Stickelberger's and Herbrand's theorems

Motivation.

Understanding class numbers is essential in Iwasawa theory.

Iwasawa's theorem - growth of class numbers

Vandiver's conjecture — $p \nmid h_{\mathbb{Q}(\zeta_p)^+}$

On that note, no more Iwasawa — all cyclotomy.

Analytic class number formula

$$\operatorname{res}_{s=1}(\zeta_K, s) = \frac{2^{r_1}(2\pi)^{r_2} \operatorname{Reg}_K \, h_K}{w_K \sqrt{|\operatorname{disc}_K|}}$$

$$\zeta_K(s) = \prod L(s, \chi)$$

$$\prod L(1, \chi) = \text{RHS.}$$

(what are these?)

Def. χ prim Dirichlet char, $f_\chi \mid m$, $B_{n,\chi}$ are s.t.

$$\sum_{a=1}^{m} \chi(a) \frac{te^{at}}{e^{mt}-1} = \sum_{n \geq 0} B_{n,\chi} \frac{t^n}{n!}$$

Facts

$\tau(\chi) = \sum_{a=1}^{f_\chi} \chi(a)\zeta_f^a$

- $L(\chi,1) = \dfrac{\pi i\, \tau(\chi)}{f_\chi} B_{1,\bar\chi}$ χ odd

- $B_{1,\chi} = \dfrac{1}{m}\sum_{a=1}^{m} \chi(a)\, a$

Let $\omega : \mathbb{F}_p^\times \longrightarrow \mu_{p-1}(\mathbb{Z}_p)$ be inverse to reduction mod p

(Teichmüller character) $\sigma(\zeta) = \zeta^{\omega(\sigma)}$

$\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \mathbb{F}_p^\times$

- $B_{1,\omega^n} \equiv \dfrac{B_{n+1}}{n+1} \bmod p$ if n odd, $n \not\equiv -1 \bmod p-1$

and both sides are in $\mathbb{Z}_p$.

Thus, analytic class number formula implies a connection between Bernoulli numbers and class numbers.

Thm (Kummer). $p \mid h_{\mathbb{Q}(\zeta_p)}^+ \iff p \mid B_j$ for some $j = 2, 4, \dots, p-3$

"pf." the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)^+/\mathbb{Q}) \cong \{1, \omega^2, \dots, \omega^{p-3}\}$

use the formulae above

Rmk. $p \nmid h_{\mathbb{Q}(\zeta_p)}^+$ yields proof of FLT for exponent p.

Herbrand's thm

Now, we refine this

Def. G fin Ab, $\chi \in \hat{G}$

$$\varepsilon_\chi := \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\, \sigma^{-1}$$

this makes sense in $R[G]$ for any ring R s.t. $|G| \in R^\times$ and $\chi(\sigma) \in R \ \forall \chi \forall \sigma$

Prop. 1. The ε_χ are orthogonal idempotents in $R[G]$ summing to 1

2. $\varepsilon_\chi \sigma = \chi(\sigma)\, \varepsilon_\chi$

Cor. Let M be an $R[G]$-module. Then $M = \bigoplus_\chi M_\chi$ where $M_\chi = \varepsilon_\chi M = \chi(\sigma)$-eigenspace of $\sigma : M \to M$.

e.g. $G = G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \mathbb{F}_p^\times$

$\hat{G} = \{\omega^i \mid 0 \le i \le p-2\}$

A = p-part of $Cl_{\mathbb{Q}(\zeta_p)}$, a $\mathbb{Z}_p[G]$-module

Then $A = \bigoplus A_{\omega^i}$. Let $A_i = A_{\omega^i}$.

Thm (Herbrand). $3 \le i \le p-2$ odd

$A_i \neq 0 \Rightarrow p \mid B_{1,\omega^{-i}}$

By a Bernoulli fact, this implies that $p \mid B_{p-i}$

(Converse is Ribet's pf. Zi L.)

This is a refinement of Kummer's result

Recall $p \nmid h_{\mathbb{Q}(\zeta_p)} \rightsquigarrow$ FLT(p)

$\approx 60\%$ expected to satisfy this

w/a more careful analysis of how many Bernoulli numbers a prime divides, can use weird heuristics to estimate $1 - 10^{-300000}$ percent of primes have FLT.

Thus, a Herbrand-Ribet refinement of Kummer's result aids this sort of thing.

How to prove Herbrand?

Stickelberger theory

Def. $\{x\} \in [0,1)$ fractional part

$G = G(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ for $m \geq 1$

$\theta = \sum_{a \in (\mathbb{Z}/m)^\times} \left\{\frac{a}{m}\right\} \sigma_a^{-1} \in \mathbb{Q}[G]$ Stickelberger element

$\mathcal{J} = \mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$ ideal

Lemma. $I = \langle b - \sigma_b \mid (b,m)=1 \rangle$

Then $I = \{ r \in \mathbb{Z}[G] \mid r\theta \in \mathbb{Z}[G] \}$

Thm. (Stickelberger) $\mathcal{J}$ annihilates $Cl_{\mathbb{Q}(\zeta_p)}$.

pf. Later

pf. of Herbrand's thm. supposing Stickelberger

where's the Bernoulli?

$\theta = \frac{1}{p} \sum_{a=1}^{p-1} a\sigma_a^{-1}$. $\varepsilon_i \theta = \frac{1}{p} \sum_{a=1}^{m-1} a\omega^{-i}(a)\varepsilon_i = B_{1,\omega^{-i}}\varepsilon_i$

so $\varepsilon_i (b - \sigma_b)\theta = (b - \omega^i(b)) B_{1,\omega^{-i}} \varepsilon_i \in \mathcal{J}$.

Hence, this annihilates A_i.

Rmk. We can show $\{1\}$ but $i=1$ is interesting

Let $b = 1+p$

$$\left((1+p) - \omega(1+p)\right) B_{1,\omega^{-1}} = p\, B_{1,\omega^{-1}}$$

$$= \sum_{a=1}^{p-1} a\omega^{-1}(a)$$

$$\left(\omega \text{ is inverse to reduction mod } p\right) \equiv p-1 \mod p$$

thus, this element is non zero mod p, hence a p-adic unit. But it annihilates A_1, a finite p group $\Rightarrow$ a $\mathbb{Z}_p$-module. units can only kill 0. $\therefore A_1 = 0$

Let $3 \le i \le p-2$ odd.

Let b be a primitive root mod p

$$b^i \equiv \omega^i(b) \bmod p$$

$$\#\#$$

$$b$$

so $b - \omega^i(b)$ a p-adic unit

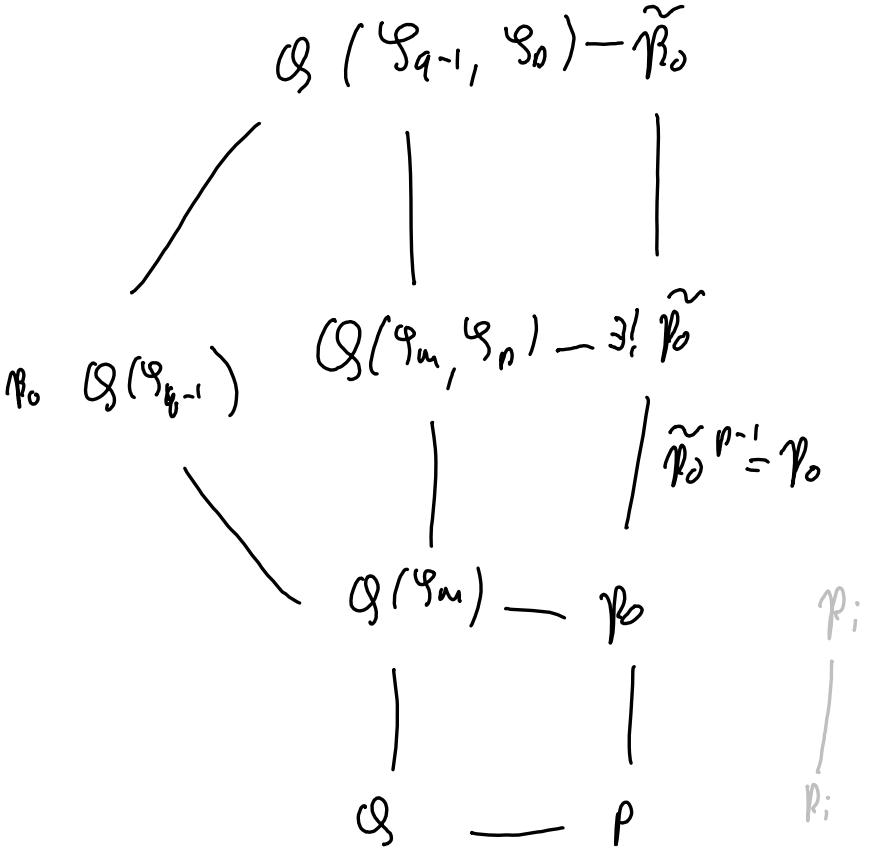
$(b - \omega^i b) B_{1,\omega^{-i}}$ kills A_i, so $B_{1,\omega^{-i}}$ kills A_i

If $A_i \neq 0$, $B_{1,\omega^{-i}}$ cannot be a p-adic unit, so $p \mid B_{1,\omega^{-i}}$

Back to Stickelberger

$m \geq 1$, $(p, m) = 1$, $f = \text{ord}_{\mathbb{Z}/m\mathbb{Z}^\times}(p)$ mod m, $q = p^f$.

Then $m \mid q-1$ $\therefore$ let $d = \frac{q-1}{m}$



Idea. factor a Gauss sum to get a solution in the class group.

Def. $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$. $g(\chi) := -\sum_{a \in \mathbb{F}_q^\times} \chi(a)\, \zeta_p^{\mathrm{Tr}(a)}$

Take $\chi = \omega^{-d}$.

Rmk. $g(\chi)\overline{g(\chi)} = q$, so its factorization contains only primes $/p$

Also, $\chi^m = 1$ so $g(\chi) \in \mathcal{O}(\zeta_m, \zeta_p)$, so

$$(g(\chi)) = (\tilde{\beta}_0)^{v_{\tilde{\beta}_0}(g(\chi))}$$

Step 1. $\mathfrak{p}_0^{m\theta} = (g(\chi)^m)$ in $\mathcal{O}(\zeta_m, \zeta_p)$

"Pf" compute $v_{\tilde{\beta}_0}(g(\chi))$ somehow.

rmk. use $\tilde{\beta}_0^{p-1} = p_0$ to get that in there

see Washington

Step 2. Move this relation down to $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$.

Pf. $\mathcal{I} \subseteq \mathcal{O}(\zeta_m)$ an integral ideal s.t. $(\mathcal{I}, m) = 1$.

$\mathcal{I} = \prod \mathfrak{p}_i$

ala step 1, $\mathfrak{p}_i^{m\theta} = (g(\pi_i)^m)$

Let $\gamma = \prod g(\chi_i)$, so $\mathcal{I}^{m\theta} = (\gamma^m)$

Let $\beta \in \mathbb{Z}[G]$ s.t. $\beta\theta \in \mathbb{Z}[G]$

Let $P = \prod p_i$. Then $\gamma \in \mathcal{O}(\zeta_{mp})$.

and $\pm^{m \mid \theta} = \left(\zeta^{p^m}\right)$

at each completion, $\mathcal{O}(\zeta_m, \gamma^\beta)/\mathcal{O}(\zeta_m)$ looks like adjoining an m^{th} root of an element as we got DVRs at all completions

Thus, ramification can occur only at m

$$\mathcal{O}(\zeta_{mp}) / \underbrace{\mathcal{O}(\zeta_m, \gamma^\beta) / \mathcal{O}(\zeta_m}_{m \text{ ramification}} \Big/$$

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{p \text{ ramification}}$$

$(m, p) = 1$ so $\mathcal{O}(\zeta_m, \gamma^\beta)/\mathcal{O}(\zeta_m)$ is unramified.

Lemma. $\mathcal{O}(\zeta_n) / \underbrace{K / \mathcal{O}(\zeta_m)}_{\text{unramified}}$ Then $K = \mathcal{O}(\zeta_m)$.

pf. Per Washington, $\exists x$ for K s.t. $f_x \nmid m$ $\therefore$ ramified, so

contrapositive → Say $m = p^e$

or, Let E be the p-inertia. so p unram in $E/\mathcal{O}$.

If $q \neq p$, q unram in K $\therefore$ $E/\mathcal{O}$ unramified $\therefore E = \mathcal{O}$.

$\therefore$ $\mathfrak{p}$ totally ramified in K, and in $\mathcal{O}(\zeta_m)$, so $K = \mathcal{O}(\zeta_m)$ as it's unramified

Hence, $\gamma^\beta \in \mathcal{O}(\zeta_m)$

so $I^\beta \mathcal{O} = (\gamma^\beta)$ in $\mathcal{O}(\zeta_m)$

$\therefore \beta\theta \in \mathcal{L}$ annihilating $Cl_{\mathcal{O}(\zeta_m)}$

Rmk. can do this $K/\mathbb{Q}$ ab via $K \subseteq \mathcal{O}(\zeta_m)$ and counting $G(\mathcal{O}(\zeta_m)/K)$ actions

step 3. $(I, m) = 1$ dependence

all ideal classes are representable by ideals prime to m

eg, Ramyar asserts all prime $\mathfrak{L}$ s.t. $\mathfrak{L}/\ell$ and ℓ completely split.

Chebotarev density