A : ideal class group of F

Main theorem: Let $\chi : Gal(F/K) \to \mathbb{Z}_p$ irred. character. Then

$$\#A^{\chi} \leq \#\left(\mathcal{O}_F^{\times}/\langle \mu_F, \eta_{(1,\sigma)} \rangle\right)^{\chi}$$

LHS RHS

where $M^{\chi} := \{ m \in M \otimes_{\mathbb{Z}} \mathbb{Z}_p : \sigma m = \chi(\sigma) m \quad \forall \sigma \in \mathrm{Gal}(F/k) \}$

Recall: τ is square free ideal of $\mathcal{O}$ coprime to $6 N_E p \mathfrak{q}$

(Previous talk) - $\eta(n, \tau) = \Lambda_E \left(\frac{\Omega}{\Psi(\mathfrak{p}^n \tau)} \right)$

Ψ Hecke char. att. to E

$E(\mathbb{C}) \simeq \mathbb{C} / L$

$L = \mathcal{O} \cdot \Omega$

$$\eta(n, \tau) \in K(E[\mathfrak{p}^n \tau])^{\chi}$$

[ES Machine]: K_n Euler system + character χ

$\Downarrow$

bounding of A^{χ} of K_1

Cor: Suppose $\eta(1, \mathcal{O})^{\chi} \in \mu_F^{\chi}((\mathcal{O}_F^{\times})^{\chi})^p$

Then $\underline{A^{\chi} = 0}$

Because it relates to the vanishing of the Selmer gp

① RHS: Let χ be a non-trivial character of $\Delta := \mathrm{Gal}(F/K)$. Then:

$$\left(\mathcal{O}_F^\times/\mu_F\right)^\chi \text{ is a free module of rank 1 over } \mathbb{Z}_p$$

Sketch: K is tot. imag. $\Rightarrow$ so is F

$\Rightarrow$ F admits $2\cdot[F:K] = 2\cdot|\mathrm{Gal}(F/K)|$ pairs of complex conjugate $\hookrightarrow \mathbb{C}$ no real embedding

Dirichlet unit $\Rightarrow$ $\#\ \mathcal{O}_F^\times/\mu_F = \mathbb{Z}^{|\mathrm{Gal}(F/K)|-1}$

Note: $\#\ \mathbb{Q}[\mathrm{Gal}(F/K)] = \mathbb{Q}^{|\mathrm{Gal}(F/K)|}$ ($\mathrm{Gal}(F/K) = \Delta$)

$\mathbb{Q}[\Delta] \simeq \mathbb{Q}^\Delta$

$$0 \to \left(\mathcal{O}_F^\times/\mu_F\right)\otimes\mathbb{Q} \to \mathbb{Q}[\Delta] \to \mathbb{Q} \to 0$$

B/c $\mathbb{Z}_p$ is flat $\mathbb{Z}$-mod $\to$ tensor with $\mathbb{Z}_p$ exact seq.

Taking χ-eig: $\left(\mathbb{Q}\otimes\mathbb{Z}_p\right)^\chi = 0$

Exercise: $(\mathbb{Q}[\Delta] \otimes \mathbb{Z}_p)^\chi$ is rank 1

LHS: Idea is to construct a sequence of primes $\mathfrak{q}$ in K and $\mathfrak{Q}/\mathfrak{q}$ of F for which the image of these primes generates A^χ

Main tool: Let $\alpha \in \mathrm{Hom}(A, \mathbb{Z}/M\mathbb{Z})$, $\neq 0$

$K \in F^\times/(F^\times)^M$

Then there exists a prime $\mathfrak{q} \in R_{1,M}$ of K and $\mathfrak{Q}$ of F above $\mathfrak{q}$ s.t

1. $\alpha([\mathfrak{Q}]) \neq 0$ $\quad$ $[\mathfrak{Q}]$: class of $\mathfrak{Q}$ in A

2. $\Rightarrow [K]_{\mathfrak{q}} = 0$

$\Leftrightarrow d \cdot \Phi_{\mathfrak{q}}(K) = 0 \Leftrightarrow K^d \in (F^\times)^M \ \forall d \in \mathbb{Z}$

Recall : ⊙ $R = \{$ square free ideals of $\mathcal{O}$ coprime to $\mathfrak{G} N_E \mathfrak{p} \mathfrak{a} \}$

$R_{\underline{n}, \underline{\underline{M}}} = \{ r \in R$ s.t every prime $\mathfrak{q} | r$ satisfies

1. $\mathfrak{q}$ splits in $K_{\underline{n}} / K$
2. $\underline{\underline{M}} \mid (N\mathfrak{q} - 1) \}$

⊙ Denote the group of ideals of F

$\mathcal{I} = \bigoplus_{\mathfrak{Q}} \mathbb{Z}\mathfrak{Q}$ $\quad \mathfrak{Q}$: prime of F

If $\mathfrak{q}$ prime in K : $\underline{\underline{\mathcal{I}_{\mathfrak{q}}}} = \bigoplus_{\mathfrak{Q} | \mathfrak{q}} \mathbb{Z}\mathfrak{Q}$

Let $x \in F$, (x) : ideal gen.

for some $M = p^k$

$[x]_{\mathfrak{q}} \in \mathcal{I}_{\mathfrak{q}} / M \mathcal{I}_{\mathfrak{q}}$

⊙ Define $\phi'_{\mathfrak{q}} : (\mathcal{O}_F/\mathfrak{q})^\times \to \mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}$

as follows. For every $\mathfrak{Q} \mid \mathfrak{q}$, let $\gamma_{\mathfrak{Q}}$

$\gamma_{\mathfrak{Q}} \in (\mathcal{O}_F/\mathfrak{Q})^\times$: the generator $\downarrow \mathbb{Z}$

Then $\alpha \in (\mathcal{O}_F/\mathfrak{q})^\times$: $\alpha \equiv \gamma_{\mathfrak{Q}}^{a_{\mathfrak{Q}}(\alpha)} \bmod \mathfrak{Q}$

$$\phi'_{\mathfrak{q}}(\alpha) := \sum_{\mathfrak{Q} \mid \mathfrak{q}} a_{\mathfrak{Q}}(\alpha) \cdot \mathfrak{Q}$$

Define $j_{\mathfrak{q}} : \{K \in F^\times/(F^\times)^M : [K]_{\mathfrak{q}} = 0\}$

$K \downarrow$ $\qquad\qquad \downarrow$

$\mathcal{O}_F^\times \ni z$ $\qquad (\mathcal{O}_F/\mathfrak{q})^\times / ((\mathcal{O}_F/\mathfrak{q})^\times)^M$

s.t $\mathrm{ord}_{\mathfrak{Q}}(z) = 0 \ \forall \mathfrak{Q} \mid \mathfrak{q}$

$$\boxed{\phi_{\mathfrak{q}} := \phi'_{\mathfrak{q}} \circ j_{\mathfrak{q}}}$$

Sketch of main tool :

Define $\rho \in \mathrm{Hom}(G_{F_M}, \mu_M)$

$\| \; F(\mu_M)$

$\sigma \mapsto (K^{1/M})^{\sigma - 1}$

$\alpha \in \mathrm{Hom}(A, \mathbb{Z}/M\mathbb{Z})$

Define $H_\alpha = \{ \sigma \in G_{F_M} : \alpha(\sigma) = 0 \}$

$H_\rho = \{ \sigma \in G_{F_M} : \rho(\sigma)$ has order less than the order of K in $F^\times/(F^\times)^M$

$\|$ By Kummer theory: $\exists \gamma \in G_{F_M}$ s.t

$\gamma \notin H_\rho \cup H_\alpha$

Let L be a finite Galois ext. of F containing

$\left\{ \begin{array}{l} F_M = F(\mu_M) \\ H : \text{Hilbert class field of } F \end{array} \right.$

s.t both α and ρ are trivial in the subgp of G_L

Chebotarev: choose a prime $\mathfrak{Q}'$ of L coprime to $G \cdot d \cdot N_E$ s.t. if $\mathfrak{q}$ is the prime of K below $\mathfrak{Q}'$,

$$\begin{cases} [K]_{\mathfrak{q}} = 0 \\ \gamma|_L = \mathrm{Frob}_{\mathfrak{Q}'} \end{cases}$$

Choose $\mathfrak{Q}$ be the prime of F below $\mathfrak{Q}'$
c is ideal class of $\mathfrak{Q}$ in A.

Main theorem: Let χ is irred. character of $A = \mathrm{Gal}(H_1^m/F)$

$$\#\, A^{\chi} \leq \#\left(\mathcal{O}_F^{\times} / \langle \mu_F, \eta(1,0) \rangle\right)^{\chi}$$

Sketch: ⊙ χ is trivial, $A^{\chi} = 0$

⊙ χ is non-trivial: $\left(\mathcal{O}_F / \underbrace{\langle \mu_F, \eta(1,0) \rangle}_{\mathfrak{C}}\right)^{\chi}$

$$\simeq \mathbb{Z}_p / \underline{m}\mathbb{Z}_p$$

$m = p^k$ for some $k \geq 0$.

1. Use the main tool to construct

classes $c \in A$ $\{c_i\}$

$K \in F^\times/(F^\times)^M$ $\{k_i\}$ relates to Euler system

ES $\leftrightarrow$

2. $\{c_i^\chi\}$ generate A^χ. Let

s_i = order of c_i^χ in $A^\chi/\langle c_1^\chi, \ldots, c_{i-1}^\chi \rangle$

$$\# A^\chi = \prod_{i=1}^{k} s_i$$

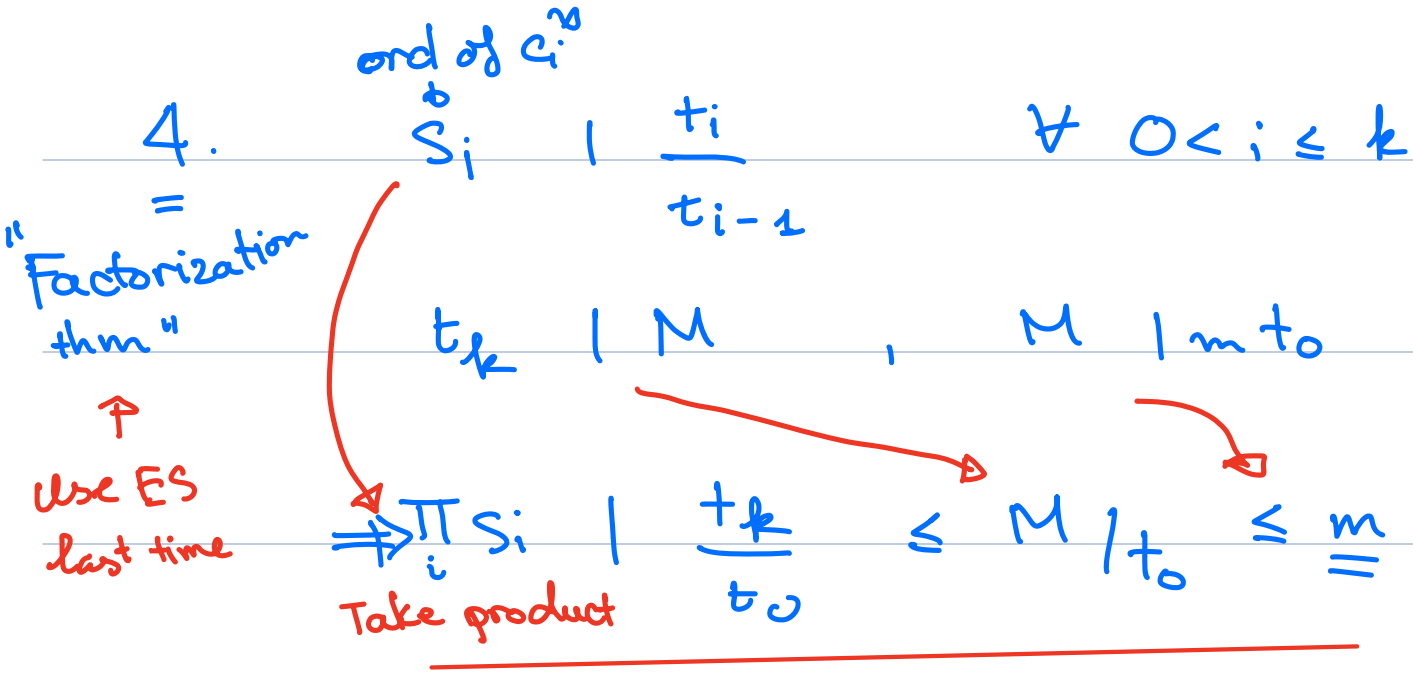
3.

t_i = order of K^χ in $F^\times/(F^\times)^M$

$\Rightarrow$ $t_i \mid t_{i+1}$

We choose $M = p \cdot \# \left(\mathcal{O}_F^\times/c\right)^\chi \cdot \# A^\chi$

$\Rightarrow$ $M/m \mid t_0 \mid t_i \quad \forall i$



We used ES in the construction of K_i
(I didn't write down explicitly)

and in their properties in the last steps
(3, 4)