On the Herbrand–Ribet's Theorems

Nicolas Keng

2026/6/21

目录

我们具体地阐述了 Herbrand 和 Ribet 关于分圆域类群中特征分量的结果. 对偶数 $k \in [2, p-3]$, Herbrand–Ribet 定理断言

$$A^{(1-k)} \neq 0 \iff p \mid B_k,$$

其中 A 是 $\mathbb{Q}(\zeta_p)$ 的类群的 p-primary part. Herbrand 的方向利用 Stickelberger 理想对类群的零化作用, 将 $A^{(1-k)} \neq 0$ 转化为广义 Bernoulli 数的消失, 再由 Kummer 同余推出 $p \mid B_k$.

Ribet 的逆向证明从 Eisenstein 级数之间的模 $\mathfrak{p}$ 同余出发, 利用 Deligne–Serre 提升引理构造 weight-2, level-p 的正规尖特征形式. 随后通过相伴的 p-adic Galois 表示和 Ribet 引理选取适当的稳定格, 得到一个非分裂的剩余表示

$$\begin{pmatrix} 1 & * \\ 0 & \omega^{k-1} \end{pmatrix}.$$

Raynaud 的有限平坦群概形唯一延拓定理用于证明该表示在 p 处半单, 从而构造出 $\mathbb{Q}(\zeta_p)$ 上处处非分歧的非平凡 p-初等 Abel 扩张, 其 Galois 群上的 Δ-作用由 ω^{1-k} 给出. 类域论于是推出 $A^{(1-k)} \neq 0$.

最后, 我们说明了这一结论的现代上同调表述.

设 p 为奇素数. 令

- A 表示类群 $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ 的 p-primary part, 即 p-Sylow 子群

$$\mathrm{Cl}(\mathbb{Q}(\zeta_p))[p^\infty] := \left\{ [\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Q}(\zeta_p)) \,\middle|\, \mathfrak{a}^{p^n} = (\alpha) \text{ is principal ideal}, \exists n \in \mathbb{Z}_{\geq 0} \right\};$$

- $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, 其同构由 $a \mapsto \sigma_a$, $\sigma_a(\zeta_p) = \zeta_p^a$ 给出;
- $\omega : \Delta \to \mathbb{Z}_p^\times$ 为 Teichmüller 特征, 满足 $\omega(\delta) \equiv \delta \pmod p$, 其中 $\delta \in \Delta$ 视为 $(\mathbb{Z}/p\mathbb{Z})^\times$ 中的元素.

我们一般不区分 $\omega(\sigma_a)$ 和 $\omega(a)$.

由于 $p \nmid |\Delta|$, 由 Maschke 定理, 群环 $\mathbb{Z}_p[\Delta]$ 是半单的, Δ 的全体不可约表示恰是 ω^i, $i = 0, 1, \cdots, p-2$. 因此, 有一组正交幂等元:

$$\{e_i\}_{i=0}^{p-2}, \quad e_i = \frac{1}{p-1} \sum_{\delta \in \Delta} \omega(\delta)^{-i} \delta \in \mathbb{Z}_p[\Delta],$$

即它满足

$$e_i e_j = 0, \quad e_i^2 = e_i, \quad \sum_{i=0}^{p-2} e_i = 1, \ (\forall i, \forall j \neq i).$$

这诱导了 $\mathbb{Z}_p[\Delta]$ 的半单分解:

$$\mathbb{Z}_p[\Delta] = \bigoplus_{i=0}^{p-2} \mathbb{Z}_p e_i.$$

将其作用在 A 上, 得到 A 的分解 $A = \bigoplus_{i=0}^{p-2} A^{(i)}$, 其中

$$A^{(i)} := e_i A = \left\{ a \in A \,\middle|\, \delta(a) = \omega(\delta)^i a, \forall \delta \in \Delta \right\}.$$

Kummer 在他研究 FLT 的时候证明了

Thm 0.1 (Kummer) $A \neq 0$ 当且仅当 p 整除某个 Bernoulli 数, 即 p 整除 Bernoulli 数 $B_2, B_4, \cdots, B_{p-3}$ 的分子.

现在我们将结果细化到特征分量的层面.

Thm 0.2 (Herbrand–Ribet) $A^{(1-k)} \neq 0 \iff p | B_k$, 其中 $2 \mid k$ 且 $2 \leq k \leq p-3$.

Herbrand [Her32] 证明了方向 $\Rightarrow$, Ribet [Rib76] 证明了方向 $\Leftarrow$.

1 Bernoulli Numbers

Def 1.1 Bernoulli 数 B_n 由生成函数

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

定义. 例如 $B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}$.

Def 1.2 Bernoulli 多项式 $B_n(X)$ 由生成函数

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!}$$

定义. 于是

$$B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}.$$

例如 $B_1(X) = X - \frac{1}{2}, B_2(X) = X^2 - X + \frac{1}{6}$.

Def 1.3 设 χ 是导子为 f 的 Dirichlet 特征. 广义 Bernoulli 数 $B_{n,\chi}$ 由

$$\sum_{a=1}^{f} \chi(a)\frac{te^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}$$

定义.

Prop 1.1 若 g 是 f 的任意正倍数, 则

$$B_{n,\chi} = g^{n-1}\sum_{a=1}^{g} \chi(a)B_n\left(\frac{a}{g}\right).$$

Proof. 比较生成函数. 由 Bernoulli 多项式的定义,

$$\sum_{n=0}^{\infty} g^{n-1}\sum_{a=1}^{g} \chi(a)B_n\left(\frac{a}{g}\right)\frac{t^n}{n!} = \sum_{a=1}^{g} \chi(a)\frac{1}{g}\frac{gte^{at}}{e^{gt} - 1}.$$

写 $g = hf$ 且 $a = b + cf$, 其中 $1 \le b \le f, 0 \le c \le h - 1$. 因为 $\chi(b + cf) = \chi(b)$, 上式等于

$$\sum_{b=1}^{f}\sum_{c=0}^{h-1} \chi(b)\frac{te^{(b+cf)t}}{e^{fht} - 1} = \sum_{b=1}^{f} \chi(b)\frac{te^{bt}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}.$$

比较 t^n 的系数即得. □

Lemma 1.2 $L(1 - n, \chi) = -\frac{B_{n,\chi}}{n}, n \ge 1$.

Proof. 由 Hurwitz zeta 函数的特殊值公式

$$\zeta(1 - n, x) = -\frac{B_n(x)}{n}$$

以及

$$L(s, \chi) = f^{-s}\sum_{a=1}^{f} \chi(a)\zeta\left(s, \frac{a}{f}\right),$$

得到

$$L(1-n,\chi)=f^{n-1}\sum_{a=1}^{f}\chi(a)\zeta\left(1-n,\frac{a}{f}\right)=-\frac{1}{n}f^{n-1}\sum_{a=1}^{f}\chi(a)B_n\left(\frac{a}{f}\right).$$

由 **Prop** 1.1 取 $g=f$, 右边等于 $-\dfrac{B_{n,\chi}}{n}$. □

Eg 1.1 若 χ 是模 p 的 Dirichlet 特征, 则

$$L(0,\chi)=-B_{1,\chi}=-\frac{1}{p}\sum_{a=1}^{p}\chi(a)\left(a-\frac{p}{2}\right),$$

且

$$L(-1,\chi)=-\frac{B_{2,\chi}}{2}=-\frac{1}{2p}\sum_{a=1}^{p}\chi(a)\left(a^2-pa+\frac{p^2}{6}\right).$$

Lemma 1.3 令

$$S_m(n)=1^m+2^m+\cdots+(n-1)^m.$$

则

$$(m+1)S_m(n)=\sum_{k=0}^{m}\binom{m+1}{k}B_k n^{m+1-k}.$$

Proof. 由生成函数计算,

$$\begin{aligned}\sum_{m=0}^{\infty}S_m(n)\frac{t^m}{m!}&=\sum_{a=0}^{n-1}e^{at}=\frac{e^{nt}-1}{e^t-1}\\&=\left(\sum_{l=1}^{\infty}n^l\frac{t^{l-1}}{l!}\right)\left(\sum_{k=0}^{\infty}B_k\frac{t^k}{k!}\right).\end{aligned}$$

比较 t^m 的系数, 得

$$\frac{S_m(n)}{m!}=\sum_{k=0}^{m}\frac{B_k}{k!}\frac{n^{m+1-k}}{(m+1-k)!}.$$

两边乘以 $(m+1)!$ 即得. □

Prop 1.4 pB_m 是 p-整的. 若 $(p-1)\nmid m$, 则 B_m 是 p-整的.

Proof. 对 m 归纳. 由 **Lem** 1.3 取 $n=p$ 并重排, 有

$$S_m(p)=pB_m+\binom{m}{1}B_{m-1}\frac{p^2}{2}+\binom{m}{2}B_{m-2}\frac{p^3}{3}+\cdots+B_0\frac{p^{m+1}}{m+1}.$$

归纳假设给出 pB_j 对 $j<m$ 都是 p-整的. 因此右边除第一项外的所有项都是 p-整且模 p 为 0, 从而 pB_m 也是 p-整, 并且

$$pB_m\equiv S_m(p)\pmod{p}.$$

若 $(p-1)\nmid m$, 则

$$S_m(p)=\sum_{a=1}^{p-1}a^m\equiv 0 \pmod p,$$

所以 $pB_m\equiv 0 \pmod p$, 即 B_m 是 p-整的. □

Lemma 1.5 *若 m 为正偶数且 $p\geq 5$, 则*

$$pB_m\equiv\sum_{a=1}^{p-1}a^m \pmod{p^2}.$$

Proof. 仍使用 **Lem** 1.3 中 $S_m(p)$ 的展开. 对 $k\geq 2$, 项

$$\binom{m}{k}B_{m-k}\frac{p^{k+1}}{k+1}$$

的 p-进阶至少为 2, 因为 pB_{m-k} 是 p-整且 $k-\mathrm{ord}_p(k+1)\geq 2$. 对 $k=1$, 若 $m>2$, 则 $B_{m-1}=0$; 若 $m=2$, 该项为 $2B_1p^2/2$, 也被 p^2 整除. 因此

$$S_m(p)\equiv pB_m \pmod{p^2}.$$

由于 $S_m(p)=\sum_{a=1}^{p-1}a^m$, 结论成立. □

Prop 1.6 (Kummer) *若 $m\equiv n\not\equiv 0 \pmod{p-1}$, 则*

$$\frac{B_m}{m}\equiv\frac{B_n}{n} \pmod p.$$

Proof. 取 g 为模 p 的原根. 考虑

$$F(t)=\frac{gt}{e^{gt}-1}-\frac{t}{e^t-1}=\sum_{m=1}^{\infty}(g^m-1)B_m\frac{t^m}{m!}.$$

令 $u=e^t-1$, 则

$$F(t)=tG(u),\quad G(u)=\frac{g}{(1+u)^g-1}-\frac{1}{u}=\sum_{r=0}^{\infty}c_ru^r,\quad c_r\in\mathbb{Z}_{(p)}.$$

于是

$$G(e^t-1)=\sum_{r=0}^{\infty}c_r(e^t-1)^r=\sum_{m=1}^{\infty}A_m\frac{t^m}{m!},$$

其中 A_m 都是 p-整的. 进一步, $(e^t-1)^r$ 的系数是整数 r^m 的整线性组合, 因此由 Fermat 小定理, $A_{m+p-1}\equiv A_m \pmod p$.

比较 $F(t)=tG(e^t-1)$ 中 t^m 的系数, 得

$$(g^m-1)\frac{B_m}{m}=A_{m-1}.$$

若 $(p-1)\nmid m$, 则 $g^m-1\not\equiv 0 \pmod p$. 因而 $\dfrac{B_m}{m}$ 是 p-整的. 又当 $m\equiv n\not\equiv 0 \pmod{p-1}$ 时,

$$g^m-1\equiv g^n-1 \pmod p, \quad A_{m-1}\equiv A_{n-1} \pmod p.$$

于是

$$\frac{B_m}{m}\equiv\frac{B_n}{n} \pmod p.$$

□

2 Herbrand's Theorem

Stickelberger's Theorem

对一般的 Abel 数域 F, 设 $G=\mathrm{Gal}(F/\mathbb{Q})$ 为其 Galois 群. 由 Kronecker–Weber 定理, 存在正整数 n 使得 $F\subseteq\mathbb{Q}(\mu_n)=F_n$, 记 $G_n=\mathrm{Gal}(F_n/\mathbb{Q})$, 则有限制同态:

$$\mathrm{res}_n: G_n\to G, \quad \sigma\mapsto\sigma|_F.$$

Def 2.1 对分圆域 $F_n=\mathbb{Q}(\zeta_n)$, 其 **Stickelberger 元素**定义为:

$$\theta(F_n)=\frac{1}{n}\sum_{\substack{a=1\\(a,n)=1}}^{n} a\sigma_a^{-1}\in\mathbb{Q}[G_n].$$

对一般的 Abel 数域 F, 其 Stickelberger 元素定义为:

$$\theta(F)=\frac{1}{n}\sum_{a=1}^{n} a\cdot\mathrm{res}_n(\sigma_a^{-1})\in\mathbb{Q}[G].$$

Def 2.2 Abel 数域 F 的 **Stickelberger 理想** $I(F)$ 定义为:

$$I(F)=\theta(F)\mathbb{Z}[G]\cap\mathbb{Z}[G]\lhd\mathbb{Z}[G].$$

对于分圆域 $F=F_m$ 结果类似; 此时 $I(F_m)$ 可由 $(a-\sigma_a)\theta(F_m)$ 生成.

这本质上就是 $\mathbb{Z}[G]$ 中所有形如 $\theta(F)\cdot x$ 的元素组成的理想.

Thm 2.1 (Stickelberger) 对任意 Abel 数域 F, Stickelberger 理想 $I(F)$ 零化 $\mathrm{Cl}(F)$, 即

$$I(F)\cdot\mathrm{Cl}(F)=0.$$

Proof. [Was12, Thm 6.10]. □

Eg 2.1 若 F 是全实 Abel 数域, 则:

$$\theta(F)=\frac{\varphi(n)}{2[F:\mathbb{Q}]}\sum_{\sigma\in G}\sigma.$$

我们显然可以在 $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ 下讨论 Stickelberger 理想, 此时 $I_p = I(F)\mathbb{Z}_p[\Delta]$ 恰好是 $I(F)$ 在 $\mathbb{Z}_p[\Delta]$ 中的扩张, 依旧零化 A.

我们来看 Herbrand 的证明. 记 $\theta := \theta(\mathbb{Q}(\zeta_p))$ 是 Stickelberger 元,

Proof of Thm 0.2, $\Rightarrow$. 首先证明对任意 $(b,p)=1$, $(\sigma_b - b)\theta \in I_p$. 这是因为 $\sigma_b - b \in \mathbb{Z}_p[\Delta]$, 且

$$\begin{aligned}(\sigma_b - b)\theta &= \frac{1}{p}\sum_{a=1}^{p-1} a\sigma_a^{-1}\sigma_b - \frac{1}{p}\sum_{a=1}^{p-1} ab\sigma_a^{-1} \\ &= \frac{1}{p}\sum_{c=1}^{p-1}(c^{-1}b \bmod p)\sigma_c^{-1} - \frac{1}{p}\sum_{d=1}^{p-1} b(d^{-1} \bmod p)\sigma_d \\ &= \frac{1}{p}\sum_{k=1}^{p-1}\left((bk^{-1} \bmod p) - b(k^{-1} \bmod p)\right)\sigma_k \in \mathbb{Z}[\Delta] \subset \mathbb{Z}_p[\Delta].\end{aligned}$$

其中我们做了变量替换 $c = a^{-1}b \pmod p$ 和 $d = a^{-1} \pmod p$. 既然 I_p 零化 A, 那让 $(\sigma_b - b)\theta$ 作用在 $A^{(1-k)}$ 上就应该为零. 对任意 $x \in A^{(1-k)}$, 由定义有 $\sigma_a(x) = \omega(a)^{1-k}x$, 故:

$$\sigma_b\sigma_a^{-1}(x) = \sigma_b(\omega(a)^{k-1}x) = \omega(b)^{1-k}\omega(a)^{k-1}x.$$

代入, 注意到 $B_{1,\chi} = \dfrac{1}{N}\displaystyle\sum_{a=1}^{N}\chi(a)a$, 有

$$\begin{aligned}(\sigma_b - b)\theta \cdot x &= \frac{1}{p}\sum_{a=1}^{p-1} a\sigma_b\sigma_a^{-1}(x) - \frac{1}{p}\sum_{a=1}^{p-1} ab\sigma_a^{-1}(x) \\ &= \left(\omega(b)^{1-k} - b\right)\left(\frac{1}{p}\sum_{a=1}^{p-1} a\omega^{k-1}(a)\right)\cdot x \\ &= \left(\omega(b)^{1-k} - b\right) B_{1,\omega^{k-1}} \cdot x = 0.\end{aligned}$$

但是存在 $b \in (\mathbb{Z}/p\mathbb{Z})^\times$ 使得 $\omega(b)^{1-k} \not\equiv b \pmod p$, 即 $\omega(b)^{1-k} - b$ 是 $\mathbb{Z}_p^\times$ 中的单位. 这是因为 $p-1 \nmid k$ 时, $\mathbb{F}_p^\times$ 中不可能每个元素的阶都整除 k.

现在计算 $B_{1,\omega^{k-1}}$ 与普通 Bernoulli 数的同余. 由 **Lem 4.2**, 有 $\omega(a) \equiv a^p \pmod{p^2}$. 令

$$t = 1 + p(k-1).$$

则 t 为正偶数, $t \equiv k \pmod{p-1}$, 且 $t \equiv 1 \pmod p$. 因为 $\displaystyle\sum_{a=1}^{p-1}\omega^{k-1}(a) = 0$, 有

$$B_{1,\omega^{k-1}} = \frac{1}{p}\sum_{a=1}^{p-1} a\omega^{k-1}(a) \equiv \frac{1}{p}\sum_{a=1}^{p-1} a^t \equiv B_t \pmod p.$$

这里最后一步使用了 **Lem 1.5**. 再由 **Prop 1.6**,

$$B_t = t\frac{B_t}{t} \equiv t\frac{B_k}{k} \equiv \frac{B_k}{k} \pmod p.$$

若 $A^{(1-k)} \neq 0$, 则 $B_{1,\omega^{k-1}} \equiv 0 \pmod{p}$, 因此 $p|B_k$. □

3 Statement of Ribet's Result

Thm 3.1 (Ribet, 1976) *设 $k \in [2, p-3]$ 为偶数. 若 $p|B_k$, 则 $A^{(1-k)} \neq 0$.*

我们遵循 Ribet 的原始证明思路, 之后固定 $k \in [2, p-3]$ 为偶数. 首先将解释如何将这一结论归结为构造一个具有特定性质的 Galois 表示.

Thm 3.2 *设 $p|B_k$. 则存在 Galois 扩张 $F/\mathbb{Q}$ 包含 $\mathbb{Q}(\zeta_p)$, 满足*

i. *扩张 $F/\mathbb{Q}(\zeta_p)$ 处处非分歧;*
ii. *群 $H = \mathrm{Gal}(F/\mathbb{Q}(\zeta_p))$ 是非零有限维 $\mathbb{F}_p$ 空间, 即 $H \cong (\mathbb{F}_p)^n$, $n > 0$;*
iii. *$\forall \sigma \in \mathrm{Gal}(F/\mathbb{Q})$, 记 $\bar{\sigma} \in \Delta$ 为其在 $\mathbb{Q}(\zeta_p)$ 上的限制, 有*

$$\forall \tau \in H,\ \sigma\tau\sigma^{-1} = \omega(\bar{\sigma})^{1-k} \cdot \tau.$$

Proof of Thm 3.2 ⇒ Thm 3.1. *令 $K = \mathbb{Q}(\zeta_p)$. 商群 A/pA 是 K 的理想类群的最大 p-初等商. 令 L/K 为最大处处非分歧的 p-初等 Abel 扩张. 由于 K 的类群有限, L/K 是有限扩张, 且类域论给出 $\mathbb{F}_p$-空间的同构*

$$\psi : A/pA \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

首先说明 $L/\mathbb{Q}$ 是 Galois 扩张. 对任意 $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, 因为 $K/\mathbb{Q}$ 是 Galois 扩张, 共轭域 $\sigma(L)$ 仍包含 K. 而且 $\sigma(L)/K$ 仍然处处非分歧, 其 Galois 群仍是 p-初等 Abel 群. 由 L 的最大性有 $\sigma(L) \subset L$. 对 σ^{-1} 应用同一论证得到反包含, 因而 $\sigma(L) = L$. 所以 $L/\mathbb{Q}$ 是 Galois 扩张.

下面说明 ψ 与 $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ 的作用相容. 在 A/pA 上, $\bar{\sigma} \in \Delta$ 通过理想共轭作用; 在 $\mathrm{Gal}(L/K)$ 上, $\bar{\sigma}$ 通过共轭作用. 具体地, 取 $\bar{\sigma}$ 在 $\mathrm{Gal}(L/\mathbb{Q})$ 中的一个提升 $\tilde{\sigma}$, 并对 $x \in A/pA$ 选取一个由理想类 $[\mathfrak{a}] \in A$ 给出的提升. Artin 符号与域自同构相容, 因而在本文采用的 Artin 映射约定下,

$$\psi(\bar{\sigma}x) = \tilde{\sigma}\psi(x)\tilde{\sigma}^{-1}.$$

右端与 $\tilde{\sigma}$ 的选取无关, 因为两个提升之差属于 Abel 群 $\mathrm{Gal}(L/K)$. 因此 ψ 是 $\mathbb{F}_p[\Delta]$-模同构.

现在设 $F/\mathbb{Q}$ 满足 Thm 3.2. 因为 F/K 处处非分歧, 且

$$H = \mathrm{Gal}(F/K)$$

是非零 p-初等 Abel 群, 由 L 的最大性有 $F \subset L$. 限制映射给出非零满射

$$\mathrm{Gal}(L/K) \twoheadrightarrow H.$$

又因为 $F/\mathbb{Q}$ 是 Galois 扩张, 这个限制映射与 Δ 的共轭作用相容. 结合 ψ, 得到一个 $\mathbb{F}_p[\Delta]$-模满射

$$A/pA \twoheadrightarrow H.$$

由条件 (iii), Δ 在 H 上通过特征 ω^{1-k} 作用. 换言之,

$$e_{1-k}H = H,$$

其中 e_{1-k} 是与 ω^{1-k} 对应的幂等元, 下标按 $p-1$ 取模. 对任意 $h \in H$, 取 $a \in A/pA$ 映到 h, 则 $e_{1-k}a$ 仍映到 $e_{1-k}h = h$. 因而限制映射诱导满射

$$(A/pA)^{(1-k)} = e_{1-k}(A/pA) \twoheadrightarrow H.$$

由于 $H \neq 0$, 得到 $(A/pA)^{(1-k)} \neq 0$.

最后, $p \nmid |\Delta|$ 保证幂等元分解与模 p 商相容, 所以

$$(A/pA)^{(1-k)} \cong A^{(1-k)}/pA^{(1-k)}.$$

左端非零立即推出 $A^{(1-k)} \neq 0$. 这正是 **Thm** 3.1 的结论. □

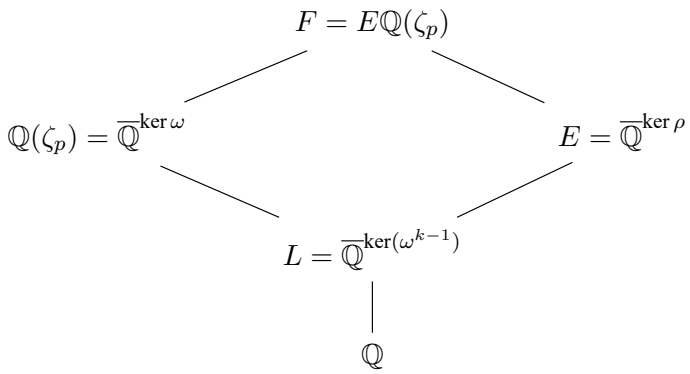
Thm 3.3 设 $p|B_k$. 则存在有限扩张 $K/\mathbb{F}_p$ 和连续表示 $\rho : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(2, K)$, 满足

1. ρ 在所有素数 $\ell \neq p$ 处非分歧;
2. ρ 是 ω^{k-1} 对于平凡特征的扩张, 即存在非平凡的 $\gamma : \mathrm{Gal}_{\mathbb{Q}} \to K$ 使得 $\rho \sim \begin{pmatrix} 1 & \gamma \\ 0 & \omega^{k-1} \end{pmatrix}$;
3. p 整除 $\mathrm{im}\,\rho$ 的阶;
4. p 不整除 $\mathrm{im}\,\rho|_{D_p}$ 的阶.

Remark. 注意, 这里的 γ 不是群同态而是 1-cocycle, 即交叉同态; 但是限制在 $\ker\omega^{k-1}$ 上是群同态.

Proof of Thm 3.3 ⇒ Thm 3.2. 默认 (1) 指代 **Thm** 3.3 中的条件, 而 (i) 指代要证的结论.

取 $\rho : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(2, K)$, $K/\mathbb{F}_p$ 满足 **Thm** 3.3 的条件, 构造如下域扩张图:



我们来证明域图中的 F 即为所求.

首先, 证明 $E \cap \mathbb{Q}(\zeta_p) = L$. 方向 $\supseteq$ 显然. 注意到

$$E \cap \mathbb{Q}(\zeta_p) \subset L \iff \ker(\omega^{k-1}) \subset \ker\rho\ker\omega,$$

取 $\sigma \in \ker\omega^{k-1}$, 那么 $\omega(\sigma)^{k-1} = 1$. 设 $\omega(\sigma)$ 的阶为 d, 则 $d|p-1$, $(d,p) = 1$, 且 $\sigma^d \in \ker\omega$. 在 $\ker\omega^{k-1}$ 上, γ 是群同态. 取整数 m 使得 $md \equiv 1 \pmod p$, 并令 $\tau = (\sigma^d)^m$. 则 $\tau \in \ker\omega$, 且

$$\gamma(\tau) = m\gamma(\sigma^d) = md\gamma(\sigma) = \gamma(\sigma).$$

因此 $\rho(\sigma\tau^{-1}) = I_2$. 我们于是有了

$$\sigma = (\sigma\tau^{-1})\tau \in \ker\rho \cdot \ker\omega, \quad E \cap \mathbb{Q}(\zeta_p) = L.$$

现在取 $H \coloneqq \mathrm{Gal}(F/\mathbb{Q}(\zeta_p)) \cong \mathrm{Gal}(E/L)$, 对应正合列:

$$1 \to \mathrm{Gal}(E/L) \to \mathrm{im}\,\rho \to \mathrm{im}\,\omega^{k-1} \to 1,$$

故 $H \cong \mathrm{im}\,\gamma\big|_{\ker\omega^{k-1}} \subseteq K$. 该像非零. 否则 γ 在 $\ker\omega^{k-1}$ 上为零, 从而降为有限群 $\mathrm{im}\,\omega^{k-1}$ 上的 1-cocycle; 但 $|\mathrm{im}\,\omega^{k-1}|$ 与 p 互素, 所以 $H^1(\mathrm{im}\,\omega^{k-1}, K) = 0$, 这迫使扩张分裂, 与 **Thm** 3.3 中的非平凡性矛盾. 因此 H 是非零有限维 $\mathbb{F}_p$-空间, 满足 **Thm** 3.2 中的条件 (ii).

现在来证明 (i), 这只需要 E/L 处处非分歧. 由 (1), 在 $\ell \neq p$ 处 $\rho(I_\ell)$ 平凡, 那么 ℓ 处 ω^{k-1} 也非分歧, 从而 $L/\mathbb{Q}$ 在 ℓ 处非分歧. 又因为 $\ker\rho \subset \ker\omega^{k-1}$, $E/\mathbb{Q}$ 也在 ℓ 处非分歧, 故 ℓ 处 E/L 非分歧.

现在来看 p 处. 由条件 (4), $p \nmid |\rho(D_p)|$, 故 $p \nmid |\rho(I_p)|$. 要证 E/L 在 p 处非分歧, 只需取

$$\sigma \in I_p \cap \ker\omega^{k-1}$$

并证明 $\rho(\sigma) = 1$. 对这样的 σ, 有

$$\rho(\sigma) = \begin{pmatrix} 1 & \gamma(\sigma) \\ 0 & 1 \end{pmatrix}.$$

若 $\gamma(\sigma) \neq 0$, 则 $\rho(\sigma)$ 是非平凡幺幂矩阵, 在特征 p 中阶为 p, 与 $p \nmid |\rho(I_p)|$ 矛盾. 因此 $\gamma(\sigma) = 0$, 即 $\rho(\sigma) = 1$. 这证明了 E/L 在 p 处非分歧, 从而得到 (i).

最后证明 (iii). 对任意 $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, 记 $\tilde\sigma$ 为 σ 在 $\mathrm{Gal}_\mathbb{Q}$ 中的提升, $\bar\sigma$ 为 σ 在 Δ 中的限制. 简记 $c = \omega(\bar\sigma)^{k-1} = \omega(\tilde\sigma)^{k-1}$. 对任意 $\tau \in H$, 它和 $t \in \mathrm{im}\,\gamma\big|_{\ker\omega^{k-1}} \subseteq K$ 对应, 即 $\rho(\tau) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$. 若 $\rho(\tilde\sigma) = \begin{pmatrix} 1 & u \\ 0 & c \end{pmatrix}$, 则

$$\begin{aligned} \rho(\tilde\sigma\tau\tilde\sigma^{-1}) &= \rho(\tilde\sigma)\rho(\tau)\rho(\tilde\sigma)^{-1} \\ &= \begin{pmatrix} 1 & u \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -uc^{-1} \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} 1 & c^{-1}t \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

故 $\sigma\tau\sigma^{-1} = \omega(\bar\sigma)^{1-k}\tau$. □

现在我们只需要找满足上述条件的 Galois 表示即可.

4 Eigenforms

回顾对 $\mathbb{F}_p^\times$ 上面非平凡的偶特征 χ, 我们有如下的 weight-2 type-χ 的 Eisenstein 级数

$$G_{2,\chi} = \frac{L(-1,\chi)}{2} + \sum_{n\geq 1}\sum_{d|n}\chi(d)d\,q^n,$$

$$s_{2,\chi} = \sum_{n\geq 1}\sum_{d|n}\chi\left(\frac{n}{d}\right)d\,q^n.$$

这两个形式构成 Eisenstein 空间 $\mathcal{E}_2(\Gamma_1(p),\chi)$ 的一组基. 注意 $s_{2,\chi}$ 是一个半尖形式.

对 $\mathbb{F}_p^\times$ 上面非平凡的奇特征 χ, 我们有如下的 weight-1 type-χ 的 Eisenstein 级数

$$G_{1,\chi} = \frac{L(0,\chi)}{2} + \sum_{n\geq 1}\sum_{d|n}\chi(d)q^n.$$

以上三个形式的系数定义在 $\mathbb{Q}(\zeta_{p-1})$ 上. 令 $\mathfrak{p}$ 为 $\mathbb{Q}(\zeta_{p-1})$ 中 above p 的任一非分歧素理想. 可以证明上述 Eisenstein 形式的系数都是 $\mathfrak{p}$-整的.

对于平凡特征 $\chi = 1$, 我们有 $\mathcal{M}_k(\Gamma_0(p)) = \mathcal{M}_k(p,1)$ 中的 Eisenstein 级数

$$G_k = -\frac{B_k}{2k} + \sum_{n\geq 1}\sum_{d|n} d^{k-1}q^n, \quad k\geq 4.$$

Lemma 4.1 (Hensel) 设 R 关于理想 I 完备, $f(x)\in R[x]$.

1. 若存在 $a\in R$ 使得 $f(a)\equiv 0 \pmod I$ 且 $f'(a)\in R^\times \pmod I$, 则存在唯一 $b\in R$ 使得 $b\equiv a \pmod I$ 且 $f(b)=0$.
2. 更一般地, 若 $f(a)\equiv 0 \pmod{f'(a)^2 I}$, 则存在 $b\in R$ 使得 $b\equiv a \pmod{f'(a)I}$ 且 $f(b)=0$. 若 $f'(a)$ 可逆, 则这样的 b 唯一.

Lemma 4.2 对 $(n,p)=1$, 我们有 $\omega(n)\equiv n^p \pmod{\mathfrak{p}^2}$, 这里 $\mathfrak{p}\in\Sigma_{\mathbb{Q}(\zeta_{p-1})}$ above p 如上所述.

Proof. 在 $\mathbb{Q}(\zeta_{p-1})$ 中, p 完全分裂. 因此 $\mathbb{Q}(\zeta_{p-1})_{\mathfrak{p}}\cong\mathbb{Q}_p$, 且 $\mathfrak{p}$ 在局部环中由 p 生成. Teichmüller 值 $\omega(n)$ 是满足

$$x^{p-1}=1, \quad x\equiv n \pmod{\mathfrak{p}}$$

的唯一根.

令 $u=n^p$. 因为 $(n,p)=1$, 由 Fermat 小定理 $n^{p-1}=1+pt, t\in\mathbb{Z}_p$. 于是

$$u^{p-1} = n^{p(p-1)} = (1+pt)^p \equiv 1 \pmod{p^2}.$$

同时 $u\equiv n \pmod p$. 现在我们可以对 $f(x)=x^{p-1}-1$ 应用 Hensel 提升 **Lem** 4.1.

更精确地, 因为 $f(u)\in p^2\mathbb{Z}_p$ 且 $f'(u)=(p-1)u^{p-2}\in\mathbb{Z}_p^\times$, Newton 迭代中第一步以及之后每一步的修正项都属于 $p^2\mathbb{Z}_p$. 因此得到的精确根 b 满足 $b\equiv u \pmod{\mathfrak{p}^2}$. 由于 $b\equiv n \pmod{\mathfrak{p}}$, 由

Teichmüller 根的唯一性知 $b=\omega(n)$. 因此

$$\omega(n)\equiv n^p \pmod{\mathfrak{p}^2}.$$

□

现在我们来具体阐述 Ribet 对于一个 weight-2 level-p 的特征尖形式的构造, 它满足某些很好的性质. 我们取 $k\in[2,p-3]$ 为偶数, $\mathfrak{p}\in\Sigma_{\mathbb{Q}(\zeta_{p-1})}$ above p 如上所述.

Lemma 4.3 记 $\chi=\omega^{k-2}$, 那么 $G_{2,\chi}$ 和 $G_{1,\omega^{k-1}}$ 的 Fourier 系数在 $\mathbb{Q}(\zeta_{p-1})$ 中是 $\mathfrak{p}$-整的, 并且

$$G_{2,\chi}\equiv G_{1,\omega^{k-1}}\equiv G_k \pmod{\mathfrak{p}}.$$

Proof. 由 Teichmüller 特征定义, $\omega(a)\equiv a \pmod{\mathfrak{p}}$, 因此 $\chi(d)d\equiv\omega^{k-1}(d)\equiv d^{k-1} \pmod{\mathfrak{p}}$.

现在只需考虑常数项. 由 **Lem** 1.2, 有

$$L(0,\chi)=-B_{1,\chi},\quad L(-1,\chi)=-\frac{1}{2}B_{2,\chi}.$$

由 **Lem** 4.2, $\omega(a)\equiv a^p \pmod{\mathfrak{p}^2}$. 注意到正交关系 $\sum_{a=1}^{p-1}\chi(a)=0$, 那么

$$\begin{aligned}pL(0,\omega^{k-1})&=-\sum_{a=1}^{p-1}\omega^{k-1}(a)\left(a-\frac{p}{2}\right)\\&\equiv-\sum_{a=1}^{p-1}a^{(k-1)p+1}+\frac{p}{2}\sum_{a=1}^{p-1}\omega^{k-1}(a)=-\sum_{a=1}^{p-1}a^{(k-1)p+1}\pmod{\mathfrak{p}^2}.\end{aligned}$$

注意到对偶整数 t, **Lem** 1.5 给出

$$L(0,\omega^{k-1})\equiv-\frac{1}{p}\sum_{a=1}^{p-1}a^{(k-1)p+1}\equiv-B_{1+p(k-1)}\pmod{\mathfrak{p}}.$$

由于 $1+p(k-1)\equiv k \pmod{p-1}$ 且 $1+p(k-1)\equiv 1 \pmod{p}$, **Prop** 1.6 给出

$$B_{1+p(k-1)}\equiv(1+p(k-1))\frac{B_k}{k}\equiv\frac{B_k}{k}\pmod{\mathfrak{p}}.$$

因此

$$L(0,\omega^{k-1})\equiv-\frac{B_k}{k}\pmod{\mathfrak{p}}.$$

同理, 对 $\chi=\omega^{k-2}$ 有

$$2pL(-1,\chi)\equiv-\sum_{a=1}^{p-1}a^{2+p(k-2)}\equiv-pB_{2+p(k-2)}\pmod{\mathfrak{p}^2}.$$

又 $2+p(k-2)\equiv k \pmod{p-1}$ 且 $2+p(k-2)\equiv 2 \pmod{p}$, 所以

$$B_{2+p(k-2)} \equiv 2\frac{B_k}{k} \pmod{\mathfrak{p}}.$$

于是

$$L(-1,\chi) \equiv -\frac{B_k}{k} \equiv L(0,\omega^{k-1}) \pmod{\mathfrak{p}}.$$

□

Remark. 这指的是形式 Fourier 展开的每一对应系数模 $\mathfrak{p}$ 相等, 尽管这三个 Eisenstein 级数的 weight 不同, 但这种比较依然合法.

Lemma 4.4 存在 $g \in \mathcal{M}_2(p,\chi)$, 其 Fourier 系数在 $\mathbb{Q}(\zeta_{p-1})$ 上 $\mathfrak{p}$-整且常数项是 $\mathfrak{p}$-单位.

Proof. 若 $p \nmid B_k$, 则 $G_{2,\chi}$ 满足题意. 事实上, 由上一引理, $G_{2,\chi}$ 的 Fourier 系数是 $\mathfrak{p}$-整的, 且其常数项模 $\mathfrak{p}$ 同余于 $-B_k/k$, 因而是 $\mathfrak{p}$-单位.

若 $p \mid B_k$, 且存在正偶数 $n+m\equiv k \pmod{p-1}$, $n,m\in[2,p-3]$, 使得 $p\nmid B_nB_m$, 那么

$$G_{1,\omega^{n-1}} \cdot G_{1,\omega^{m-1}}$$

满足题意. 这是 weight-2 的模形式, 其 type 为 $\omega^{n-1}\omega^{m-1}=\omega^{k-2}=\chi$. 又由 **Lem** 4.3 及 **Prop** 1.6, 两个因子的常数项分别模 $\mathfrak{p}$ 同余于 $-B_n/n$ 和 $-B_m/m$, 因此乘积的常数项是 $\mathfrak{p}$-单位.

若 $p \mid B_k$, 且任意正偶数 $n+m\equiv k \pmod{p-1}$, $n,m\in[2,p-3]$, 都有 $p\mid B_n$ 或 $p\mid B_m$: 记

$$S = \{n\in[2,p-3], 2|n \,|\, p \mid B_n\}.$$

令

$$E = \{0,2,4,\cdots,p-3\}.$$

这里把 0 加入 E 只是为了使 $n\mapsto k-n \pmod{p-1}$ 在 E 上封闭; 0 并不属于 S. 对 $n\in E$, 令 $\iota(n)$ 是 $k-n$ 在 E 中的代表元. 则 ι 是 E 上的配对. 若 $n,\iota(n)$ 都非零, 由本段假设, 轨道 $\{n,\iota(n)\}$ 至少有一个元素属于 S. 唯一含 0 的轨道是 $\{0,k\}$, 而现在 $p\mid B_k$, 所以 $k\in S$, 这个轨道也与 S 相交. 因此 ι 的每个轨道都与 S 相交. 由于每个轨道大小至多为 2, 有

$$|S| \geq |E/\iota| \geq \frac{|E|}{2} = \frac{p-1}{4}.$$

另一方面, Kummer 的相对类数公式给出, 见例如 [Was12, Chapter 4],

$$\mathrm{ord}_p(h_p^-) = \sum_{\substack{2\leq r\leq p-3\\ 2|r}} \mathrm{ord}_p\left(\frac{B_r}{r}\right).$$

由于 r 均为 p-单位, 上式推出 $p^{|S|}|h_p^-$. 但是 Carlitz–Olson 的结果 [CO55] 给出 $h_p^- < p^{(p-1)/4}$, 从而 $|S|<(p-1)/4$, 矛盾. 因此这种情况不可能发生. □

Cusp Forms

以下 Deligne–Serre [DS74] 的观察是很重要的:

Thm 4.1 (Deligne–Serre) 取 DVR $(R, \mathfrak{m}, \kappa)$, M 是 R 上的有限秩自由模, $K = \operatorname{Frac} R$. 设 S 是 (不必有限的) M 上交换的 R-自同态集.

设 $f \in M$ 在 $M/\mathfrak{m}M$ 中的像非零, 且是模 $\mathfrak{m}M$ 下所有算子 $T \in S$ 的特征向量, 即对每个 $T \in S$, 存在 $a_T \in R$ 使得

$$Tf \equiv a_T f \pmod{\mathfrak{m}M}.$$

则存在一个包含 R 的 DVR R', 其极大理想 $\mathfrak{m}'$ 包含 $\mathfrak{m}$, 分式域 K' 是 K 的有限扩张, 以及一个非零向量 $f' \in R' \otimes_R M$, 使得对每个 $T \in S$ 有 $Tf' = a'_T f'$, 且特征值 $a'_T \in R'$ 满足

$$a'_T \equiv a_T \pmod{\mathfrak{m}'}.$$

Proof. 令 $\mathbb{T}$ 为 S 在 $\operatorname{End}_R(M)$ 中生成的 R-代数. 因为 M 是有限秩自由 R-模, $\operatorname{End}_R(M)$ 也是有限秩自由 R-模, 从而 $\mathbb{T}$ 作为 R-子模是有限生成的. 特别地, $\mathbb{T}$ 是 Noether 环, 且作为 DVR 上的有限无挠模, $\mathbb{T}$ 是有限自由 R-模.

将 f 在 $M/\mathfrak{m}M$ 中的像记作 $\bar{f}$. 由假设, 对每个 $T \in S$ 有 $T\bar{f} = \bar{a}_T \bar{f}$. 因为 S 中算子两两交换, 这个关系唯一地延拓为一个 R-代数同态

$$\lambda : \mathbb{T} \longrightarrow \kappa, \quad T \longmapsto \bar{a}_T,$$

使得 $T\bar{f} = \lambda(T)\bar{f}$ 对所有 $T \in \mathbb{T}$ 成立. 于是 $\kappa_\lambda = \mathbb{T}/\ker\lambda$ 作为 $\mathbb{T}$-模嵌入 $M/\mathfrak{m}M$, $1 \mapsto \bar{f}$. 因此 $\ker\lambda$ 属于 $\operatorname{Supp}_{\mathbb{T}}(M/\mathfrak{m}M)$.

由 Nakayama 引理, $\ker\lambda$ 也属于 $\operatorname{Supp}_{\mathbb{T}}(M)$. 在局部环 $\mathbb{T}_{\ker\lambda}$ 的 $\operatorname{Supp}(M_{\ker\lambda})$ 中取一个极小素理想, 并记其在 $\mathbb{T}$ 中的收缩为 $\mathfrak{p}$. 于是 $\mathfrak{p} \subset \ker\lambda$, 且 $\mathfrak{p}\mathbb{T}_{\ker\lambda}$ 是 $M_{\ker\lambda}$ 的伴随素理想. 若 $\mathfrak{m} \subset \mathfrak{p}$, 则素元会成为 $M_{\ker\lambda}$ 的零因子; 但 M 是自由 R-模, 矛盾. 因此 $\mathfrak{p} \cap R = (0)$.

于是 $\mathbb{T}/\mathfrak{p}$ 是 R 上有限整的整环. 记其分式域为 K', 并取 R' 为 K' 中延拓 R 的一个离散赋值环, 极大理想记为 $\mathfrak{m}'$. 则 R' 包含 R, $\mathfrak{m}' \cap R = \mathfrak{m}$, 且 K'/K 是有限扩张.

商映射给出

$$\lambda' : \mathbb{T} \longrightarrow \mathbb{T}/\mathfrak{p} \hookrightarrow R', \quad T \longmapsto a'_T.$$

由于 $\mathfrak{p} \subseteq \ker\lambda$, 对 $T \in S$ 有

$$a'_T = \lambda'(T) \equiv \lambda(T) = a_T \pmod{\mathfrak{m}'}.$$

现在证明对应的特征向量存在. 令

$$\mathfrak{P} = \ker\left(K' \otimes_R \mathbb{T} \longrightarrow K'\right)$$

为 λ' 在 generic fiber 上的核. 由于 $\mathfrak{p} \in \mathrm{Supp}_{\mathbb{T}}(M)$ 且 $\mathfrak{p} \cap R = (0)$, 基变换到 K' 后, $\mathfrak{P}$ 属于

$$\mathrm{Supp}_{K' \otimes_R \mathbb{T}}(K' \otimes_R M).$$

另一方面 $K' \otimes_R \mathbb{T}$ 是 Artin 环, 所以其支集中的素理想都是 associated prime. 因此存在 $0 \neq f'' \in K' \otimes_R M$ 使得 $\mathfrak{P} f'' = 0$.

于是对每个 $T \in S$,

$$(T - a'_T) f'' = 0.$$

将 f'' 乘以 $K'^{\times}$ 中合适的元素, 可令它落在 $R' \otimes_R M$ 中且仍非零. 记所得向量为 f', 就得到 $Tf' = a'_T f'$ 和所需同余. □

Prop 4.5 设 $k \in [2, p-3]$ 为偶数, $p | B_k$, 则存在正规尖特征形式 $f = \sum_{n>0} a_n q^n \in \mathcal{S}_2(p, \chi)$ 和数域 K_f 中 above p 的素理想 $\mathfrak{p}$, 使得对所有素数 $\ell \neq p$, a_ℓ 是 $\mathfrak{p}$-整的, 且

$$a_\ell \equiv 1 + \ell^{k-1} \equiv 1 + \chi(\ell)\ell \pmod{\mathfrak{p}}.$$

Proof. Step1. 先构造一个半尖形式, 它模 $\mathfrak{p}$ 是所有 $(n, p) = 1$ 的 Hecke 算子的共同特征向量.

取满足 **Lem** 4.4 条件的 g, 并记 $a_0(g)$ 为 g 的常数项. 令

$$c = \frac{L(-1, \chi)}{2}, \quad \alpha = \frac{c}{a_0(g)}, \quad f_0 \coloneqq G_{2,\chi} - \alpha g.$$

由 **Lem** 4.4, $a_0(g)$ 是 $\mathfrak{p}$-单位. 又由 $p | B_k$ 和前面对常数项的同余计算, $c \equiv 0 \pmod{\mathfrak{p}}$. 因此 $\alpha \equiv 0 \pmod{\mathfrak{p}}$, 且 f_0 的常数项为 0. 换言之, f_0 是半尖形式, 并且

$$f_0 \equiv G_{2,\chi} \pmod{\mathfrak{p}}.$$

特别地, $f_0 \bmod \mathfrak{p}$ 非零, 因为 $G_{2,\chi}$ 的 q-系数为 1. 于是对每个素数 $\ell \neq p$,

$$T_\ell f_0 \equiv T_\ell G_{2,\chi} = (1 + \chi(\ell)\ell) G_{2,\chi} \equiv (1 + \chi(\ell)\ell) f_0 \pmod{\mathfrak{p}}.$$

由 Hecke 算子的乘法关系, 同样的同余对所有 $(n, p) = 1$ 的 T_n 成立.

Step2. 应用 Deligne–Serre 提升.

取一个包含 $G_{2,\chi}, g$ 的有限扩张 $K/\mathbb{Q}(\zeta_{p-1})$, 并令 R 为其整数环在 $\mathfrak{p}$ 上方某个素理想处的局部化. 令 M 为 weight-2, level-p, type-χ 的半尖形式中由一组 q-展开系数在 R 中的基生成的自由 R-模. 令

$$S = \{T_n \mid (n, p) = 1\}.$$

由于 q-展开原理, 上一步说明 f_0 在 $M/\mathfrak{m}M$ 中的像是非零的 S-共同特征向量. 由 **Thm** 4.1, 在有限扩张后存在非零半尖形式 f' 和特征值 λ_n 使得

$$T_n f' = \lambda_n f', \quad \lambda_\ell \equiv 1 + \chi(\ell)\ell \pmod{\mathfrak{p}}$$

对所有 $(n,p)=1$ 成立, 特别地对所有素数 $\ell \neq p$ 成立.

Step3. 证明 f' 实际上是尖形式, 并归一化为 newform.

半尖空间有分解

$$\mathcal{S}_2'(p,\chi) = \mathcal{S}_2(p,\chi) \oplus \mathbb{C}s_{2,\chi}.$$

写 $f' = h + as_{2,\chi}$, 其中 $h \in \mathcal{S}_2(p,\chi)$. 若 $a \neq 0$, 对 $\ell \neq p$ 比较 $T_\ell f' = \lambda_\ell f'$ 在 Eisenstein 分量上的投影, 得

$$\lambda_\ell = \ell + \chi(\ell).$$

结合上面的同余, 得

$$\ell + \chi(\ell) \equiv 1 + \chi(\ell)\ell \pmod{\mathfrak{p}},$$

即 $(\ell-1)(1-\chi(\ell)) \equiv 0 \pmod{\mathfrak{p}}$. 对每个 $u \in \mathbb{F}_p^\times$, $u \neq 1$, 由 Dirichlet 定理可取素数 $\ell \neq p$ 使得 $\ell \equiv u \pmod{p}$. 因而 $\chi(u) = 1$. 又 $\chi(1) = 1$, 这迫使 χ 平凡. 但这里 $\chi = \omega^{k-2}$ 非平凡, 因为 $p | B_k$ 时不可能有 $k = 2$. 矛盾. 因此 $a = 0$, 即 f' 是尖形式.

最后, level 为 p 的 weight-2 oldform 只能来自更低 level. 若考虑带 Nebentypus χ 的空间, 更低 level 必要求 χ 的导子也除以更低 level; 这里 $\chi = \omega^{k-2}$ 非平凡且导子为 p, 因而没有 oldform. 等价地, 在平凡角色的 level-1 情形也有 $S_2(\mathrm{SL}_2(\mathbb{Z})) = 0$. 所以 f' 属于 p-new 子空间.

由 newform 理论中的强重数一, p-new 子空间中由所有 T_n, $(n,p)=1$, 给出的共同特征系统确定一条 newform 直线. 因此 f' 是某个正规 newform 的标量倍, 从而自动也是所有 Hecke 算子的共同特征向量. 将 f' 乘以常数归一化, 得到正规尖特征形式

$$f = \sum_{n>0} a_n q^n \in \mathcal{S}_2(p,\chi).$$

取 $\mathfrak{p}$ 为其系数域中由上面 DVR 给出的素理想的限制. 因为 λ_ℓ 在该 DVR 中 $\mathfrak{p}$-整, 归一化后对所有素数 $\ell \neq p$ 有

$$a_\ell = \lambda_\ell \equiv 1 + \chi(\ell)\ell \equiv 1 + \ell^{k-1} \pmod{\mathfrak{p}}.$$

□

5 Galois Side

现在取特征 0 的局部域 $K/\mathbb{Q}_p$, 其极大理想 $\mathfrak{m}$, 剩余域 κ. 取一个 profinite 群上的 2 维连续表示 $\rho : G \to \mathrm{GL}(V)$, 那么存在一个 G-稳定的 $\mathcal{O}_K$-格 $\Lambda \subset V$. 于是 Λ 诱导一个

$$\rho_\Lambda : G \to \mathrm{GL}(\Lambda) \to \mathrm{GL}(\Lambda/\mathfrak{m}\Lambda),$$

称作 ρ 在 Λ 上的约化. mod$p$ 的表示的基础理论告诉我们有

Thm 5.1 (Brauer–Nesbitt) ρ_Λ 的半单化 $\bar{\rho}$ 只依赖于 ρ, 不依赖于 Λ 的选取.

半单化指的是其所有 Jordan-Hölder 因子的直和 $M^{\mathrm{ss}} = \bigoplus_{i=0}^{n-1} (M_{i+1}/M_i)$. 现在假定 $\bar{\rho}$ 可约, 即有两个特征标 $\varphi_i : G \to \kappa^\times$ 使得 $\bar{\rho} \sim \varphi_1 \oplus \varphi_2$.

对一个给定的 Λ, ρ_Λ 同构于

$$\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}, \quad \begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix} \tag{1}$$

之一, 且若 $\rho_\Lambda(G)$ 的阶与 p 互素, 则 ρ_Λ 是半单的. 现在我们需要著名的

Lemma 5.1 (Ribet) 取二维不可约表示 $\rho : G \to \mathrm{GL}(V)$, 但是 $\bar{\rho} \sim \varphi_1 \oplus \varphi_2$ 可约, 且 $\varphi_1 \neq \varphi_2$. **(Eq 1)** 中的两个标准型都可以通过合适的 Λ 实现; 即存在 Λ 使得 ρ_Λ 是非半单的, 且可以事先指定为上述任一类型.

Proof. 设 $\mathcal{O} = \mathcal{O}_K$, 其素元为 ϖ. 我们先证明: 对给定顺序 (φ_1, φ_2), 存在一个 G-稳定格, 使得约化为上三角型

$$\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$$

且非半单.

取一个 G-稳定 $\mathcal{O}$-格 Λ_0 且固定一个 $\mathcal{O}$-基, 将 ρ 视为 $G \to \mathrm{GL}(2, \mathcal{O})$. 经过模 ϖ 的换基, 可设约化的半单化为 $\varphi_1 \oplus \varphi_2$. 若约化已经是非半单的上三角型, 则已经完成. 若它是下三角型, 即

$$\rho_{\Lambda_0} \sim \begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix},$$

则令

$$P = \begin{pmatrix} 1 & 0 \\ 0 & \varpi \end{pmatrix}, \quad P \begin{pmatrix} a & \varpi b \\ c & d \end{pmatrix} P^{-1} = \begin{pmatrix} a & b \\ \varpi c & d \end{pmatrix},$$

用格 $P\Lambda_0$ 代替 Λ_0 后, 约化就变为所需的上三角型. 因此以下可假设

$$\rho(G) \subset \begin{pmatrix} \mathcal{O}^\times & \mathcal{O} \\ \varpi\mathcal{O} & \mathcal{O}^\times \end{pmatrix}, \quad \rho_{\Lambda_0} \sim \begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}.$$

现在设所有这种上三角型约化都是半单的, 然后反证. 我们递归构造

$$M_i = \begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathcal{O})$$

使得

$$M_i \rho(G) M_i^{-1} \subset \begin{pmatrix} \mathcal{O}^\times & \varpi^i\mathcal{O} \\ \varpi\mathcal{O} & \mathcal{O}^\times \end{pmatrix}.$$

对 $i = 0$, 取 $M_0 = I_2$. 假设 M_i 已构造. 于是

$$P^i M_i \rho(g) M_i^{-1} P^{-i} \in \begin{pmatrix} \mathcal{O}^\times & \mathcal{O} \\ \varpi^{i+1}\mathcal{O} & \mathcal{O}^\times \end{pmatrix}.$$

于是 B_i 的约化仍是所需的上三角型. 由反设, 这个约化是半单的, 故存在

$$U_i = \begin{pmatrix} 1 & u_i \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathcal{O})$$

使得 $U_i P^i M_i \rho(g) M_i^{-1} P^{-i} U_i^{-1}$ 的右上角对所有 g 都属于 $\varpi\mathcal{O}$. 同时, 上三角幺幂矩阵共轭不改变左下角项, 因而

$$U_i P^i M_i \rho(G) M_i^{-1} P^{-i} U_i^{-1} \subset \begin{pmatrix} \mathcal{O}^\times & \varpi\mathcal{O} \\ \varpi^{i+1}\mathcal{O} & \mathcal{O}^\times \end{pmatrix}.$$

定义

$$M_{i+1} = P^{-i} U_i P^i M_i = \begin{pmatrix} 1 & t_i + u_i \varpi^i \\ 0 & 1 \end{pmatrix}.$$

则

$$M_{i+1} \rho(G) M_{i+1}^{-1} = P^{-i} U_i P^i M_i \rho(G) M_i^{-1} P^{-i} U_i^{-1} P^i \subset \begin{pmatrix} \mathcal{O}^\times & \varpi^{i+1}\mathcal{O} \\ \varpi\mathcal{O} & \mathcal{O}^\times \end{pmatrix}.$$

递归构造完成.

因为 $t_{i+1} = t_i + u_i \varpi^i$, 序列 (M_i) 在 $\mathrm{GL}(2, \mathcal{O})$ 中收敛到某个

$$M = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \lim_{n\to\infty} M_n \in \mathrm{GL}(2, \mathcal{O}).$$

对任意 $g \in G$, 矩阵 $M_i \rho(g) M_i^{-1}$ 的右上角属于 $\varpi^i\mathcal{O}$. 令 $i \to \infty$, 得到

$$M \rho(G) M^{-1} \subset \begin{pmatrix} \mathcal{O}^\times & \bigcap_{i\geq 0} \varpi^i\mathcal{O} \\ \varpi\mathcal{O} & \mathcal{O}^\times \end{pmatrix} = \begin{pmatrix} \mathcal{O}^\times & 0 \\ \varpi\mathcal{O} & \mathcal{O}^\times \end{pmatrix}.$$

这说明 K-直线 $\begin{pmatrix} 0 \\ 1 \end{pmatrix} K$ 被 G 稳定, 与 ρ 不可约矛盾. 所以至少存在一个上三角型约化非半单.

将上述论证应用于顺序 (φ_2, φ_1), 再交换两个基向量, 即得到

$$\begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix}$$

型的非半单约化. 因此 **(Eq 1)** 中的两个标准型都可以实现. □

Remark. Joël Bellaïche 用一个更新的, 更几何的方法证明了 Ribet 引理, 使用了 Bruhat–Tits tree.

Thm 5.2 设 $f \in \mathcal{S}_2(N, \chi)$ 是一个正规化特征形式, 其数域为 K_f. 设 ℓ 是一个素数. 对 $\mathcal{O}_{K_f}$ 中每个 above ℓ 的极大理想 $\mathfrak{m}$, 存在一个二维 Galois 表示

$$\rho_{f,\mathfrak{m}} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(2, K_{f,\mathfrak{m}}),$$

该表示在每个满足 $p \nmid \ell N$ 的素数 p 处非分歧. 对任意这样的 p, 取 $\mathfrak{p} \subset \mathbb{Z}$ 为 above p 的极大理想, 则 $\rho_{f,\mathfrak{m}}(\mathrm{Frob}_{\mathfrak{p}})$ 满足多项式方程

$$x^2 - a_p(f)x + \chi(p)p = 0.$$

特别地, 若 $f \in \mathcal{S}_2(\Gamma_0(N))$, 则关系为 $x^2 - a_p(f)x + p = 0$.

Proof. [DS05, Thm 9.5.4] □

于是我们现在利用 **Prop** 4.5 中的特征形式 f, 令 $k \in [2, p-3]$ 为偶数, $p | B_k$, 取 $\chi = \omega^{k-2}$. 记

$$\rho_{f,\mathfrak{p}} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(2, V_{f,\mathfrak{p}})$$

是 f 在 $\mathfrak{p}$ 处的相伴表示. 记 $\chi_{\mathrm{cyc}} : \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ 是分圆特征, 由 **Thm** 5.2,

$$\mathrm{tr}(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)) = a_\ell(f), \quad \det(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)) = \chi(\ell)\ell.$$

注意这里的 p, ℓ 和定理中的 p, ℓ 是相反的. 下面解释这里所用的 Chebotarev 密度定理及其拓扑含义.

Def 5.1 设 F 是数域, S 是 F 的非零素理想集合. 若极限

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{q} \in S} N\mathfrak{q}^{-s}}{\sum_{\mathfrak{q}} N\mathfrak{q}^{-s}}$$

存在, 则称 $\delta(S)$ 为 S 的 Dirichlet 密度. 这里分母对 F 的所有非零素理想求和.

Thm 5.3 (Chebotarev) 设 L/F 是有限 Galois 扩张, $C \subset \mathrm{Gal}(L/F)$ 是一个共轭类. 那么在 F 中非分歧素理想 $\mathfrak{q}$ 中, 满足

$$\mathrm{Frob}_{\mathfrak{q}} \in C$$

的素理想集合具有 Dirichlet 密度 $\#C/\#\mathrm{Gal}(L/F)$. 特别地, 每个共轭类中都有无穷多个 Frobenius 元.

Def 5.2 绝对 Galois 群 $\mathrm{Gal}_{\mathbb{Q}}$ 上的 Krull 拓扑定义如下: 对有限 Galois 扩张 $L/\mathbb{Q}$, 限制映射给出有限商

$$\mathrm{Gal}_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(L/\mathbb{Q}).$$

在 $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$ 附近的一组开邻域基由

$$\sigma\,\mathrm{Gal}(\overline{\mathbb{Q}}/L) = \{\tau \in \mathrm{Gal}_{\mathbb{Q}} \mid \tau|_L = \sigma|_L\}$$

给出. 换言之, $\mathrm{Gal}_{\mathbb{Q}} = \varprojlim_L \mathrm{Gal}(L/\mathbb{Q})$, 并赋予逆极限拓扑.

因此, 一个子集 $D \subset \mathrm{Gal}_{\mathbb{Q}}$ 稠密, 当且仅当对每个有限 Galois 扩张 $L/\mathbb{Q}$, 它在有限商 $\mathrm{Gal}(L/\mathbb{Q})$ 中的像等于整个 $\mathrm{Gal}(L/\mathbb{Q})$. 事实上, 若某个有限商中少了一个元素 σ, 那么 $\sigma\,\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ 是一个与 D 不相交的非空开集; 反过来, 每个非空开集都包含某个这样的有限层 cylinder.

现在来看 Frobenius 元. 严格地说, 对素数 ℓ 和有限 Galois 扩张 $L/\mathbb{Q}$, Frob_ℓ 在 $\mathrm{Gal}(L/\mathbb{Q})$ 中只

在共轭意义下由 ℓ 决定; 选择 L 中位于 ℓ 上方的素理想会在同一个共轭类中改变 Frobenius 代表. 由 **Thm** 5.3, 对任意 $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, 存在无穷多个不分歧素数 ℓ 使得某个 Frobenius 代表等于 σ. 避开有限多个分歧素数以及 $\ell = p$, 仍可做到这一点. 因此所有 Frobenius 代表构成的集合

$$\{\mathrm{Frob}_\ell \mid \ell \neq p\}$$

在 Krull 拓扑中稠密. 对本文当前用途, 我们只把 Frobenius 元代入连续特征, 其值不依赖于共轭代表. 所以可以直接说 Frob_ℓ 在 $\mathrm{Gal}_\mathbb{Q}$ 中稠密. 于是两个连续特征 $\det(\rho_{f,\mathfrak{p}})$, $\chi_{\mathrm{cyc}} \circ \chi$ 在稠密集上相等, 它们本身也相等.

Lemma 5.2 *$\rho_{f,\mathfrak{p}}$ 是绝对不可约表示.*

Proof. 反设 $\rho_{f,\mathfrak{p}}$ 可约. 那么取半单化后可写为两个连续特征

$$\rho_{f,\mathfrak{p}}^{\mathrm{ss}} = \chi_1 \oplus \chi_2.$$

它们在 p 外非分歧, 且

$$\chi_1\chi_2 = \det \rho_{f,\mathfrak{p}} = \chi\chi_{\mathrm{cyc}}.$$

这里不能对任意连续 p-adic 特征直接作这样的分类; 我们使用的是 Serre 对来自 weight-2 特征形式的 p-adic Galois 表示的一维子商的描述 [Ser97, Chapter III, Page III-1]. 具体地, 存在整数 n_1, n_2 和有限阶特征 η_1, η_2, 使得

$$\chi_i = \eta_i \chi_{\mathrm{cyc}}^{n_i}, \quad n_1 + n_2 = 1.$$

因此可假设 $n_1 \geq 1$ 且 $n_2 \leq 0$. 对任意充分大的素数 $\ell \neq p$, 有

$$a_\ell(f) = \chi_1(\mathrm{Frob}_\ell) + \chi_2(\mathrm{Frob}_\ell) = \eta_1(\ell)\ell^{n_1} + \eta_2(\ell)\ell^{n_2}.$$

取复嵌入后, $\eta_i(\ell)$ 都是单位根, 因而

$$|a_\ell(f)| \geq |\eta_1(\ell)\ell^{n_1}| - |\eta_2(\ell)\ell^{n_2}| = \ell^{n_1} - \ell^{n_2} \geq \ell - 1.$$

这与 weight-2 尖形式的 Ramanujan–Petersson 估计 (或者说, 与 Weil 猜想)

$$|a_\ell(f)| \leq 2\sqrt{\ell}$$

矛盾. 故 $\rho_{f,\mathfrak{p}}$ 不可约. □

Lemma 5.3 *存在一个 $\mathrm{Gal}_\mathbb{Q}$ 稳定的 $\mathcal{O}_{f,\mathfrak{p}}$-格 $\Lambda \subset V_{f,\mathfrak{p}}$, 使得约化*

$$\rho_{f,\mathfrak{p},\Lambda} \sim \begin{pmatrix} 1 & * \\ 0 & \omega^{k-1} \end{pmatrix}, \quad * \neq 0.$$

Proof. 由 **Prop** 4.5, 对所有 $\ell \neq p$ 有

$$\mathrm{tr}(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)) \equiv 1 + \omega^{k-1}(\ell) \pmod{\mathfrak{p}}, \quad \det(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)) \equiv \omega^{k-1}(\ell) \pmod{\mathfrak{p}}.$$

Chebotarev 密度定理和 Brauer–Nesbitt 定理给出

$$\bar{\rho}^{\mathrm{ss}}_{f,\mathfrak{p}} \cong 1 \oplus \omega^{k-1}.$$

这里 $1 \neq \omega^{k-1}$, 因为 $2 \leq k \leq p-3$. 由 **Lem** 5.2 和 **Lem** 5.1, 可取一个 $\mathrm{Gal}_{\mathbb{Q}}$-稳定格, 使得约化表示为上三角非半单型. 即得到所需结论. □

Thm 5.4 (Raynaud) 设 $E/\mathbb{Q}_p$ 是有限扩张, 其绝对分歧指数 $e(E/\mathbb{Q}_p) < p-1$, 整数环为 $\mathcal{O}_E$. 若 G/E 是被 p 的幂零化的有限平坦交换群概形, 则 G 到 $\mathcal{O}_E$ 上有限平坦交换群概形的延拓至多唯一.

这是 Raynaud 的有限平坦群概形唯一延拓定理. 我们只在下面使用其唯一性: 当一个 generic fiber 有一个显然的 finite flat model 时, 任意另一个 finite flat model 必与它相同.

Prop 5.4 令 $M = \Lambda/\mathfrak{p}\Lambda$, 它带有 $r = \rho_{f,\mathfrak{p},\Lambda}$ 给出的 $\mathrm{Gal}_{\mathbb{Q}}$-作用. 取 $L = \mathbb{Q}_p(\zeta_p)^+$, 并固定嵌入 $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, 记

$$D = \mathrm{Gal}(\overline{\mathbb{Q}}_p/L) \subset D_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p).$$

则 D-模 M 来自 $\mathcal{O}_L$ 上的一个有限平坦 p-初等交换群概形 $\mathcal{M}$.

Proof. 记 $\mathcal{O}_f$ 为 K_f 的整数环, $\mathcal{O}_{f,\mathfrak{p}}$ 为 K_f 在 $\mathfrak{p}$ 处的整数环. 由 Eichler–Shimura 构造, 特征形式 f 对应一个 $\mathbb{Q}$ 上的 Abel 簇 A_f, 且

$$K_f \subset \mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}.$$

我们需要把前面由 Ribet 引理选出的格 Λ 放进这个 Abel 簇的 torsion 中. 这是格与 p-power isogeny 的标准对应: 若 $T_{\mathfrak{p}}(A_f)$ 是 A_f 的 $\mathfrak{p}$-adic Tate module, 则 Λ 与 $T_{\mathfrak{p}}(A_f)$ 在 $V_{f,\mathfrak{p}}$ 中 commensurable. 将 Λ 乘以 $K_f^\times$ 中合适的元素不改变其模 $\mathfrak{p}$ 约化, 因而可设存在 n 使得

$$\mathfrak{p}^n T_{\mathfrak{p}}(A_f) \subset \Lambda \subset T_{\mathfrak{p}}(A_f).$$

有限商 $T_{\mathfrak{p}}(A_f)/\Lambda$ 给出 $A_f[\mathfrak{p}^n]$ 的一个 $\mathrm{Gal}_{\mathbb{Q}}$-稳定有限子群. 对 A_f 商去这个子群, 可得到一个 $\mathbb{Q}$ 上的 Abel 簇 A, 仍在 A_f 的 isogeny 类中, 且 $\mathcal{O}_f \subset \mathrm{End}(A)$, 其 $\mathfrak{p}$-adic Tate module 正是 Λ. 因而

$$A[\mathfrak{p}] \subset A[p]$$

的几何点给出与 $M = \Lambda/\mathfrak{p}\Lambda$ 同构的 D-模.

我们还使用 Ribet 证明中的另一个标准输入: 这个 level-p 的 modular Abelian variety 在

$$L = \mathbb{Q}_p(\zeta_p)^+$$

上有好约化. 这可由 $X_1(p)$ 的半稳定模型和 Néron–Ogg–Shafarevich 判别得到, 也是 Ribet 原文中

性质 (0.7) 的内容. 令 $\mathcal{A}/\mathcal{O}_L$ 为 A_L 的 Néron 模型. 因为 A 在 L 上有好约化, $\mathcal{A}$ 实际上是 Abel scheme. 乘以 p 的核

$$\mathcal{A}[p] \subset \mathcal{A}$$

是 $\mathcal{O}_L$ 上有限平坦交换群概形, 且其 generic fiber 是 $A[p]$. 取 $A[\mathfrak{p}]$ 在 $\mathcal{A}[p]$ 中的 schematic closure, 记为 $\mathcal{M}$. 有限平坦群概形中闭子群概形的 schematic closure 仍有限平坦, 因而 $\mathcal{M}/\mathcal{O}_L$ 是有限平坦 p-初等交换群概形. 它的 generic fiber 的几何点正是 M, 所以 M 来自 $\mathcal{M}$. □

Prop 5.5 上述表示 r 限制到 D_p 后半单. 因而 $p \nmid |\mathrm{im}(r|_{D_p})|$.

Proof. 因为

$$[D_p : D] = [L : \mathbb{Q}_p] = \frac{p-1}{2}$$

与 p 互素, 只需证明 M 作为 D-模半单. 事实上, 若 $M|_D$ 半单, 则对任一 D_p-稳定子空间, 可先在 D 上取补空间, 再对有限商 D_p/D 平均投影, 得到 D_p-稳定补空间.

由 **Lem** 5.2 和 **Lem** 5.1, 我们已经选取 Λ 使得

$$r \sim \begin{pmatrix} 1 & * \\ 0 & \omega^{k-1} \end{pmatrix}, \quad * \neq 0.$$

因此对 D 也有一个 D-稳定的 $\mathbb{F}$-直线 $X \subset M$, 使得 D 在 X 上平凡作用, 而在商

$$Y = M/X$$

上通过 ω^{k-1} 作用. 这里 $\mathbb{F} = \mathcal{O}_{f,\mathfrak{p}}/\mathfrak{p}$. 因为 $L = \mathbb{Q}_p(\zeta_p)^+$, 字符 $\omega|_D$ 的像为 $\{\pm 1\}$; 又 $k-1$ 为奇数, 故 $\omega^{k-1}|_D$ 是非平凡二次字符. 特别地, Y 是 ramified 的 D-模.

令 $\mathcal{X}$ 为 X 在 $\mathcal{M}$ 中的 schematic closure. 因为 $\mathcal{M}$ 有限平坦, $\mathcal{X}$ 作为闭子群概形也是 $\mathcal{O}_L$ 上有限平坦群概形. 又因为 X 是平凡 D-模, 其 generic fiber 有常值有限平坦模型 $X_{\mathcal{O}_L}$. 由 **Thm** 5.4, $\mathcal{X}$ 必等于这个常值模型, 因而 $\mathcal{X}$ 是 étale 群概形. 所以 $\mathcal{M}$ 不是连通的: 它含有非零的 étale 子群概形 $\mathcal{X}$.

另一方面, $\mathcal{M}$ 是 $\mathbb{F}$-向量群概形. 设 $\mathcal{M}^0$ 为 $\mathcal{M}$ 的最大连通闭子群概形, 并令 M^0 为其 generic fiber 的几何点构成的 D-子模. 则 M^0 是 M 的 $\mathbb{F}[D]$-子模. 商群概形 $\mathcal{M}/\mathcal{M}^0$ 是最大 étale 商, 因而 M/M^0 是 unramified 的 D-模.

我们有 $M^0 \neq M$, 因为 $\mathcal{M}$ 已经不是连通的. 同时 $M^0 \neq 0$: 否则 $\mathcal{M}$ 是 étale, 从而 M unramified, 这会推出其商 Y unramified, 与上面 Y ramified 矛盾. 因此 M^0 是二维 $\mathbb{F}$-空间 M 中的一条 D-稳定直线.

最后, $M^0 \neq X$. 若 $M^0 = X$, 则 $M/M^0 = Y$ 应当 unramified; 但 Y 是 ramified 的. 所以 X 和 M^0 是 M 中两条不同的 D-稳定直线. 于是

$$M = X \oplus M^0$$

作为 D-模分裂, 即 $M|_D$ 半单. 由第一段, $M|_{D_p}$ 也半单.

半单化的两个角色是 1 和 ω^{k-1}. 因此 D_p 在 M 上的作用通过 $1 \oplus \omega^{k-1}$, 其像是 $\mathbb{F}^\times$ 中的有限

子群, 阶数与 p 互素. 即 $p \nmid |\operatorname{im}(r|_{D_p})|$. □

Prop 5.6 $r := \rho_{f,\mathfrak{p},\Lambda}$ 满足 **Thm** 3.3 中的四条性质, 于是 **Thm** 3.1 成立.

Proof. 我们逐条验证 **Thm** 3.3. 首先, r 是 $\rho_{f,\mathfrak{p}}$ 沿 $\mathrm{Gal}_{\mathbb{Q}}$-稳定格 Λ 的约化. 因为 $\rho_{f,\mathfrak{p}}$ 在所有 $\ell \neq p$ 处非分歧, 其约化 r 也在所有 $\ell \neq p$ 处非分歧. 这给出条件 (1).

由 **Lem** 5.2 和 **Lem** 5.1 的选取,

$$r \sim \begin{pmatrix} 1 & \gamma \\ 0 & \omega^{k-1} \end{pmatrix}$$

且这个扩张非半单. 因而 γ 不是 coboundary, 特别不是零的上三角项. 这正是条件 (2).

条件 (3) 也由非半单性推出. 若 $p \nmid |\operatorname{im} r|$, 则有限群 $\operatorname{im} r$ 在特征 p 的表示完全可约, 于是 r 必半单, 与上面的非半单性矛盾. 因此 $p \mid |\operatorname{im} r|$.

最后, 条件 (4) 正是 **Prop** 5.5 的结论:

$$p \nmid |\operatorname{im}(r|_{D_p})|.$$

因此 r 满足 **Thm** 3.3 的四条性质. 由 **Thm** 3.3 $\Rightarrow$ **Thm** 3.2, 再由 **Thm** 3.2 $\Rightarrow$ **Thm** 3.1, 得到 **Thm** 3.1. □

6 Cohomological Reformulation

最后用更现代的 Galois 上同调语言重新表述上述结论. 仍令

$$K = \mathbb{Q}(\zeta_p), \quad \Delta = \mathrm{Gal}(K/\mathbb{Q}),$$

并重新令 L/K 为最大处处非分歧的 p-初等 Abel 扩张. 令 $\mathbb{F}_p(\omega^{1-k})$ 表示底层加法群为 $\mathbb{F}_p$, $\mathrm{Gal}_{\mathbb{Q}}$ 通过特征 ω^{1-k} 作用的一维表示.

Def 6.1 定义处处非分歧上同调群

$$H^1_{\mathrm{ur}}\left(\mathbb{Q}, \mathbb{F}_p(\omega^{1-k})\right) := \ker\left(H^1\left(\mathrm{Gal}_{\mathbb{Q}}, \mathbb{F}_p(\omega^{1-k})\right) \longrightarrow \prod_{\ell} H^1\left(I_\ell, \mathbb{F}_p(\omega^{1-k})\right)\right),$$

其中 I_ℓ 是 ℓ 处的惯性群. 换言之, 这里考虑的是在每个有限素数处都非分歧的上同调类.

Prop 6.1 有自然同构

$$H^1_{\mathrm{ur}}\left(\mathbb{Q}, \mathbb{F}_p(\omega^{1-k})\right) \cong \mathrm{Hom}_{\mathbb{F}_p[\Delta]}\left(A/pA, \mathbb{F}_p(\omega^{1-k})\right).$$

特别地,

$$H^1_{\mathrm{ur}}\left(\mathbb{Q}, \mathbb{F}_p(\omega^{1-k})\right) \neq 0 \iff A^{(1-k)} \neq 0.$$

Proof. 考虑正合列

$$1 \longrightarrow \mathrm{Gal}_K \longrightarrow \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \Delta \longrightarrow 1.$$

因为 $p\nmid|\Delta|$, 对任意 $\mathbb{F}_p[\Delta]$-模 N 都有

$$H^i(\Delta, N) = 0, \quad i > 0.$$

对 $N = \mathbb{F}_p(\omega^{1-k})$ 应用 inflation–restriction 正合列, 得到限制映射诱导的同构

$$H^1\left(\mathrm{Gal}_{\mathbb{Q}}, \mathbb{F}_p(\omega^{1-k})\right) \xrightarrow{\sim} H^1\left(\mathrm{Gal}_K, \mathbb{F}_p(\omega^{1-k})\right)^{\Delta}.$$

由于 $\omega|_{\mathrm{Gal}_K} = 1$, Gal_K 在系数模 $\mathbb{F}_p(\omega^{1-k})$ 上作用平凡. 因而右端可写成

$$\mathrm{Hom}_{\mathrm{cont}}\left(\mathrm{Gal}_K, \mathbb{F}_p(\omega^{1-k})\right)^{\Delta}.$$

处处非分歧条件恰好要求这个同态在 K 的每个惯性群上为零, 所以它通过 K 的最大处处非分歧 p-初等 Abel 扩张的 Galois 群分解. 由前面的 Artin 同构,

$$A/pA \xrightarrow{\sim} \mathrm{Gal}(L/K),$$

因此得到

$$H^1_{\mathrm{ur}}\left(\mathbb{Q}, \mathbb{F}_p(\omega^{1-k})\right) \cong \mathrm{Hom}_{\mathbb{F}_p[\Delta]}\left(A/pA, \mathbb{F}_p(\omega^{1-k})\right).$$

在 p 处也没有额外问题: $K/\mathbb{Q}$ 的惯性商包含在 Δ 中, 其阶与 p 互素, 所以 inflation–restriction 中来自该有限商的 H^1 消失. 因而在 $\mathbb{Q}$ 上局部非分歧和限制到 Gal_K 后通过处处非分歧类域分解给出同一个局部条件.

最后, $\mathbb{F}_p[\Delta]$ 是半单环, 且 $\mathbb{F}_p(\omega^{1-k})$ 是与幂等元 e_{1-k} 对应的一维表示. 所以

$$\mathrm{Hom}_{\mathbb{F}_p[\Delta]}\left(A/pA, \mathbb{F}_p(\omega^{1-k})\right) \neq 0 \iff (A/pA)^{(1-k)} \neq 0.$$

又有

$$(A/pA)^{(1-k)} \cong A^{(1-k)}/pA^{(1-k)},$$

故右端非零当且仅当 $A^{(1-k)} \neq 0$. □

现在解释这个上同调类与原证明中的矩阵表示及域扩张为何是同一个对象. 一个类

$$[c] \in H^1\left(\mathrm{Gal}_{\mathbb{Q}}, \mathbb{F}_p(\omega^{1-k})\right)$$

对应一个扩张

$$0 \longrightarrow \mathbb{F}_p \longrightarrow V_c \longrightarrow \mathbb{F}_p(\omega^{k-1}) \longrightarrow 0.$$

选取与这条正合列相容的基以后, 表示具有形式

$$\rho_c(\sigma) = \begin{pmatrix} 1 & \gamma(\sigma) \\ 0 & \omega^{k-1}(\sigma) \end{pmatrix}.$$

这里若采用通常的左 1-cocycle 约定, 则

$$c(\sigma) = \gamma(\sigma)\omega^{1-k}(\sigma).$$

扩张非分裂当且仅当 $[c] \neq 0$, 这正对应于原证明中上三角表示不是半单表示.

另一方面, 将 c 限制到 Gal_K 后, 系数作用变为平凡, 所以

$$c|_{\mathrm{Gal}_K} : \mathrm{Gal}_K \longrightarrow \mathbb{F}_p$$

是连续群同态. 若 $[c]$ 处处非分歧, 这个同态通过 A/pA 分解. 其核在 Δ 的共轭作用下稳定, 因此它在 $\mathrm{Gal}_{\mathbb{Q}}$ 中正规. 令 F 为其核在 $\overline{\mathbb{Q}}$ 中的固定域, 则 $F/\mathbb{Q}$ 是 Galois 扩张, F/K 处处非分歧, 且

$$H = \mathrm{Gal}(F/K) = \mathrm{im}\,(c|_{\mathrm{Gal}_K})$$

是非零 p-初等 Abel 群. c 的 Δ-等变性又给出

$$\sigma\tau\sigma^{-1} = \omega(\bar{\sigma})^{1-k}\tau,$$

这正是 **Thm** 3.2 的条件 (iii). 反过来, 从满足 **Thm** 3.2 的 F/K 出发, Artin 映射给出 $A/pA \twoheadrightarrow H$; 再取任一非零的 $\mathbb{F}_p[\Delta]$-线性映射

$$H \longrightarrow \mathbb{F}_p(\omega^{1-k}),$$

就得到一个非零的处处非分歧上同调类. 因此原文的类群特征分量, 非分歧域扩张, 非分裂上三角表示和现代语言中的

$$H^1_{\mathrm{ur}}\left(\mathbb{Q}, \mathbb{F}_p(\omega^{1-k})\right) \neq 0$$

是完全等价的四种表述.

参考文献

[CO55] Leonard Carlitz and Frank R Olson. Maillet's determinant. *Proceedings of the American Mathematical Society*, 6(2):265–269, 1955.

[DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. In *Annales scientifiques de l'École Normale Supérieure*, volume 7, pages 507–530, 1974.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[Her32] Jacques Herbrand. Sur les classes des corps circulaires. *Journal de Mathématiques Pures et Appliquées*, 11:417–441, 1932.

[Rib76] Kenneth A Ribet. A modular construction of unramified p-extensions of q (μ p). *Inventiones mathematicae*, 34(3):151–162, 1976.

[Ser97] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. AK Peters/CRC Press, 1997.

[Was12] Lawrence C Washington. *Introduction to cyclotomic fields*. Springer Science & Business Media, 2012.