Math 726: L-functions and modular forms — Fall 2011

Lecture 29 : End of proof of the Serre-Deligne theorem

Instructor: Henri Darmon — *Notes written by: Francesca Gala*

The goal of this lecture is to conclude the proof of the **Serre-Deligne theorem**, which accompanied us along the last few lectures.
Recall that last week we associated to our eigenform $f \in S_1(D, \epsilon)$ a family of representations:

$$\overline{\rho_{f,\lambda}} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_\lambda),$$

where $\lambda \in \Sigma = \{\lambda \triangleleft \mathcal{O}_{K_f} | \mathcal{O}_{K_f}/\lambda \cong \mathbb{F}_\ell\}$. We let

$$G := G_\ell = \overline{\rho_{f,\lambda}}(G_{\mathbb{Q}}).$$

We would like to bound the cardinality of G_ℓ independently of ℓ.
Recall that G is a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, it is semisimple by construction and it is X-sparse for a suitable integer $X > 0$, i.e. there exists a subgroup $H \leq G$ such that $|H| \geq \frac{3}{4}|G|$ and the elements in H have at most X distinct characteristic polynomials.

Theorem 1. *If G is a semisimple, X-sparse subgroup of $\mathrm{GL}_2(\mathbb{F}_l)$, then $\exists A$ independent of ℓ such that $|G| \leq A$.*

Proof. To prove this theorem we will use the following proposition:

Proposition 1. *If G is a semisimple subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ then only the following four cases can arise:*
1. $G \supset SL_2(\mathbb{F}_\ell)$
2. G is contained in a Cartan subgroup T, either split or non-split, which means that $T \simeq \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$ or $T \simeq \mathbb{F}_{\ell^2}^\times$.
3. $G \subset N_{\mathrm{GL}_2(\mathbb{F}_\ell)}(T)$, where $N_{\mathrm{GL}_2(\mathbb{F}_\ell)}(T)$ is the normaliser of a Cartan subgroup T
Note that $[N(T) : T] = 2$ and there exists a split exact sequence:
$1 \to T \to N(T) \to \pm 1 \to 1$.
4. G is an 'exceptional subgroup', namely its image in $PGL_2(\mathbb{F}_\ell)$ is A_4, S_4 or S_5

Proof. Reference: J. P. Serre, Proprietes galoisiennes des points d'ordre fini des courbes elliptiques, chapter 2. □

REMARK 1. The semisimplicity assumption is crucial, for example if we consider

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} | a \in \mathbb{F}_\ell \right\},$$

then G is 1-sparse but $|G| = \ell$, so clearly we are not able to bound the cardinality of G independently of ℓ.

Now we can prove Theorem 1 by analysing separately the four cases of the proposition. Our strategy will be to bound the order of H by bounding the number of elements in $\mathrm{GL}_2(\mathbb{F}_\ell)$ which have the same characteristic polynomial, i.e. by bounding the number of elements in a given conjugacy class.

1. We know that $|\mathrm{GL}_2(\mathbb{F}_\ell)| = (\ell^2-1)(\ell^2-l) = \ell(\ell+1)(\ell-1)^2$.

Let $\sigma \in \mathrm{GL}_2(\mathbb{F}_\ell)$, then the cardinality of the set $C(\sigma) := \{\tau\sigma\tau^{-1}, \tau \in \mathrm{GL}_2(\mathbb{F}_\ell)\}$ is given by

$$|C(\sigma)| = \frac{|\mathrm{GL}_2(\mathbb{F}_\ell)|}{|Z(\sigma)|},$$

where $Z(\sigma) = \{\tau | \tau\sigma = \sigma\tau\}$ is the centraliser of σ in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Let us suppose that $\mathrm{char}(\sigma) = (x-a)^2$. This means that $\sigma \in C(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}) \cup C(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix})$.

Since

$$\left| Z(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}) = \left\{ \begin{pmatrix} u & v \\ 0 & u \end{pmatrix} | u \in \mathbb{F}_\ell^\times, v \in \mathbb{F}_\ell \right\} \right| = (\ell-1)\ell$$

we have that $\left| C(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}) \right| = \ell^2 - 1$,while clearly $\left| C(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}) \right| = 1$. So we have that: $|\{\sigma | \, \mathrm{char}(\sigma) = (x-a)^2\}| = \ell^2$.

Now clearly:

$$\left| \{\sigma | \, \mathrm{char}(\sigma) = (x-a)(x-b), a, b \in \mathbb{F}_\ell^\times a \neq b\} \right| = \left| C(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}) \right| = \ell^2 + \ell$$

since $\left| Z(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}) \right| = (\ell-1)^2$.

The last case to consider is the one of $\sigma \in \mathrm{GL}_2(\mathbb{F}_\ell)$ with $\mathrm{char}(\sigma)$ equal to a polynomial $p(x) = x^2 + ax + b$, which is irredubile over $\mathbb{F}_\ell$. In this case $|Z(\sigma)| = \ell^2 - 1$, so that:

$$|C(\sigma)| = (\ell-1)\ell.$$

Therefore we can deduce the following bound:

$$\frac{3}{4} |\mathrm{SL}_2(\mathbb{F}_\ell)| = \frac{3}{4}\ell(\ell+1)(\ell-1) \leq |H| \leq X(\ell^2+\ell),$$

which is a bound on H, independent of ℓ since for the inequalities to hold we must have $\ell-1 \leq X^{\frac{4}{3}}$.
2. In T there are at most two elements with a given characteristic polynomial, in fact since $\mathrm{char}(\sigma)=x^2-\mathrm{tr}(\sigma)+\det(\sigma)$, then we have $\{\sigma \in T|\,\mathrm{char}(\sigma)=x^2-ax+b\}=\{\sigma,\overline{\sigma}\}$. Hence in this case we have $|H| \leq 2X$ which implies:

$$|G| \leq \frac{8}{3}X.$$

3. Let $G_0 = G \cap T$ so that, since $[N(T):T]=2$, $|G_0|=\frac{1}{2}|G|$ and let $H_0 = H \cap T$ so that $|H_0| \geq \frac{1}{2}|G_0|$. Now from case 2. we can deduce that $|H_0| \leq 2X$, so that $|G_0| \leq 4X$ which implies $|G| \leq 8X$.
4. Consider the map:

$$\begin{array}{rccc} \eta: & G & \rightarrow & \mathrm{PGL}_2(\mathbb{F}_\ell)\times\mathbb{F}_\ell^\times \\ & \sigma & \mapsto & (\overline{\sigma},\det(\sigma)) \end{array}$$

Since we know that the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is A_4, S_4 or A_5 and X is the number of different characteristic polynomials in H we have that: $|\eta(H)| \leq |A_5|\,X = 60X$ and also $\ker(\eta)=\left\{\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1\end{pmatrix}\right\} \simeq \mathbb{Z}/2\mathbb{Z}$.
This implies that $|H| \leq 120X$ and $|G| \leq 160X$.
This concludes case 4. and the proof of the theorem. □

We are now able to deduce a significant bound on the size of the Fourier coefficients of the eigenform $f \in S_1(\Gamma_0(D),\epsilon)$.

Theorem 2. *For all primes p, the coefficient $a_p(f)$ is a sum of roots of unity. In particular $|a_p(f)| \leq 2$.*

Proof. Let

$$\mathbb{P}_{\overline{K_f}} = \{g(x)=(x-\alpha)(x-\beta) \in \mathcal{O}_{\overline{K_f}}[x] | \alpha \text{ and } \beta \text{ are roots of unity of order } \leq A\}$$

and, for every $\lambda \in \Sigma$,

$$\mathbb{P}_\lambda = \{g(x)=(x-\alpha)(x-\beta) \in \mathcal{O}_{K_f}/\lambda[x] | \alpha,\beta \in \overline{\mathcal{O}_{K_f/\lambda}} \text{ and } \mathrm{ord}(\alpha),\mathrm{ord}(\beta) \leq A\}.$$

We have that $\mathbb{P}_{\overline{K_f}}$ and $\mathbb{P}_\lambda$ are finite and there exists a reduction map mod λ:

$$\mathrm{red}_\lambda : \mathbb{P}_{\overline{K_f}} \rightarrow \mathbb{P}_\lambda,$$

which is bijective if $\ell > A$.
If we let $\sigma = \mathrm{Frob}_p$, then the characteristic polynomial $\mathrm{char}(\overline{\rho_{f,\lambda}}) = x^2 - a_p x + \epsilon(p) \in$

$\mathcal{O}_{K_f}/\lambda[x]$ belongs the set $\mathbb{P}_\lambda$. Since $\mathbb{P}_{\overline{K_f}}$ is finite, there exists a polynomial $g \in \mathbb{P}_{\overline{K_f}}$ such that $\mathrm{red}_\lambda(g) \cong x^2 - a_p x + \epsilon(p) \bmod \lambda$, for infinitely many λ, which implies that $g = x^2 - a_p x + \epsilon(p)$. So we can conclude that

$$x^2 - a_p x + \epsilon(p) \in \mathbb{P}_{\overline{K_f}},$$

and the roots of $x^2 - a_p x + \epsilon(p)$ are roots of unity of order $\leq A$. □

End of the proof of Serre-Deligne's theorem.
The embedding of G_ℓ in $\mathrm{GL}_2(\mathbb{F}_\ell)$ gives a two-dimensional representation ρ_ℓ of G_ℓ over the field $\mathbb{F}_\ell$. Because G_ℓ is of cardinality prime to ℓ, there is a complex two-dimensional representation ρ of G_ℓ satisfying

$$\mathrm{tr}(\rho(\sigma)) = \mathrm{tr}(\rho_\ell(\sigma)) \bmod \lambda$$

for a suitable prime λ above ℓ in the field generated by the traces of ρ. This representation is the desired lift.