权为一的模形式与Galois表示

阳恩林[*]
指导教师：印林生教授

摘　要

本文主要目的是介绍模形式与Galois表示。历史上有三个关于模形式与Galois表示的重要猜想，其中之一为Serre猜想，2009年C.Khare彻底解决了Serre猜想。第二章中我们将介绍模形式的概念及其性质，以及引入Artin L函数、Artin导子、Galois表示等概念，最后叙述Serre猜想并给出若干推论。第三章中我们给出Deligne-Serre猜想的证明，这个证明属于Deligne-Serre。

关键词：Galois表示；新形式；单项域；拟分圆域；导子；提升；η级数；θ级数

§1　引言

§1.1　一系列猜想

设$G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$，其中$\overline{\mathbb{Q}}$为$\mathbb{Q}$的某个代数闭包，我们将$G_{\mathbb{Q}}$看为投射有限群（profinite group）。我们将考察$G_{\mathbb{Q}}$的如下三种（连续）表示：

(a) $\rho : G_{\mathbb{Q}} \to GL_n(\mathbb{C})$，$n$维复表示，其中复数域$\mathbb{C}$考虑为离散拓扑。

(b) $\rho : G_{\mathbb{Q}} \to GL_n(\overline{\mathbb{F}_p})$，其中$\overline{\mathbb{F}_p}$为$p$阶有限域$\mathbb{F}$的代数闭包，将$GL_n(\overline{\mathbb{F}_p})$看成离散拓扑群。

(c) $\rho : G_{\mathbb{Q}} \to GL_n(K)$，其中$K$为$\mathbb{Q}_p$的有限扩张, 并将其看成$p-adic$拓扑群。

给定嵌入$\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$，我们将复共轭运算$c$限制到$\overline{\mathbb{Q}}$上，从而$c$可看成$G_{\mathbb{Q}}$中的元素。注意$c$是一个两阶元。我们称上述三种表示是奇表示如果$\det(\rho(c)) = -1$。对应于上面三种表示，有三个著名的猜想：

[*]基数63

(a) Artin-Langlands：如果$\rho: G_{\mathbb{Q}} \to GL_2(\mathbb{C})$是不可约连续奇表示，则$\rho$可由权为1的新形式提升而来(我们将在后面给出新形式与提升的精确概念)。

(b) Serre：如果$\rho: G_{\mathbb{Q}} \to GL_n(\overline{\mathbb{F}_p})$ 是不可约连续奇表示，设ρ的Serre权为$k(\rho)$，Serre导子为$N(\rho)$。则ρ可由权为$k(\rho)$，$\Gamma_1(N(\rho))$上的新形式提升而来。

(c) Fontaine-Mazur：假设奇表示$\rho: G_{\mathbb{Q}} \to GL_n(\mathcal{O}_K)$绝对不可约，只在有限个素点处分歧，并且$\rho\mid_{D_p}$半稳定。其中$\mathcal{O}_K$为$K$的整环，$K/\mathbb{Q}$为有限扩张。假设$\rho\mid_{D_p}$具有Hodge-Tate权$(a,b)(a \geq b)$，则$\rho \otimes \chi_p^{-b}$可由权为$a-b+1$的新形式提升而来。

我们知道从猜想(b)可以推出猜想(a)与(c)，而猜想(c)也可以得到猜想(b)。而Serre猜想已经于2009年被Chandrashekhar Khare与Jean-Pierre Wintenberger所证明 [1, 2]，从而上面三个猜想都是正确的。

上面这些猜想是说，给定一个新形式，便能给出Galois表示，反之，满足一定条件的Galois表示就给出了一新形式。新形式与Galois表示之间的这种对应，使得，我们在考虑Galois表示时，可以借用模形式的研究方法，以及在考虑模形式问题时，可借用Galois表示中的方法。更加广泛的猜想是Langlands猜想。

§1.2 工作介绍

Serre 在文[3]、[4]中提出了Serre猜想，并详细的考察了$G_{\mathbb{Q}}$的2维复表示与权为一的模形式的关系。本文的第一个目的是在Serre猜想被解决情况大背景下，重新考察Serre的工作，并给出某些命题的推广。对于两维复Galois表示（Artin表示）ρ而言，有三个重要的量：

(a) 表示ρ所给出的Artin L 函数$L(s,\rho)$。

(b) 表示ρ的Artin导子。

(c) ρ所对应的新形式。

Deligne-Serre定理是说，给定一个新形式$f = \sum a_n q^n \in S_1(\Gamma_0(N), \epsilon)$，便有一个Artin表示$\rho$与之对应，并且成立：

$$\begin{aligned} Trace(\rho(Frob_p)) &= a_p \\ \det(\rho(Frob_p)) &= \epsilon(p) \end{aligned}$$

Weil-Langlands定理则断言，给定一个Artin表示，便能给出一个新形式，且这个新形式所对应的L函数与该表示的Artin L函数一致。我们在第三章中将给出Deligne-Serre的证明。

在第四章中，我们利用Tate的方法先给出2维Artin L函数的一个积分表达式（或换成新形式的语言，给出了新形式所对应L函数的积分表达）。接着，利用Serre关于分歧群的结论，计算得到了拟分圆域$\mathbb{Q}(\sqrt{u_{pq}})$（p奇）不可约表示的导子，以及给出了$p=2$时导子在素点2处的一个估计。利用结论$M_0(\Gamma_1(N))=\mathbb{C}$，我们给出了一个模形式何时为乘积$\eta$级数的简单刻画。最后我们引入了单项域的概念，并给出了单项域一些性质与不变量猜想。

§2　知识回顾

§2.1　模形式、Hecke算子、新形式

§2.1.1　模形式的定义

令$\mathcal{H}=\{z\in\mathbb{C};Im(z)>0\}$为上半平面，

$$\Gamma=SL_2(\mathbb{Z})=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix};ad-bc=1,a,b,c,d\in\mathbb{Z}\right\}.$$

Γ通过如下方式作用在$\mathcal{H}$上：

$$\sigma z=\frac{az+b}{cz+d},\text{其中}\sigma=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma,z\in\mathcal{H}.$$

很容易验证上述作用为一个群作用，也即有$1z=z$，以及对所有的σ、$\tau\in\Gamma$，$\sigma(\tau z)=(\sigma\tau)z$。很自然的，上述作用诱导出了$\Gamma$对定义于$\mathcal{H}$上函数的一个作用：设$k$是一个整数，$f$是$\mathcal{H}$上的函数，定义

$$f\Big|_k\sigma(z)=(cz+d)^{-k}f(\sigma z)=(cz+d)^{-k}f\left(\frac{az+b}{cz+d}\right),\sigma\text{同上}.$$

为方便，我们定义$j(\sigma,z)=(cz+d)^{-1}$。我们称Γ_1是Γ的同余子群，如果Γ_1是Γ的子群，且$|\Gamma:\Gamma_1|<\infty$，后者也等价于说存在正整数N 使得$\begin{pmatrix} 1 & N \\ & 1 \end{pmatrix}\in\Gamma_1$。下面这两个同余子群是比较常见的：

$$\Gamma_0(N)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma;c\equiv 0\ mod\ N\right\}$$

$$\Gamma_1(N)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma;a\equiv b\equiv 1\ mod\ N,c\equiv 0\ mod\ N\right\}.$$

下面我们正式给出同余子群上模形式的定义 [5]。

定义2.1. 设N是大于*1*的整数，$\epsilon:(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$是*Dirichlet*特征，我们将其延拓为$\mathbb{Z}$上的特征，也即当$(n,N)\neq 1$时，令$\epsilon(n)=0$。注意，在本文中，我们都将这样看待*Dirichlet*特征。我们用R_d表示Γ中位置$(2,2)$处元素为d的任一矩阵，并令$\epsilon(R_d):=\epsilon(d)$。我们称函数$f$是$\Gamma_0(N)$上型为$(k,\epsilon)$的模形式，如果:

(1) f在$\mathcal{H}$上全纯。

(2) 对所有整数d，$f\big|_k R_d=\epsilon(d)f$。

(3) f在尖点处全纯。

类似得可以定义任一同余子群上的模形式，参见*[5]*。

我们来解释条件(3)：如果f满足条件(1)，则$f(z+1)=f(z)$，从而f有如下的傅里叶展开：

$$f(z)=\sum_{n=-\infty}^{\infty} a_n q^n,\ q=e^{2\pi iz.}$$

我们称f在无穷远点全纯，如果对所有$n<0$，$a_n=0$。称f在无穷远点消失，如果对所有的$n\leq 0$，$a_n=0$。如果对所有的$\sigma\in\Gamma$，$f\big|_k\sigma$在无穷远点出全纯，则称f在尖点处全纯。同理可定义f在尖点处消失。如果f在所有尖点处消失，则称f为尖（点）形式。我们用$M_k(\Gamma_0(N),\epsilon)$表示$\Gamma_0(N)$上型为$(k,\epsilon)$的模形式所形成的$\mathbb{C}$向量空间，用$S_k(\Gamma_0(N),\epsilon)$表示$\Gamma_0(N)$上型为$(k,\epsilon)$的尖点形式所形成的$\mathbb{C}$向量空间。

注记2.1. 由于$-I\in\Gamma_0(N)$，所以$(-1)^{-k}f=f\big|_k(-I)=\epsilon(-1)f$。假如$\epsilon(-1)\neq(-1)^k$，则推出$M_k(\Gamma_0(N),\epsilon)=0$。于是我们总假定$\epsilon(-1)=(-1)^k$。

注记2.2. $M_k(\Gamma_0(N),\epsilon)\in M_k(\Gamma_1(N),1)$

§2.1.2 Hecke算子及其性质

设p是一个素数，$f=\sum_{n\geq 0}a_nq^n\in M_k(\Gamma_0(N),\epsilon)$，定义Hecke算子$T_p$如下：

$$f\Big|_k T_p=\sum_{n=0}^{\infty}a_{np}q^n+\epsilon(p)p^{k-1}\sum_{n=0}^{\infty}a_nq^{np}.$$

注意，当$p|N$时，$\epsilon(p)=0$，此时有$f\big|_kT_p=\sum_{n\geq 0}a_{np}q^n$。

定理2.1. 如果$f\in M_k(\Gamma_0(N),\epsilon)$，则$f\big|_kT_p\in M_k(\Gamma_0(N),\epsilon)$。如果$f\in S_k(\Gamma_0(N),\epsilon)$，则$f\big|_kT_p\in S_k(\Gamma_0(N),\epsilon)$。

Proof. 对素数p，令$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$。考虑陪集分解$\Gamma_1(N)\alpha\Gamma_1(N) = \cup_j \Gamma_1(N)\beta_j$。由[6]第五章可知：

$$f\big|_k T_p = \sum_j f\big|_k \beta_j. \tag{2-1}$$

由于$\Gamma_1(N)$是$\Gamma_0(N)$的正规子群，对任何$\gamma \in \Gamma_0(N)$，成立：$\Gamma_1(N)\alpha\Gamma_1(N) = \cup_j \Gamma_1(N)\gamma\beta_j\gamma^{-1}$。于是$(f\big|_k T_k)\big|_k \gamma = (\sum_j f\big|_k \beta_j)\big|_k \gamma = (\sum_j f\big|_k \gamma\beta_j\gamma^{-1})\big|_k \gamma = \sum_j f\big|_k \beta_j = f\big|_k T_k$。所以$f\big|_k T_p \in M(\Gamma_0(N), k, \epsilon)$。当$f$为尖点形式时，从$T_p$的定义容易看出$f\big|_k T_p$依然为尖点形式。 □

§2.1.3 新形式、本原形式

设$\epsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$是Dirichlet特征，选取最小的整数$Cond(\epsilon)$，使得对所有的整数$n$成立$\epsilon(n \ mod \ N) = \epsilon(n \ mod \ Cond(\epsilon))$，一般地有$Cond(\epsilon)\big|N$，我们称$Cond(\epsilon)$为$\epsilon$的导子。我们将$S_k(\Gamma_0(N), \epsilon)$中由

$$\bigcup_M \bigcup_n \{f(nz); f(z) \in S(\Gamma_0(M), k, \epsilon)\}$$

张成的子空间记为$S^1(\Gamma_0(N), k, \epsilon)$，这里$M$ 遍历所有满足$Cond(\epsilon)\big|M$、$M\big|N$、$M \neq N$的正整数，而n遍历$\frac{N}{M}$的因子。我们称$S^1(\Gamma_0(N), k, \epsilon)$中模形式为旧形式。为了定义新形式，我们还需要引入Petersson内积。对任意f、$g \in S_k(\Gamma_0(N), \epsilon) \subset S_k(\Gamma_1(N))$，定义内积如下：

$$< f, g >:= \frac{1}{\mu(\Gamma_1(N))} \int_F f(z)\overline{g(z)} y^k \frac{dxdy}{y^2}, \mu(\Gamma_1(N)) = \int_F \frac{dxdy}{y^2}, F = \Gamma_1(N)\backslash\mathcal{H}.$$

我们把$S^1(\Gamma_0(N), k, \epsilon)$ 关于Petersson内积在$S_k(\Gamma_0(N), \epsilon)$中的正交补记为$S^0(\Gamma_0(N), k, \epsilon)$。并称$S^0(\Gamma_0(N), k, \epsilon)$为新形式空间。我们称$S^0(\Gamma_0(N), k, \epsilon)$中非零元素$f = \sum_{n\geq 1} a_n q^n$为特征形，如果对所有素数$p$，存在复数$\lambda_p$，使得$f\big|_k T_p = \lambda_p f$。事实上我们可以证明$\lambda_p = a_1^{-1} a_p$。由于

$$\lambda_p f = \sum_{n=1}^{\infty} \lambda_p a_n q^n = \sum_{n=1}^{\infty} a_{np} q^n + \epsilon(p) p^{k-1} \sum_{n=1}^{\infty} a_n q^{np},$$

对比系数便得到

$$\lambda_p a_n = \begin{cases} a_{np} + \epsilon(p) p^{k-1} a_{n/p}, & p|n, \qquad (2\text{-}2a) \\ a_{np}, & p \nmid n. \qquad (2\text{-}2b) \end{cases}$$

在（2-2b）中取$n = 1$，便得到$\lambda_p = a_1^{-1} a_p$。如果特征形f满足$a_1 = 1$，则称f为本原特征形或本原尖点形式或新形式(newform)。在这种情况下，式子（2-2b）是说a_n是积性

的，也即当$(n,m)=1$时，$a_{nm}=a_na_m$。式子（2-2a）可以化为：

$$a_{p^{m+1}}=a_pa_{p^m}-\epsilon(p)p^{k-1}a_{p^{m-1}}.$$

特别的，当$p\big|N$时，$a_{p^m}=(a_p)^m$。上面这些式子说明，当f为本原形式时，f傅里叶展开式中的系数由素数项系数决定。

注记2.3. 读者应该注意，在有些书籍中，新形式仅仅指新形式空间中的一个元素。

§2.1.4 函数方程

设χ是Dirichlet特征，$f=\sum_{n\geq 0}a_nq^n\in M_k(\Gamma_0(N),\epsilon)$。定义：

$$\begin{aligned}
L(s,\chi,f) &= \sum_{n\geq 1}a_n\chi(n)n^{-s},\\
\Lambda(s,\chi,f) &= (2Cond(\chi)^{-1}\pi)^{-s}\Gamma(s)L(s,\chi,f),\\
L(s,\chi,f) &= \sum_{n\geq 1}a_n\chi(n)n^{-s},\\
\Lambda(s,f) &= (2\pi\sqrt{N})^{-s}\Gamma(s)L(s,f).
\end{aligned}$$

我们知道$L(s,\chi,f)$与$L(s,f)$具有函数方程，且可以解析延拓到整个复平面。如果f还是本原尖点形式，则由式子（2-2a）、（2-2b）很容易证明：

$$L(s,f)=\prod_p(1-a_pp^{-s}+\epsilon(p)p^{k-1-2s})^{-1}.$$

令$\overline{f}=\sum\overline{a_n}q^n, f_1=N^{-k/2}z^{-k}f(\frac{1}{Nz})$，可以证明 [7] f_1是$S(\Gamma_0(N),k,\overline{\epsilon})$中特征形，进一步，存在复数$c$使得$f_1=cf$，且满足函数方程$\Lambda(s,f)=ci^k\Lambda(s,\overline{f})$。

§2.2 Frobenius置换，Artin导子，非交换Artin-L函数

§2.2.1 Frobenius置换

设E/K是数域的Galois扩张，$G=Gal(E/K)$。设$\mathfrak{p}$是K的有限素点，且E/K在$\mathfrak{p}$处非分歧。取E中在$\mathfrak{p}$之上的素点$\mathfrak{q}$。则在G中存在唯一元$Frob_{\mathfrak{p},\mathfrak{q}}$使得$Frob_{\mathfrak{p},\mathfrak{q}}(x)\equiv x^{N(\mathfrak{p})}\ mod\ \mathfrak{q}$，其中$N(\mathfrak{p})=\#(\mathcal{O}_K)/\mathfrak{p}$，$\mathcal{O}_K$为数域$K$的整环。容易证明对所有的$\sigma\in G$，$Frob_{\mathfrak{p},\sigma(\mathfrak{q})}=\sigma(Frob_{\mathfrak{p},\mathfrak{q}})\sigma^{-1}$。从而$Frob_{\mathfrak{p},\mathfrak{q}}$在$G$中所处的共轭类与$\mathfrak{q}$的选取无关。我们将这个共轭类记为$Frob_{\mathfrak{p}}$，称之为$E/K$在$\mathfrak{p}$处的Frobenius置换。

§2.2.2 Artin导子及其性质

关于这一小节，请读者参见[8]。依然采用§2.2.1中记号。设E/K是数域的Galois扩张，$G=Gal(E/K)$。

对E的任一素除子$\mathfrak{q}$，定义分解群$D_{\mathfrak{q}}=\{\sigma\in G;\sigma(\mathfrak{q})=\mathfrak{q}\}$。当$\mathfrak{q}$为无限素除子时，$D_{\mathfrak{q}}$的阶为1或2。经典的结论是$D_{\mathfrak{q}}=Gal(E_{\mathfrak{q}}/K_{\mathfrak{p}})$，其中$E_{\mathfrak{q}}$为$E$关于$\mathfrak{q}$的完备化，$K_{\mathfrak{q}}$为$K$关于$\mathfrak{p}$的完备化，而$\mathfrak{p}=\mathfrak{q}\cap\mathcal{O}_K$。惯性群$I_{\mathfrak{q}}$被定义为自然态射$D_{\mathfrak{q}}\to Gal(\overline{E}/\overline{K})$的核，其中$\overline{E}=\mathcal{O}_E/\mathfrak{q}$，$\overline{K}=\mathcal{O}_E/\mathfrak{p}$。我们还需要$i$次分歧群的概念。对任意的整数$i\geq -1$，定义$i$次分歧群如下：

$$G_{\mathfrak{q},i}=\{s\in D_{\mathfrak{q}};\nu_{E,\mathfrak{q}}(s(a)-a)\geq i+1,\forall a\in\mathcal{O}_{E_{\mathfrak{q}}}\},$$

其中$\nu_{E,\mathfrak{q}}$为$E_{\mathfrak{q}}$关于$\mathfrak{q}$的赋值。容易知道$G_{\mathfrak{q},-1}=D_{\mathfrak{q}}$，$G_{\mathfrak{q},0}$为惯性群$I_{\mathfrak{q}}$，且对充分大的$i$，$G_{\mathfrak{q},i}=\{1\}$。

假设(ρ,V)为G的复表示，$\chi=Trace(\rho)$为其特征标。定义：

$$n(\chi,\mathfrak{p}):=n(\rho,\mathfrak{p}):=\sum_{i\geq 0}\frac{|G_{\mathfrak{q},i}|}{|G_{\mathfrak{q},0}|}(\chi(1)-\chi(G_{\mathfrak{q},i})),$$

其中$\chi(G_{\mathfrak{q},i})=|G_{\mathfrak{q},i}|^{-1}\sum_{s\in G_{\mathfrak{q},i}}\chi(s)$。注意上式定义与$\mathfrak{q}$的选取无关。Artin证明了$n(\chi,\mathfrak{p})$为一个整数。特别地，当$E/K$在$\mathfrak{p}$处非分歧时，$n(\chi,\mathfrak{p})=0$，而当当$E/K$在$\mathfrak{p}$处弱分歧时（即$G_{\mathfrak{q},1}=\{1\}$），$n(\chi,\mathfrak{p})=|\chi(1)-\chi(G_{\mathfrak{q},0})|$。

定理2.2. *表示ρ的Artin导子被定义为$Cond(\chi):=Cond(\rho):=\Pi_{\mathfrak{p}}\mathfrak{p}^{n(\chi,\mathfrak{p})}$。它有如下三个基本性质:*

(a) 对G的任意两个表示$\rho_1(\chi_1)$与$\rho_2(\chi_2)$，$Cond(\chi_1+\chi_2)=Cond(\chi_1)Cond(\chi_2)$。

(b) 设H是G的商群，χ'是H的某个特征标，χ为χ'的提升，则$Cond(\chi)=Cond(\chi')$。

(c) 设H为G的子群，H所对应的中间域为F。设χ为H的特征标，$\chi^*=Ind_H^G(\chi)$，则

$$Cond(\chi^*)=|Disc(F/K)^{\chi(1)}|\cdot Norm_{F/K}(Cond(\chi)),$$

其中$Norm_{F/K}$为范映射,$Disc(F/K)$为域扩张的判别式。

Proof. 参见Serre的书籍“Corps locaux”第四章[8]。我们将在后面用到这些性质，故摘录在这儿。 □

§2.2.3 非交换Artin-L函数及其性质

设E/K是数域的Galois扩张，$G=Gal(E/K)$。设$\mathfrak{p}$是K的有限素点，$\mathfrak{q}$是E中在$\mathfrak{p}$之上的素理想。考虑G的n维复表示$\rho:G\to GL_n(V)$,$\chi=Trace(\rho)$。令$V^{I_{\mathfrak{q}}}:=\{v\in V;\forall\sigma\in I_{\mathfrak{q}},\rho(\sigma)v=v\}$。定义Artin-L函数如下：

$$L(s,\chi):=L(s,\rho):=\prod_{\mathfrak{p}:\text{有限素点}}\det_{V^{I_{\mathfrak{q}}}}(1-N(\mathfrak{p})^{-s}\rho(Frob_{\mathfrak{p}}))^{-1},Re(s)>1,$$

其中$N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$。与Artin导子相对应，Artin-L函数有下面三个性质：

(a) 对G的任意两个表示$\rho_1(\chi_1)$与$\rho_2(\chi_2)$，$L(s,\chi_1+\chi_2) = L(s,\chi_1)L(s,\chi_2)$。

(b) 设H是G的商群，χ'是H的某个特征标，χ为χ'的提升，则$L(s,\chi) = L(s,\chi')$。

(c) 设H为G的子群，H所对应的中间域为F。设χ为H的特征标，$\chi^* = Ind_H^G(\chi)$，则$L(s,\chi^*) = L(s,\chi)$。

关于Artin-L函数在无穷素点处因子的定义请参见文献[9]中J.Martinet的文章"Character theory and Artin L-functions"。

Artin猜想是说：当χ不包含单位特征标时，$L(s,\chi)$可解析延拓为整个复平面上的全纯函数。Artin猜想对维数为一的特征标是正确的，这可由Hecke理论可知！再由§2.2.3(a)可知，对一维特征标的线性组合，Artin猜想依然成立。事实上，对于二维不可约奇特征标，Artin猜想也是对的，参见下一小节！Brauer证明了$L(s,\chi)$具有亚纯延拓性，Langlands与Tunnel证明了当二维表示ρ的像为可解群群时，Artin猜想成立。Langlands还有个更强的猜想：存在$GL_n(\mathbb{A}_{\mathbb{Q}})$的尖（cuspidal）自守表示$\pi$使得$L(s,\rho) = L(s,\pi)$。Godement-Jacquet已证明$L(s,\pi)$可解析延拓了整个复平面，从而Langlands猜想意味中Artin猜想。

§2.2.4 Galois表示、Serre权、Serre导子

所谓Galois表示，指的是Galois群（特别是$G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$）的连续表示，包括复表示，模$p$表示以及$p-adic$表示。称$G_{\mathbb{Q}}$的表示$\rho$为奇表示，如果$\det(\rho(c)) = -1$，其中$c$为复共轭（此时，我们固定一个嵌入$\mathbb{Q} \hookrightarrow \mathbb{C}$）。称Galois表示$\rho$在$p$处非分歧，如果$\rho|_{I_p}$平凡。

定义2.2. *(a) 如果$\rho: G_{\mathbb{Q}} \to GL_2(\mathbb{C})$为两维、不可约、连续、奇表示，则称$\rho$为Artin表示。另外，我们称Artin表示具有Artin权1。*

(b) 如果$\rho : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}_p})$为2维连续、不可约、奇表示，则称$\rho$为Serre表示，其中$\mathbb{F}_p$为$p$元有限域。Serre表示有两个重要的指标，即Serre权$k(\rho)$与Serre导子$N(\rho)$。Serre导子$N(\rho)$被定义为Artin导子$Cond(\rho)$中与p互素的那一部分。定义Serre权需要较长的篇幅，这里略去，请读者参见文献[3]。

我们称Artin表示的Artin导子以及Serre表示Serre导子简称为该表示的导子。而将Artin权与Serre权简称为表示的权。

给定新形式$f \in S_k(\Gamma_0(N),\epsilon)$，考虑它的$q$展开：$f = \sum_{n\geq 1} a_n q^n$，其中$a_1 = 1$。对$\overline{\mathbb{Q}}$的每一个素点$\lambda$，固定一个嵌入$\iota_\lambda : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$，则存在一个连续且不可约的半单表示$\rho_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Q}}_p)$满足：

1. $\rho_{f,\lambda}$在Np之外非分歧，也即对所有的素数l，$\rho_{f,\lambda}$在l处非分歧，其中p是λ的剩余类域特征。

2. 对所有的$l \nmid Np$，$Trace(\rho_{f,\lambda}(Frob_l)) = \iota_\lambda(a_q)$。

3. 对所有的$l \nmid Np$，$\det(\rho_{f,\lambda}(Frob_l)) = \chi_l^{k-1}\iota_\lambda(\epsilon(l))$。其中$\chi_l$为$l$分圆域特征。

上述结论，当$k=2$时由Eichler与Shimura所解决，而$k>2$时由Deligne所解决，$k=1$的情形由Deligne与Serre解决 [4]。我们称一个Galois表示ρ由模形式（新形式）提升而来，是指，存在一个新形式$f \in S_k(\Gamma_0(N), \epsilon)$，使得$\rho \cong \rho_{f,\lambda}$。反过来，给定一个满足一定条件的Galois表示，有三个主要的猜想，这在文章开头已经说及。最重要的是，2009年C.Khare与J-P.Wintenberger 彻底解决了Serre猜想 [1, 2]，也即有：

定理2.3 (Serre's conjecture)**.** *设$\mathbb{F}$为有限域，如果表示$\rho : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}})$连续，奇，且绝对不可约，则$\rho$可由$S_{k(\rho)}(\Gamma_1(N(\rho)))$中新形式提升而来。*

下面这个定理是文章[4]的主定理，也即权$k=1$时的情形。

定理2.4 (Deligne-Serre定理)**.** *设整数$N \geq 1$，ϵ是模N的Dirichlet奇特征（即$\epsilon(-1) = -1$）。再选取非零模形式$f \in M_1(\Gamma_0(N), \epsilon)$。假定对所有的素数$p \nmid N$，$f\big|_1 T_p = a_p f$。则存在一个在$N$之外非分歧的表示$\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$，使得对所有的素数$p \nmid N$:*

$$Trace(\rho(Frob_p)) = a_p, \det(\rho(Frob_p)) = \epsilon(p).$$

上述表示不可约当且仅当f是尖点形式。另外如果$f = \sum_{n=1} a_n q^n$是新形式，则$Cond(\rho) = N$，$L(s,\rho) = \sum_{n=1} a_n n^{-s}$。由于新形式所对应的$L$函数可以解析延拓到整个复平面，从而$L(s,\rho)$也可以解析延拓到整个复平面。

Proof. 这个定理的证明过于复杂，我们将其单独放到第三章。 □

注记2.4. *当2.4中的表示可约时，f为Eisenstein模形式。*

下面这个定理比文[4]中的Weil-Langlands定理更强，它是Deligne-Serre定理的逆。

定理2.5 (强Weil-Langlands定理)**.** *假定$\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$为不可约奇表示。设Artin-$L$函数有傅里叶展开: $L(s,\rho) = \sum_{n\geq 1} a_n n^{-s}$。令$N = Cond(\rho)$，$f = \sum_{n\geq 1} a_n q^n$，$\epsilon = \det(\rho)$，则$f \in S_1(\Gamma_0(N), \epsilon)$为新形式，且$\rho$由$f$提升而来。*

Proof. 事实上，我们只需要证明对$G_{\mathbb{Q}}$的所有一维表示χ，$L(s, \rho\otimes\chi)$全纯即可。当$\rho\otimes\chi$可约时，命题成立。当$\rho\otimes\chi$不可约时，由于$\rho\otimes\chi$依然为奇特征，由推论2.1，命题得证！ □

下面我们来看Serre猜想以及Deligne-Serre带来的一些推论，第一个是关于Artin猜想的。

推论2.1. 当$\rho: G_{\mathbb{Q}} \to GL_2(\mathbb{C})$为两维线性不可约奇表示时，$L(s,\rho)$全纯，也即此中情况下，$Artin$猜想成立。

Proof. 由[1]推论10.2可知，存在正整数N，使得ρ可由$S_1(\Gamma_1(N))$中某个新形式f提升而来，再由定理2.4可知，存在奇不可约表示$\rho_f: G_{\mathbb{Q}} \to GL_2(\mathbb{C})$，使得$\rho \cong \rho_f$ 且$L(s,\rho) = L(s,\rho_f) = L(s,f)$，但$L(s,f)$全纯，故$L(s,\rho)$也全纯！ □

Serre猜想告诉我们，如果新形式具有什么样的性质，则相应的，奇不可约表示也具有相对应的表示（还有更广泛的Langlands函子猜想）。比如：

推论2.2. 设ρ_1,ρ_2是$G_{\mathbb{Q}}$的两维线性不可约奇表示，且$\det(\rho_1) = \det(\rho_2)$。如果对所有的素数$p \nmid Cond(\rho_1)Cond(\rho_2)$，$Trace(\rho_1(Frob_p)) = Trace(\rho_2(Frob_p))$，则$\rho_1 \cong \rho_2$。特别地$Cond(\rho_1) = Cond(\rho_2)$。

Proof. 我们只需注意到，对于两个新形式，如果它们的傅里叶展式中除了有限项外，其它素数项的系数相等，则这两个新形式相等。然后再利用定理2.4即可。 □

然而，如果利用Cebotarev-density定理，我们可以得到一个比上述推论强一点的结论 [4]:

推论2.3. 设X是一些素数构成的集合，且密度为*1*，ρ_1、ρ_2是$G_{\mathbb{Q}}$的连续半单表示。假定对所有$p \in X$，ρ_1与ρ_2非分歧且$\det(1-\rho_1(Frob_p)T) = \det(1-\rho_2(Frob_p)T)$，则$\rho_1 \cong \rho_2$。

Proof. X的密度为1，是指$\delta(X) := \lim_{s\to 1} sup_{s>1} \frac{\sum_{p\in X} p^{-s}}{-\log(s-1)} = 1$。一个群的半单表示由它的特征多项式唯一决定（同构意义下）。从而我们只要证明ρ_1与ρ_2的特征多项式一样就可。注意到连续性条件，我们可以选取一个充分大的域扩张$K/\mathbb{Q}$，$G = Gal(K/\mathbb{Q})$ 使得ρ_1与ρ_2可以通过G进行分解。对任意的$\sigma \in G$，考虑它在G中的共轭类$[\sigma]$。由Cebotarev-density定理，$\delta(A) = \frac{|[\sigma]|}{|G|}$，其中$A = \{p素数; p非分歧,且Frob_p = [\sigma]\}$。由于X具有密度1，从而可知$X \cap A \neq \emptyset$，故存在$p \in X$使得$Frob_p = [\sigma]$。所以：

$$\begin{aligned} \det(1-\rho_1(\sigma)T) &= \det(1-\rho_1(Frob_p)T) \\ &= \det(1-\rho_2(Frob_p)T) \\ &= \det(1-\rho_2(\sigma)T) \end{aligned}$$

命题得证。 □

注记2.5. 我们可以抽象出一条原则：假如命题A只与某个$Galois$群G中共轭元有关，且如果对所有$Frobenius$置换A成立，则A是真命题。那么如果X密度为1，使得对X中所有元A真，则A对G中所有元都真。

事实上，Serre有比前面两个推论更强的结果 [9]：

定理2.6. 设ρ_1, ρ_2是$G = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$的两个$Artin$表示（或同时为$Serre$表示）。设它们的导子都为$N$，权为$k$且$\epsilon = \det(\rho_1) = \det(\rho_2)$。令$P$为$N$的素因子集，$A(N, \epsilon) = N \prod_{p \in P} p^{e_p}$，其中：

$$e_p = \begin{cases} 2, & p \nmid N, \quad (2\text{-}3) \\ 0, & p^2 | N，且\epsilon可通过模N/p定义。 \quad (2\text{-}3') \\ 1, & 其它情形。 \quad (2\text{-}3'') \end{cases}$$

如果对所有满足

$$l \notin P \text{ 且 } l \leq \frac{1}{12} A \prod_{p \in P} (1 + p^{-1})$$

的素数l，$Trace(\rho_1(Frob_l)) = Trace(\rho_2(Frob_l))$，则$\rho_1 \cong \rho_2$。

Proof. 由Serre猜想，存在新形式$f_i = \sum_{i \geq 1} a_n^i q^n, i = 1, 2$，使得对所有素数$p \nmid N$，$Trace(\rho_i(Frob_p)) = a_p^i$。令$g = f_1 - f_2 = \sum b_n q^n$，$g^* = \sum_{(n,N)=1} b_n q^n = \sum_n b_n^* q^n$。由[[7]，p.287]可知，$g^* \in S_k(\Gamma_0(A), \epsilon)$，且由假设：

$$\forall n \leq \frac{1}{12} A \prod_{p \in P} (1 + p^{-1}), b_n^* = 0. \quad (2\text{-}4)$$

设ϵ的阶为r，则$(g^*)^r \in S_k(\Gamma_0(A))$，且在无穷远点的阶至少为$\frac{r}{12}|\Gamma : \Gamma_0(A)| + r$，从而$(g^*)^r = 0$。命题得证。 □

下面这个推论表明，Hecke算子T_p在$M_1(\Gamma_0(N), \epsilon)$上的特征值落在半径为2的圆中，参见文献[4]。

推论2.4. 假设$f \in M_1(\Gamma_0(N), \epsilon)$，且对所有$p \nmid N, f\big|_1 T_p = a_p f$。则$|a_p| \leq 2$。

Proof. 由Deligne-Serre定理，存在表示$\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ 使得$a_p = Trace(\rho(Frob_p))$。由于$\rho(G_{\mathbb{Q}})$为有限群，所以$\rho(Frob_p)$为有限阶元，从而它的特征值的绝对值为1。而$a_p$为$\rho(Frob_p)$的两个特征值之和，故有$|a_p| \leq 2$。 □

注记2.6. $Serre$ 还证明了，存在密度大于零的素数集X_N，使得所有$p \in X_N$，成立$p \equiv 1 \ mod \ N$且对所有的$g \in M_1(\Gamma_0(N), \epsilon)$，$g|T_p = 2g$。

§3 Deligne-Serre定理的证明

这一章，我们的目的是证明定理2.4，这个证明属于Deligne-Serre[4]。

§3.1 证明的第一部分

我们先证明该定理的后半部分。即证明，如果$f=\sum a_n q^n \in M_1(\Gamma_0(N),\epsilon)$是新形式，则$Cond(\rho)=N$以及$L(s,\rho)=L(s,f)$。我们需要如下两个引理：

引理3.1. 假设$f=\sum a_n q^n \in M_k(\Gamma_0(N),\epsilon)$是新形式，对素数$p|N$成立:

(a) 如果$p^2|N$且ϵ可通过模N/p定义，则$a_p=0$。

(b) 如果$p^2\nmid N$且ϵ可通过模N/p定义，则$|a_p|=p^{\frac{p-2}{2}}$。

(c) 如果$p^2\nmid N$且ϵ不能通过模N/p定义，则$|a_p|=p^{\frac{p-1}{2}}$。

特别地，当$k=1$时，总有$a_p<p^{-1/2}$。

Proof. 见[7]，或参见文献[10]第275页定理3。 □

引理3.2. 令$G(s)=A^s\prod_p G_p(s), H(s)=A^s\prod_p H_p(s)$为有限*Euler*积且满足$G(1-s)=\omega H(s)$，其中$\omega\in\mathbb{C}^*$。如果$p$因子$G_p$，$H_p$是有限多个$(1-\alpha_p^{(i)}p^{-s})^{\pm}$的乘积，$|\alpha_p^{(i)}|<p^{\frac{1}{2}}$。则$A=1$且$G_p=H_p=1$。

Proof. 如果$H_p\neq 1$，则H有无穷多个零点：

$$\frac{\log(\alpha_p^{(i)})+2\pi in}{\log p}, n\in\mathbb{Z}. \tag{3-5}$$

由假定条件$|\alpha_p^{(i)}|<p^{\frac{1}{2}}$，对任何$i$与$j$，$\alpha_p^{(i)}\neq p/\alpha_p^{(j)}$。但由函数方程可知，3-5中这些点都是$G(1-s)$的零点，于是存在$i$与$j$使得

$$\frac{\log(\alpha_p^{(i)})+2\pi in}{\log p}=1-\frac{\log(\alpha_p^{(j)})+2\pi im}{\log p}. \tag{3-6}$$

所以$\alpha_p^{(i)}\alpha_p^{(j)}=p$，矛盾。

□

回到Deligne-Serre定理，令$\tilde{f}=\sum \overline{a}_n q^n$。由（[7]，page296）可知，存在常数$\lambda\neq 0$使得$f(-\frac{1}{Nz})=\lambda z\tilde{f}$，且经过简单的计算可知：

$$(-2\pi i)^{-s}\Gamma(s)\sum_{i=1}^{\infty}a_n n^{-s}=\int_0^{i\infty}f(z)z^{s-1}dz. \tag{3-7}$$

进一步，令$\Psi_f(s)=N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(s,f)$，$\widetilde{\Psi}_f(s)=\Psi_{\bar{f}}(s)$，则

$$\Psi_f(1-s)=\mu\widetilde{\Psi}_f(s),\mu=\frac{i\lambda}{\sqrt{N}} \tag{3-8}$$

对于$L(s,\rho)$而言，它也满足类似的方程。事实上令$M=Cond(\rho)$，$\zeta(s,\rho)=M^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(s,\rho)$，则有:

$$\zeta(1-s,\rho)=\nu\zeta(s,\bar{\rho}),\nu\in\mathbb{C}^*. \tag{3-9}$$

注意到当$p\nmid N$时，$L(s,f)$与$L(s,\rho)$的p局部因子是相同的。设$A=\sqrt{\frac{N}{M}}$，$H(s)=A^s\frac{\Psi_f(s)}{\zeta(s,\rho)}$，$G(s)=A^s\frac{\widetilde{\Psi}_f(s)}{\zeta(s,\bar{(\rho)})}$。令$\Psi_f(s)$的$p$局部因子为$1-a_pp^{-s}$，$\zeta(s,\rho)$的$p$局部因子为$(1-b_pp^{-s})(1-c_pp^{-s})$，则$H(s)$的$p$局部因子为$H_p(s)=\frac{1-a_pp^{-s}}{(1-b_pp^{-s})(1-c_pp^{-s})}$。由前面的函数方程可知，$H(1-s)=\frac{\mu}{\nu}G(s)$。从而由引理3.2，我们只需要证明$a_p$、$b_p$、$c_p$以及它们的共轭的绝对值小于$p^{1/2}$。引理3.1表明$|a_p|<p^{1/2}$，而对于$b_p$与$c_p$而言，它们要么为零要么为单位根（因为$\rho$为连续表示）。从而我们证明了Deligne-Serre定理的后半部分。

§3.2 证明的第二部分

在这一部分，我们需要下面这个结论（参见[4]）：设$f=\sum a_nq^n\in S_k(\Gamma_0(N),\epsilon)$，$\sigma$为$\mathbb{C}$的自同构，令$f^\sigma=\sum\sigma(a_n)q^n$。则

(a) $f^\sigma\in S_k(\Gamma_0(N),\sigma(\epsilon))$。

(b) 如果系数a_n都是代数的，则它们的分母有界。

(c) 存在有限扩张$K/\mathbb{Q}$，使得Hecke算子T_p在空间$S_k(\Gamma_0(N),\sigma(\epsilon))$上的所有特征值包含在$\mathcal{O}_K$中。

我们也可以用Galois表示的语言叙述上面的结论：给定两维Artin表示ρ，则对所有的素数p，$Trace(\rho(Frob_p))$为代数数，且它们的分母有界，集合

$$\cup_\rho\cup_p\{Trace(\rho(Frob_p))\}$$

包含在某个代数整环中，其中ρ遍历导子为N的两维Artin表示，p遍历所有素数。对于Serre表示也有类似的结论。

§3.2.1 Rankin的结果

引理3.3. 设非零元$f\in S_k(\Gamma_0(N),\epsilon)$，且对所有$p\nmid N$，$f\big|_kT_p=a_pf$。则对所有$Re(s)>k$，$\sum_{p\nmid N}|a_p|^2p^{-s}$收敛且成立:

$$\sum_{p\nmid N}|a_p|^2p^{-s}\leq log(\frac{1}{s-k})+O(1),s\to k. \tag{3-10}$$

Proof. 由第二章，我们可以假定f是新形式，则$f=\sum_{n\geq 1}a_nq^n$。对$p\nmid N$，取$GL_2(\mathbb{C})$中元φ_p使得$Trace(\varphi_p)=a_p$，$\det(\varphi_p)=\epsilon(p)p^{k-1}$。于是：

$$L(s,f)=\prod_{p|N}(1-a_pp^{-s})^{-1}\prod_{p\nmid N}\det(1-\varphi_pp^{-s})^{-1}. \tag{3-11}$$

令$L(s)=\prod_{p\nmid N}\det(1-\varphi_p\otimes\bar{\varphi}_pp^{-s})^{-1}$，由（[7]，page312）可知道：

$$\begin{aligned} L(s) &= \prod_{p\nmid N}[(1-\lambda_p\bar{\lambda}_p)(\lambda_p\bar{\mu}_p)(\mu_p\bar{\lambda}_p)(\mu_p\bar{\mu}_p)]^{-1} \\ &= H(s)\zeta(2s-2k+2)\sum_{n=1}^{\infty}|a_n|^2n^{-s}, \end{aligned}$$

其中λ_p、μ_p是φ_p的特征值，而$H(s)=\prod_{p|N}(1-p^{-2s+2k-2})(1-|a_p|^2p^{-s})$。由引理3.1可知，对$p\big|N$，$|a_p|<\sqrt{p}$，所以$H(s)$在$Re(s)\geq k$上全纯且没有零点。另外，$\sum_{n=1}^{\infty}|a_n|^2n^{-s}$在$Re(s)>k$上收敛，而$\zeta(2s-2k+2)$能亚纯延拓到整个复平面且只在$s=k$处有单极点。故$L(s)$在整个复平面上亚纯，在$Re(s)\geq k$上全纯且只在$s=k$处有单极点，在$Re(s)>k$上$L(s)\neq 0$。令：

$$g_m(s)=\sum_{p\nmid N}|Trace(\varphi_p^m)|^2\frac{p^{-ms}}{m}, g(s)=\sum_{m\geq 1}g_m(s). \tag{3-12}$$

g是Dirichlet级数且系数非负，对充分大的s，可证明它等于$\log L(s)$。事实上，

$$\begin{aligned} \log L(s) &= \sum_{p\nmid N}(\log(1-\lambda_p\bar{\lambda}_pp^{-s})+\cdots \\ &= \sum_{p\nmid N}\sum_{m\geq 1}\frac{(\lambda_p\bar{\lambda}_pp^{-s})^m}{m} \\ &= \sum_{m\geq 1}\sum_{p\nmid N}|Trace(\varphi_p^m)|^2\frac{p^{-ms}}{m} \\ &= \sum_{m\geq 1}g_m(s). \end{aligned}$$

由于对$s>k$，$L(s)\neq 0$全纯，由Landu定理$g(s)$在$Re(s)>k$上全纯。因$L(s)$在$s=k$处有单极点，所以$g(s)=\log(\frac{1}{s-k})+O(1)$，$s\to k$。显然$g_1(s)\leq g(s)$，从而证明了$\sum_{p\nmid N}|a_p|^2p^{-s}\leq log(\frac{1}{s-k})+O(1), s\to k$。 □

设P是所有素数构成的集合，对P的子集X，定义（super）密度如下：

$$dens.sup(X)=\lim_{s\to 1}\sup_{s>1}\frac{\sum_{p\in X}p^{-s}}{-\log(s-1)}, \tag{3-13}$$

则$0\leq dens.sup(X)\leq 1$。

引理3.4. 在引理*3.3*的条件下，取$k=1$。则对任何$\eta>0$，存在子集$X_\eta \subset P$与有限子集$Y_\eta \subset \mathbb{C}$，使得

$$dens.sup(X_\eta) \le \eta \text{ 且对所有} p \notin X_\eta, a_p \in Y_\eta. \tag{3-14}$$

Proof. 由这一节开头部分，可假定a_p是有限扩域$K/\mathbb{Q}$中整元。对$c \ge 0$，令$Y(c)=\{a \in \mathcal{O}_K; \text{对所有嵌入}\sigma : K \hookrightarrow \mathbb{C}, |\sigma(a)|^2 \le c\}$，容易知$Y(c)$是有限集。再令$X(c)=\{p \in P; a_p \notin Y(c)\}$。由于对所有$\sigma$，$\sigma(a)$依然是$T_p$的特征值，利用引理3.3得到：

$$\sum_\sigma \sum |\sigma(a_p)|^2 p^{-s} \le |K:\mathbb{Q}| \log(\frac{1}{s-1}), s \to 1. \tag{3-15}$$

如果$p \in X(c)$，则$\sum_\sigma |\sigma(a_p)|^2 \ge c$，故：

$$c \sum_{p \in X(c)} p^{-s} \le |K:\mathbb{Q}| \log(\frac{1}{s-1}), s \to 1. \tag{3-16}$$

也即$dens.sup(X(c)) \le \frac{|K:\mathbb{Q}|}{c}$。取充分大的$c$即可得证引理。 □

§3.2.2 $GL_2(F_l)$的子群

定义3.1. *(a)* 设l是素数，令$F_l=\mathbb{Z}/l\mathbb{Z}$。$\eta$与$M$是正数，我们称$GL_2(F_l)$的子群$G$具有型$(\eta, M)$，如果$G$中存在子集$H$，使得$(1-\eta)|G| \le |H|$，且$\{\det(1-hT); h \in H\}$至多有$M$个元素。我们用$|A|$表示集合$A$中元素个数。

(b) 称群G是半单的，如果存在一个半单的表示$G \to GL_2(F_l)$。

引理3.5. 令$\eta<\frac{1}{2}$，$M>0$。则存在常数$A=A(\eta, M)$使得对任何素数l以及$GL_2(F_l)$的任一(η, M)型半单子群G，成立$|G| \le A$。

Proof. 设G是$GL_2(F_l)$的半单子群，则它满足以下条件中的一个（[11]，性质15，16）：

(1) $SL_2(F_l) \subset G$。

(2) G包含在$GL_2(F_l)$的某个Cartan子群T。

(3) G包含在$GL_2(F_l)$的某个Cartan子群T的正规化子里，但不包含在T中。

(4) G在$PGL_2(F_l)=GL_2(F_l)/F_l^*$中的像同构于$A_4$、$S_4$或$A_5$。

我们分上述四种情况讨论问题：

情形(1)： 令$r = |G : SL_2(F_l)|$，则$|G| = rl(l^2-1)$。$GL_2(F_l)$中具有给定特征多项式的元素个数只有l^2+l、l^2、l^2-1 这三种可能，它们分别对应于该特征多项式在F_l中有2、1、0个根。因此，如果G为(η, M)型子群，则：

$$(1-\eta)rl(l^2-1) = (1-\eta)|G| \le |H| \le M(l^2+1). \tag{3-17}$$

从而有$|G| \le \frac{M(1+l^2)}{1-\eta}$且$l \le 1 + \frac{M}{1-\eta}$。

情形(2)： T中具有给定特征多项式的元素个数至多为2。从而$|G| \le \frac{2M}{1-\eta}$。

情形(3)： $G_1 = G \cap T$在G中指数为2。从而，如果G具有型(η, M)，则G_1具有型$(2\eta, M)$。再由情形二可知$|G| \le \frac{4M}{1-\eta}$。

情形(4)： 对于这种情况有$|G| \le \frac{120M}{1-\eta}$。

□

§3.2.3 表示的约化

设$K \subset \mathbb{C}$是代数数域。$\mathfrak{p}$是K的有限素点，$\mathcal{O}_\mathfrak{p} := \mathcal{O}_{K_\mathfrak{p}}$，$m_\mathfrak{p}$是$\mathcal{O}_\mathfrak{p}$的极大理想。令$k_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/m_\mathfrak{p}$，$p = char(k_\mathfrak{p})$。我们将记号$mod\ m_\mathfrak{p}$简写为$mod\ \mathfrak{p}$。我们称$f \in M_k(\Gamma_0(N), \epsilon)$是$\mathfrak{p}$整的，如果它的傅里叶展开式系数属于$\mathcal{O}_\mathfrak{p}$。假定$f \in M_k(\Gamma_0(N), \epsilon)$是$\mathfrak{p}$整的，我们称它是$T_l\ mod\ \mathfrak{p}$的特征向量且具有特征值$a_l \in k_\mathfrak{p}$，如果$f\big|_k T_l \equiv a_l\ (mod\ \mathfrak{p})$。

引理3.6. 设$K \subset \mathbb{C}$是代数数域。$\mathfrak{p}$是K的有限素点。设$f \in M_k(\Gamma_0(N), \epsilon)$是$\mathfrak{p}$整的，且$f\ mod\ \mathfrak{p}$不等于零。假如对所有的素数$l \nmid Np$，$f\big|_k T_l \equiv a_l\ (mod\ \mathfrak{p})$，$a_l \in k_\mathfrak{p}$。取$k_f$是包含所有$a_l$以及$\epsilon(l)$的$k_\mathfrak{p}$之子域。则存在半单表示$\rho : G = Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(k_f)$使得$\rho$在$Np$之外非分歧，且对所有素数$l \nmid Np$，$Trace(\rho(Frob_l)) = a_l$，$\det(\rho(Frob_l)) \equiv \epsilon(l)p^{k-1}\ (mod\ \mathfrak{p})$

§3.2.4 构造非分歧表示

我们回忆模形式的一个性质：对$f \in M_k(\Gamma_0(N), \epsilon)$，我们总可以将它写成$f = \sum a_i f_i(d_i z) + E(z)$的形式。其中$E$是Eisenstein级数，$f_i \in S_k(\Gamma_0(N_i), \epsilon)$是新形式，$d_i N_i | N$且$\epsilon$可通过模$N_i$定义。于是由表示的性质，在证明Deligne-Serre定理时，我们总可以假定f是一个Eisenstein级数或者新形式。对于f为Eisenstein级数的情形，Hecke在"Mathematische Werke"中已经证明，存在$(\mathbb{Z}/N\mathbb{Z})^*$的特征$\chi_1$、$\chi_2$使得：

$$\chi_1\chi_2 = \epsilon,\ a_p = \chi_1(p) + \chi_2(p)\ \forall p \nmid N. \tag{3-18}$$

通过类域论，我们将χ_1、χ_2看成$G=Gal(\overline{\mathbb{Q}}/\mathbb{Q})$的一维表示。于是取$\rho=\chi_1\oplus\chi_2$即可。下面的证明中，我们假定$f$是一个新形式。由这节开头所论述的结论，总可以选取有限Galois扩张$K/\mathbb{Q}$使得所有a_p、$\epsilon(p)$是$\mathcal{O}_K$中元。令$L=\{素数l;l在K中完全分裂\}$。对所有$l\in L$，取K中位于l之上的素点λ_l。由引理3.6，存在半单表示$\rho_l:G\to GL_2(F_l)$，使得ρ_l在Nl之外分歧，且对所有$p\nmid Nl$，$\det(1-\rho(Frob_p)T)\equiv 1-a_pT+\epsilon(p)T^2\ (mod\ \lambda_l)$。令$G_l$为$\rho(G)$在$GL_2(F_l)$中的约化。

引理3.7. *对所有$\eta>0$，存在常数M，使得对所有$l\in L$，G_l是(η,M)型子群。*

由引理3.4，存在素数集P的子集X_η，使得$dens.sup(X_\eta)\le\eta$且$\{a_p;p\nmid X_\eta\}$是有限集。取$\mathfrak{U}=\{1-a_pT+\epsilon(p);p\notin X_\eta\}$，$M=\#\mathfrak{U}$。我们断言：对所有$l\in L$，$G_l$是$(\eta,M)$型子群。事实上，取$H_l$为$\rho_l(Frob_p)$（$p\notin X_\eta$）及其共轭所构成的子集。由Cebotare密度定理，$|H_l|\ge(1-\eta)|G_l|$。另一方面，如果$h\in H_l$，$\det(1-hT)$是$\mathfrak{U}$中某个元的约化，从而$\{\det(1-hT);h\in H_l\}$至多有M个元素。引理3.7得证。结合引理3.7以及引理3.6我们得到：

引理3.8. *存在常数A，使得对所有$l\in L$，$|G_l|\le A$。*

选取A满足引理3.8，适当的扩大K，使得K中包含所有的$n(n\ \le\ A)$次单位根。令$Y=\{(1-aT)(1-bT);a,b是n次单位根,n\le A\}$。如果$p\nmid N$，则对所有$l\in L$，$l\neq p$，由$\det(1-\rho(Frob_p)T)\equiv 1-a_pT+\epsilon(p)T^2\ (mod\ \lambda_l)$以及$|G_l|\le A$，必存在$R(T)\in Y$使得：

$$1-a_pT+\epsilon(p)T^2\equiv R(T)\ mod\ \lambda_l. \tag{3-19}$$

由于Y是有限集，必存在某个$R(T)$使得上述同余关系对无限多个l都成立，所以$1-a_pT+\epsilon(p)T^2=R(T)$。令

$$L'=\{l\in L;l>A且对所有R,S\in Y,如果R\neq Y,则R-S\ (mod\ \lambda_l)不为零\}. \tag{3-20}$$

$L-L'$是有限集，所以L'是无限集。令$l\in L'$，则G_l的阶与l互素。一个经典的结论是，表示$G_l\to GL_2(F_l)$可由表示$G_l\to GL_2(\mathcal{O}_{\lambda_l})$约化而来，其中$\mathcal{O}_{\lambda_l}:=\mathcal{O}_{K_{\lambda_l}}$。通过复合自然同态$G\to G_l$得到表示$\rho:G\to GL_2(\mathcal{O}_{\lambda_l})$。由构造可知，$\rho$在$Nl$之外非分歧。对所有的$p\nmid Nl$，$\rho(Frob_p)$的特征值是阶小于等于$A$的单位根，所以$\det(1-\rho(Frob_p)T)\in Y$。由于$\det(1-\rho(Frob_p)T)\equiv 1-a_pT+\epsilon(p)T^2\ (mod\ \lambda_l)$，$1-a_pT+\epsilon(p)T^2\in Y$，我们得到$\det(1-\rho(Frob_p)T)=1-a_pT+\epsilon(p)T^2$。将$l$换为$L'$中任意素数$l'$，可得到满足相同性质的表示$\rho':G\to GL_2(\mathcal{O}_{\lambda_{l'}})$。从而对任何素数$p\nmid Nll'$，$\det(1-\rho(Frob_p)T)=\det(1-\rho'(Frob_p)T)$。由推论2.3可知$\rho$与$\rho'$作为$G$的复表示是同构的。故$\rho$在N外非分歧，且对所有$p\nmid N$，$\det(1-\rho(Frob_p)T)=1-a_pT+\epsilon(p)T^2$。

§3.2.5 最后一步

这一小节证明，当f是新形式时，上一小节构造的表示ρ是不可约的。假定ρ可约，则$\rho=\chi_1\oplus\chi_2$，其中χ_1、χ_2是在N之外非分歧的一维表示，它们满足：

$$\chi_1\chi_2=\epsilon, a_p=\chi_1(p)+\chi_2(p)\ \forall p\nmid N. \tag{3-21}$$

于是$\sum|a_p|^2p^{-s}=2\sum p^{-s}+\sum\chi_1(p)\bar{\chi}_2(p)p^{-s}+\sum\bar{\chi}_1(p)\chi_2(p)p^{-s}$。令$s\to 1$，有$\sum p^{-s}=\log(\frac{1}{s-1})+O(1)$。由于$\epsilon$为奇表示，从而$\chi_1\bar{\chi}_2\neq 1$，所以：

$$\begin{aligned}\sum\chi_1(p)\bar{\chi}_2(p)p^{-s} &= O(1)\\ \sum\bar{\chi}_1(p)\chi_2(p)p^{-s} &= O(1)\end{aligned}$$

事实上，令$\chi=\chi_1\chi_2$，$f_\chi(s)=\sum\chi_1(p)\bar{\chi}_2(p)p^{-s}$，$H(s,\chi)=\prod(1-\chi(p)p^{-s})^{-1}$。类似于引理3.1中的计算，可得到$\log H(s,\chi)=f_\chi(s)+F_\chi(s)$，其中$F_\chi(s)=\sum_{p,n\geq 2}\frac{\chi(p)^n}{p^{ns}}$。但我们知道，$|F_\chi(s)|\leq\sum_{p,n\geq 2}\frac{1}{p^{ns}}\leq\sum_p\frac{1}{p^s(p^s-1)}\leq\sum_{n\geq 2}\frac{1}{n(n-1)}=1$。由经典的Dirichlet L级数理论，当$\chi\neq 1$时，$H(1,\chi)\neq 0$。所以$\sum\chi_1(p)\bar{\chi}_2(p)p^{-s}=O(1)$。于是$\sum|a_p|^2p^{-s}=2\log\frac{1}{s-1}+O(1)$，$s\to 1$，这与引理3.1矛盾。故$\rho$不可约。

§3.3 证明过程中得到的重要结果

总结证明的第一部分，我们不难得到如下重要的结果：

定理3.1. *设有两个L级数$H(s)=\prod_p H_p(p^{-s})$, $G(s)=\prod_p G_p(p^{-s})$, 其中$H_p(t)$与$G_p(t)$是多项式。如果成立:*

(a) 存在无零点和无极点的函数$h(s)$与$g(s)$，使得$H(1-s)=h(s)H(s)$，$G(1-s)=g(s)G(s)$。

(b) 存在由素数构成的集合M，使得对所有$p\notin M$，$H_p=G_p$。

(c) 对所有的素数$p\in M$，$H_p(t)$与$G_p(t)$的根的绝对值$<\sqrt{p}$。

则$H=G$。

Proof. 假设$H\neq G$，令$L=\frac{H(s)}{G(s)}$，则$L(1-s)=c(s)L(s)$，其中$C=\frac{h(s)}{g(s)}$。类似引理3.2，可证明$L=1$。 □

定理3.2. *对于$M_1(\Gamma_0(N),\epsilon)$中本原的Eisenstein级数$f=\sum a_nq^s$，成立:*

$$\sum_{p\nmid N}|a_p|^2p^{-s}=2\log\frac{1}{s-1}+O(1), s\to 1. \tag{3-22}$$

Proof. 由Hecke“Mathematische Werke”可知：对于本原的Eisenstein级数，它所对应的表示是即约的。利用“最后一部分”中的证明即可得证上述定理。 □

参考文献

[1] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture(i). *Invent.Math.*, 178(3):485–504, 2009.

[2] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture(ii). *Invent.Math.*, 178(3):505–586, 2009.

[3] Jean-Pierre Serre. Sur les representations modulaires de degre 2 de gal($\overline{Q}$/q). *DUKE MATHEMATICAL JOURNAL*, 54(1):179–229, 1987.

[4] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *ANNALES SCIENTIFIQUES DE L'É.N.S*, 7(4):507–530, 1974.

[5] Toshitsune Miyake. *Modular Forms*. Springer, New York, 1th edition, 1989.

[6] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Springer-Verlag, New York, 1th edition, 2004.

[7] Wen-Ching Winnie Li. Newforms and functional equations. *Math.Ann*, (212):285–315, 1975.

[8] Jean-Pierre Serre. *Corps Locaux*. Hermann, Paris, 2th edition, 1968.

[9] A . Frohlich. *Algebraic Number Fields(L-functions and Galois properties)*. Academic Press, London, 1th edition, 1977.

[10] 陆洪文and 李云峰. 模形式讲义. 北京大学出版社, 北京, 1998.

[11] Jean-Pierre Serre. Proprietes galoisiennes des points d'ordre fini des courbes elliptiques. *Invent.Math.*, 15(4):259–331, 1972.