Anillos de deformación de representaciones para primos de Taylor-Wiles

Matías Alvarado

Junio 2020

Estudiaremos R_Σ para ciertos conjuntos especiales. Los elementos de Σ tienen las propiedades

- $q \equiv 1 \pmod{\ell}$
- $\overline{\rho}$ es no ramificado en q y $\overline{\rho}(\mathrm{Frob}_q)$ tiene dos valores propios distintos en k

Para estos casos especiales usaremos Q en lugar de Σ

Para $q \in Q$, denotaremos por α_q y β_q los valores propios de $\overline{\rho}(\mathrm{Frob}_q)$

Definición

Δ_q *es el cuociente maximal de* $(\mathbb{Z}/q\mathbb{Z})^\times$ *de orden potencia de* ℓ

Observación

Δ_q *es un cociente de* $G_\mathbb{Q}$ *y* G_q

$$\chi_q\colon G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \Delta_q$$

$$\chi_q\colon G_q \longrightarrow \mathrm{Gal}(\mathbb{Q}_q(\zeta_q)/\mathbb{Q}_q) \simeq (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \Delta_q$$

$$\Delta_Q = \prod \Delta_q \text{ y } \chi_Q = \prod \chi_q\colon G_{\mathbb{Q}} \to \Delta_Q$$

Definición (Ideal de augmentation)

El ideal de augmentation en $R[G]$ se define como el núcleo del morfismos $R[G] \to R$ dado por $\sum r_i g_i \mapsto \sum r_i$

Si $\#Q = r$, definimos un morfismo de $\mathcal{O}$-álgebras

$$\mathcal{O}[[S_1, ..., S_r]] \to \mathcal{O}[\Delta_Q]$$

tal que $S_i \mapsto \delta_{q_i} - 1$ (donde δ_{q_i} es generador de Δ_{q_i}), el cual induce un isomorfismo

$$\mathcal{O}[[S_1, ..., S_r]]/((1 + S_i)^{\#\Delta_{q_i}}, q \in Q) \to \mathcal{O}[\Delta_Q]$$

en donde el idel de augmentation se corresponde con $(S_q : q \in Q)$

Lema

Sea $q \in Q$, entonces $\rho_Q^{uinv}|_{G_q}$ es conjugado a $\begin{pmatrix} \xi & 0 \\ 0 & \epsilon\xi^{-1} \end{pmatrix}$ para algún caracter ξ con $\overline{\xi}(Frob_q) = \alpha_q$

Demostración: Sea f un levantamiento de Frob_q a G_q. Por lema de Hensel, $\rho_Q^{univ}(f)$ tiene valores propios en R_Q, que llamaremos $\widetilde{\alpha}_q$ y $\widetilde{\beta}_q$. Cambiando de base si fuera necesario, la imagen de f tiene la forma $\rho_Q^{univ}(f) = \begin{pmatrix} \widetilde{\alpha}_q & 0 \\ 0 & \widetilde{\beta}_q \end{pmatrix}$. Veamos ahora que para $\sigma \in I_q$, $\rho_Q^{univ}(\sigma)$ es diagonal en esta base.
$\rho_Q^{univ}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, con $a, b, c, d \in \mathfrak{m}_{R_Q}$. Como ρ_Q^{univ} es moderadamente ramificada, tenemos que
$\rho_Q^{univ}(f)\rho_Q^{univ}(\sigma)\rho_Q^{univ}(f)^{-1} = \rho_Q^{univ}(\sigma)^q$(ver anexo) por lo tanto tenemos

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} a & b\dfrac{\widetilde{\alpha}_q}{\widetilde{\beta}_q} \\ c\dfrac{\widetilde{\beta}_q}{\widetilde{\alpha}_q} & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod \mathfrak{m}_{R_Q}^2$$

Por lo tanto $\left(\dfrac{\widetilde{\alpha}_q}{\widetilde{\beta}_q} - 1\right) b, \left(\dfrac{\widetilde{\beta}_q}{\widetilde{\alpha}_q} - 1\right) c \in \mathfrak{m}_{R_Q}(b, c)$. De este modo tenemos que $(b, c)\mathfrak{m}_{R_Q} = \mathfrak{m}_{R_Q}$, con lo que concluimos que $b = c = 0$.

Consideremos ξ_q el caracter del lema.

- $\#\xi_q(I_q)|(q-1)$, pues $\rho(x) = \rho(x)^q$.
- $\xi_q|_{I_q}$ factoriza a traves de Δ_q
- Sea $\xi_Q \colon G_{\mathbb{Q}} \to R_Q^\times$ el caracter no ramificado fuera de primos de Q y $\xi|_{G_q} = \xi_q$,
- $\xi_Q|_{I_q}$ factoriza a traves de Δ_Q
- De este modo tenemos un morfismo $\Delta_Q \to R_Q^\times$
- R_Q tiene estructura de $\mathcal{O}[\Delta_Q]$-módulo

Proposición

Existe un isomorfismo de $\mathcal{O}$-álgebras $R_Q/\mathfrak{a}_Q R_Q \to R_\emptyset$, donde $\mathfrak{a}_Q$ es el ideal de augmentation

Demostración: Si existe una deformación sobre R de tipo $\emptyset$, en particular es de tipo Q, luego existe un único morfismo de $\mathcal{O}$-álgebras $R_Q \to R$. Este morfismo factoriza a traves de $R_Q/\mathfrak{a}_Q R_Q$, pues R es no ramificado en los primo de Q

Lema

(a) *Si* $q \in Q$, *entonces* $H^0(\mathbb{F}_q, ad^0\overline{\rho}) = H^0(\mathbb{F}_q, ad^0\overline{\rho}(1)) = k$ *y* $H^1(\mathbb{F}_q, ad^0\overline{\rho}) = H^1(\mathbb{F}_q, ad^0\overline{\rho}(1)) = k$.

(b) R_Q *puede ser generado topologicamente como* $\mathcal{O}$*-álgebra por*

$$\#Q + \dim_k H^1_Q(\mathbb{Q}, ad^0\overline{\rho}(1))$$

elementos

(c) *Si*

$$H^1_\emptyset(\mathbb{Q}, ad^0\overline{\rho}(1)) \simeq \bigoplus_{q \in Q} H^1(\mathbb{F}_q, ad^0\overline{\rho}(1))$$

entonces $\#Q = \dim_k H^1_\emptyset(\mathbb{Q}, ad^0\overline{\rho}(1))$ *y* R_Q *puede ser generado topologicamente como* $\mathcal{O}$*-álgebra por* $\#Q$ *elementos.*

(a) Si $q \in Q$, entonces $H^0(\mathbb{F}_q, ad^0\overline{\rho}) = H^0(\mathbb{F}_q, ad^0\overline{\rho}(1)) = k$ y $H^1(\mathbb{F}_q, ad^0\overline{\rho}) = H^1(\mathbb{F}_q, ad^0\overline{\rho}(1)) = k$.

Demostración: Frob_q actua por conjugación sobre $ad^0\overline{\rho}$. Si $M \in ad^0\overline{\rho}$ es la forma $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$,entonces

$$(\mathrm{Frob}_p).M = \begin{pmatrix} a & b\alpha_q/\beta_q \\ c\beta_q/\alpha_q & -a \end{pmatrix}$$

Por lo tanto el espacio invariante es 1 dimensional. Para $H^1(\mathbb{F}_q, ad^0\overline{\rho})$ debemos estudiar el cociente $ad^0\overline{\rho}/(\mathrm{Frob}_q - 1)ad^0\overline{\rho}$

(b) R_Q puede ser generado topologicamente como $\mathcal{O}$-álgebra por

$$\#Q + \dim_k H^1_Q(\mathbb{Q}, ad^0\overline{\rho}(1))$$

elementos

Demostración: El corolario 2.43 tenemos que el anillo R_Σ puede ser generado por

$$\dim_k H^1_\Sigma(\mathbb{Q}, ad^0\overline{\rho}(1)) + d_\ell + \sum_{p \in \Sigma - \{\ell\}} \dim_k H^0(\mathbb{Q}_p, ad^0\overline{\rho}(1))$$

$d_\ell = 0$ y $\sum \dim_k H^0(\mathbb{Q}_p, ad^0\overline{\rho}(1)) = \#Q$, por lo tanto R_Q puede ser generado por

$$\#Q + \dim_k H^1_Q(\mathbb{Q}, ad^0\overline{\rho}(1))$$

(c) Si

$$H^1_\emptyset(\mathbb{Q}, ad^0\overline{\rho}(1)) \simeq \bigoplus_{q\in Q} H^1(\mathbb{F}_q, ad^0\overline{\rho}(1))$$

entonces $\#Q = \dim_k H^1_\emptyset(\mathbb{Q}, ad^0\overline{\rho}(1))$ y R_Q puede ser generado topologicamente como $\mathcal{O}$-álgebra por $\#Q$ elementos.

Demostración: Por la parte anterior $R_\emptyset$ puede ser generado por $\#\emptyset + \dim_k H^1_\emptyset(\mathbb{Q}, ad^0\overline{\rho}(1)) = \#Q$ elementos. De este modo $R_Q/\mathfrak{a}_Q R_Q$ puede ser generado por Q elementos, por lo tanto lo mismo ocurre con R_Q

Teorema

(a) *Sea H subgrupo finito de $PGL_2(\mathbb{C})$, entonces H es isomorfo a uno de los siguientes grupos: Un grupo cíclico, un grupo dihedral, A_4, S_4 o A_5*

(b) *Sea H un subgrupo finito de $PGL_2(\overline{\mathbb{F}}_\ell)$ entonces se tiene una de las siguientes afirmaciones*
   - *H es conjugado a un subgrupo matrices triangulares superiores*
   - *H es conjugado a $PSL(F_{\ell^r})$ o $PGL_2(\mathbb{F}_{\ell^r})$ para algún r.*
   - *H es isomorfo a A_4, S_4, A_5 o un grupo dihedral*

Demostración:

- Suponemos que H está en algún $PGL_2(\mathbb{F}_{\ell^r})$
- Suponemos primero que $\ell | \# H$
- En este caso H es conjugado a un subgrupo de las triangulares superiores o contiene a $PSL_2(\mathbb{F}_{\ell^r})$
- Si $\ell \nmid \# H$, hay que estudiar la acción de H en $\mathbb{P}^1(\overline{\mathbb{F}}_\ell)$.
- Se toma el conjunto $X = \{(x, g) \in \mathbb{P}^1(\overline{\mathbb{F}}_\ell) \times H \setminus \{1\} : g(x) = x\}$

- P la proyección en la primera coordenada de X.
- H actua en P y este se separa en orbitas $P = O_1 \cup \cdots \cup O_k$
- $\#O_i = \#H/e_i$, donde e_i es el cardinal de los grupos estabilizadores de elementos de O_i
- Contando los elementos de X llegamos a

$$2(\#H - 1) = \sum_{x \in P} (\#G_x - 1)$$

- $\displaystyle\sum_{i=0}^{k} 1/e_i = k - 2 + \frac{2}{\#H}$
- Las soluciones de esta ecuación son
- Para $k = 2$, $(e_1, e_2, \#H) = (\#H, \#H, \#H)$
- Para $k = 3$, $(e_1, e_2, e_3; \#H) \in \{(2, 2, n, 2n), (2, 3, 3, 12), (2, 3, 4, 24), (2, 3, 4, 60)\}$

Lema

Sea $\mathbb{F}$ un campo finito de caracteristica ℓ impar. Si $\#\mathbb{F} \neq 5$, entonces

$$H^1(SL_2(\mathbb{F}), End^0(\mathbb{F}^2)) = 0$$

Demostración:

- Tomamos subgrupos $U \subseteq B \subseteq SL_2(\mathbb{F})$
- $H^1(G, End^0(\mathbb{F}^2)) \to H^1(B, End^0(\mathbb{F}^2))$ es inyectiva
- $H^1(B, End^0(\mathbb{F}^2)) \to H^1(U, End^0(\mathbb{F}^2))^{B/U}$ es inyectiva
- Si $\#\mathbb{F} = 3$, entonces podemos calcular directamente que $H^1(U, End^0(\mathbb{F}^2)) = 0$ usando el isomorfismo $H^1(U, End^0(\mathbb{F}^2)) \simeq \ker N/(\sigma - 1)End^0(\mathbb{F}^2)$
- En general se toman los siguientes submodulos

- $M_1 =$ matrices triangulares superiores con ceros en la diagonal
- $M_2 =$ matrices triangulares superiores
- $M_3 = End^0(\mathbb{F}^2)$
- Tomando sucesiones largas de cohomologia se ve que $H^1(U, M_3/M_2) \hookrightarrow H^1(U, M_3)$

Anexo

Sea $\sigma \in \mathrm{Gal}(\mathbb{Q}_q^{mr}/\mathbb{Q}_q^{nr})$ y $f \in \mathrm{Gal}(\mathbb{Q}_q^{mr}/\mathbb{Q}_q)$ un levantamiento del Frobenius. Como la extensión $\mathbb{Q}_q^{mr}/\mathbb{Q}_q^{nr}$ es generada por los elementos $\sqrt[n]{q}$ para $q \nmid n$, nos basta probar que $f\sigma f^{-1}(\sqrt[n]{q}) = \sigma^q(\sqrt[n]{q})$. Vemos a σ como un elemento de $\mathrm{Gal}(\mathbb{Q}_q^{nr}(\sqrt[n]{q})/\mathbb{Q}_q^{nr})$. Por teoria de Kummer

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}_q^{nr}(\sqrt[n]{q})/\mathbb{Q}_q^{nr}) &\to \mu_n \\ \eta &\mapsto \frac{\eta(\sqrt[n]{q})}{\sqrt[n]{q}} \end{aligned}$$

$$f\sigma f^{-1}(\sqrt[n]{q}) = f\sigma(\zeta_n \sqrt[n]{q}) = f(\zeta_n \sigma(\sqrt[n]{q})) = f\left(\zeta_n \sqrt[n]{q} \cdot \frac{\sigma(\sqrt[n]{q})}{\sqrt[n]{q}}\right)$$

$$= \sqrt[n]{q}\frac{\sigma^q(\sqrt[n]{q})}{\sqrt[n]{q}} = \sigma^q(\sqrt[n]{q})$$