Galois representations: Lecture 3

Shaunak Deo

Indian Institute of Science

Elliptic curves and Special values of L functions,
ICTS Bangalore
5 August, 2021

Theorem (Mazur, Ramakrishna)

If $\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ is a representation such that $\mathrm{End}_G(\bar{\rho}) = \mathbb{F}$ and G satisfies the finiteness condition (Φ_p), then there exists

- a CNL $W(\mathbb{F})$-algebra $R_{\bar{\rho}}^{\mathrm{univ}}$,
- a lift $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\mathrm{univ}})$ of $\bar{\rho}$

such that for any CNL $W(\mathbb{F})$-algebra R, the map

$$\mathrm{Hom}(R_{\bar{\rho}}^{\mathrm{univ}}, R) \to D_{\bar{\rho}}(R)$$

$$\phi \mapsto [\phi \circ \rho^{\mathrm{univ}}]$$

is a bijection.

The theorem is proved by verifying conditions of Schlessinger's criteria.
There is also an explicit construction of $R_{\bar{\rho}}^{\mathrm{univ}}$: see the article 'Explicit construction of universal deformation rings' by deSmit and Lenstra from 'Modular forms and Fermat's last theorem'.

Theorem (Mazur, Ramakrishna)

If $\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ is a representation such that $\mathrm{End}_G(\bar{\rho}) = \mathbb{F}$ and G satisfies the finiteness condition (Φ_p), then there exists

- a CNL $W(\mathbb{F})$-algebra $R^{\mathrm{univ}}_{\bar{\rho}}$,
- a lift $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R^{\mathrm{univ}}_{\bar{\rho}})$ of $\bar{\rho}$

such that for any CNL $W(\mathbb{F})$-algebra R, the map

$$\mathrm{Hom}(R^{\mathrm{univ}}_{\bar{\rho}}, R) \to D_{\bar{\rho}}(R)$$

$$\phi \mapsto [\phi \circ \rho^{\mathrm{univ}}]$$

is a bijection.

The theorem is proved by verifying conditions of Schlessinger's criteria.

There is also an explicit construction of $R^{\mathrm{univ}}_{\bar{\rho}}$: see the article 'Explicit construction of universal deformation rings' by deSmit and Lenstra from 'Modular forms and Fermat's last theorem'.

Theorem (Mazur, Ramakrishna)

If $\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ is a representation such that $\mathrm{End}_G(\bar{\rho}) = \mathbb{F}$ and G satisfies the finiteness condition (Φ_p), then there exists

- a CNL $W(\mathbb{F})$-algebra $R_{\bar{\rho}}^{\mathrm{univ}}$,
- a lift $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\mathrm{univ}})$ of $\bar{\rho}$

such that for any CNL $W(\mathbb{F})$-algebra R, the map

$$\mathrm{Hom}(R_{\bar{\rho}}^{\mathrm{univ}}, R) \to D_{\bar{\rho}}(R)$$

$$\phi \mapsto [\phi \circ \rho^{\mathrm{univ}}]$$

is a bijection.

The theorem is proved by verifying conditions of Schlessinger's criteria.

There is also an explicit construction of $R_{\bar{\rho}}^{\mathrm{univ}}$: see the article 'Explicit construction of universal deformation rings' by deSmit and Lenstra from 'Modular forms and Fermat's last theorem'.

Theorem (Mazur, Ramakrishna)

If $\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ is a representation such that $\mathrm{End}_G(\bar{\rho}) = \mathbb{F}$ and G satisfies the finiteness condition (Φ_p), then there exists

- a CNL $W(\mathbb{F})$-algebra $R^{\mathrm{univ}}_{\bar{\rho}}$,
- a lift $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R^{\mathrm{univ}}_{\bar{\rho}})$ of $\bar{\rho}$

such that for any CNL $W(\mathbb{F})$-algebra R, the map

$$\mathrm{Hom}(R^{\mathrm{univ}}_{\bar{\rho}}, R) \to D_{\bar{\rho}}(R)$$

$$\phi \mapsto [\phi \circ \rho^{\mathrm{univ}}]$$

is a bijection.

The theorem is proved by verifying conditions of Schlessinger's criteria.

There is also an explicit construction of $R^{\mathrm{univ}}_{\bar{\rho}}$: see the article 'Explicit construction of universal deformation rings' by deSmit and Lenstra from 'Modular forms and Fermat's last theorem'.

Theorem (Mazur, Ramakrishna)

If $\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ is a representation such that $\mathrm{End}_G(\bar{\rho}) = \mathbb{F}$ and G satisfies the finiteness condition (Φ_p), then there exists

- a CNL $W(\mathbb{F})$-algebra $R_{\bar{\rho}}^{\mathrm{univ}}$,
- a lift $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\mathrm{univ}})$ of $\bar{\rho}$

such that for any CNL $W(\mathbb{F})$-algebra R, the map

$$\mathrm{Hom}(R_{\bar{\rho}}^{\mathrm{univ}}, R) \to D_{\bar{\rho}}(R)$$

$$\phi \mapsto [\phi \circ \rho^{\mathrm{univ}}]$$

is a bijection.

The theorem is proved by verifying conditions of Schlessinger's criteria.

There is also an explicit construction of $R_{\bar{\rho}}^{\mathrm{univ}}$: see the article 'Explicit construction of universal deformation rings' by deSmit and Lenstra from 'Modular forms and Fermat's last theorem'.

Theorem (Mazur, Ramakrishna)

If $\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ is a representation such that $\mathrm{End}_G(\bar{\rho}) = \mathbb{F}$ and G satisfies the finiteness condition (Φ_p), then there exists

- a CNL $W(\mathbb{F})$-algebra $R_{\bar{\rho}}^{\mathrm{univ}}$,
- a lift $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\mathrm{univ}})$ of $\bar{\rho}$

such that for any CNL $W(\mathbb{F})$-algebra R, the map

$$\mathrm{Hom}(R_{\bar{\rho}}^{\mathrm{univ}}, R) \to D_{\bar{\rho}}(R)$$

$$\phi \mapsto [\phi \circ \rho^{\mathrm{univ}}]$$

is a bijection.

The theorem is proved by verifying conditions of Schlessinger's criteria.
There is also an explicit construction of $R_{\bar{\rho}}^{\mathrm{univ}}$: see the article 'Explicit construction of universal deformation rings' by deSmit and Lenstra from 'Modular forms and Fermat's last theorem'.

Universal deformation ring of a character

Let $\bar{\chi} : G \to \mathbb{F}^\times$ be a character.

Let $G^{(p)}$ be the pro-p completion of G i.e. $G^{(p)} = \varprojlim_N G/N$, where the inverse limit is taken over all closed normal subgroups N of G of finite index such that $|G/N|$ is a power of p.

Let $G^{(p),\mathrm{ab}}$ be the quotient of $G^{(p)}$ by the closure of its commutator subgroup. Since G satisfies the finiteness condition (Φ_p), it follows that $G^{(p),\mathrm{ab}}$ is a finitely generated $\mathbb{Z}_p$-module.

Let $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ be the completed group ring of $G^{(p),\mathrm{ab}}$ over $W(\mathbb{F})$. So $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] = \varprojlim_H W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$, where the inverse limit is taken over open normal subgroups H of $G^{(p),\mathrm{ab}}$ and $W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$ is the group ring of $G^{(p),\mathrm{ab}}/H$ over $W(\mathbb{F})$.

Universal deformation ring of a character

Let $\bar{\chi} : G \to \mathbb{F}^\times$ be a character.

Let $G^{(p)}$ be the pro-p completion of G i.e. $G^{(p)} = \varprojlim_N G/N$, where the inverse limit is taken over all closed normal subgroups N of G of finite index such that $|G/N|$ is a power of p.

Let $G^{(p),\text{ab}}$ be the quotient of $G^{(p)}$ by the closure of its commutator subgroup. Since G satisfies the finiteness condition (Φ_p), it follows that $G^{(p),\text{ab}}$ is a finitely generated $\mathbb{Z}_p$-module.

Let $W(\mathbb{F})[[G^{(p),\text{ab}}]]$ be the completed group ring of $G^{(p),\text{ab}}$ over $W(\mathbb{F})$. So $W(\mathbb{F})[[G^{(p),\text{ab}}]] = \varprojlim_H W(\mathbb{F})[G^{(p),\text{ab}}/H]$, where the inverse limit is taken over open normal subgroups H of $G^{(p),\text{ab}}$ and $W(\mathbb{F})[G^{(p),\text{ab}}/H]$ is the group ring of $G^{(p),\text{ab}}/H$ over $W(\mathbb{F})$.

Let $\bar{\chi} : G \to \mathbb{F}^\times$ be a character.

Let $G^{(p)}$ be the pro-p completion of G i.e. $G^{(p)} = \varprojlim_N G/N$, where the inverse limit is taken over all closed normal subgroups N of G of finite index such that $|G/N|$ is a power of p.

Let $G^{(p),\mathrm{ab}}$ be the quotient of $G^{(p)}$ by the closure of its commutator subgroup. Since G satisfies the finiteness condition (Φ_p), it follows that $G^{(p),\mathrm{ab}}$ is a finitely generated $\mathbb{Z}_p$-module.

Let $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ be the completed group ring of $G^{(p),\mathrm{ab}}$ over $W(\mathbb{F})$. So $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] = \varprojlim_H W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$, where the inverse limit is taken over open normal subgroups H of $G^{(p),\mathrm{ab}}$ and $W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$ is the group ring of $G^{(p),\mathrm{ab}}/H$ over $W(\mathbb{F})$.

Universal deformation ring of a character

Let $\bar{\chi} : G \to \mathbb{F}^\times$ be a character.

Let $G^{(p)}$ be the pro-p completion of G i.e. $G^{(p)} = \varprojlim_N G/N$, where the inverse limit is taken over all closed normal subgroups N of G of finite index such that $|G/N|$ is a power of p.

Let $G^{(p),\text{ab}}$ be the quotient of $G^{(p)}$ by the closure of its commutator subgroup. Since G satisfies the finiteness condition (Φ_p), it follows that $G^{(p),\text{ab}}$ is a finitely generated $\mathbb{Z}_p$-module.

Let $W(\mathbb{F})[[G^{(p),\text{ab}}]]$ be the completed group ring of $G^{(p),\text{ab}}$ over $W(\mathbb{F})$. So $W(\mathbb{F})[[G^{(p),\text{ab}}]] = \varprojlim_H W(\mathbb{F})[G^{(p),\text{ab}}/H]$, where the inverse limit is taken over open normal subgroups H of $G^{(p),\text{ab}}$ and $W(\mathbb{F})[G^{(p),\text{ab}}/H]$ is the group ring of $G^{(p),\text{ab}}/H$ over $W(\mathbb{F})$.

Let $\bar{\chi} : G \to \mathbb{F}^{\times}$ be a character.

Let $G^{(p)}$ be the pro-p completion of G i.e. $G^{(p)} = \varprojlim_N G/N$, where the inverse limit is taken over all closed normal subgroups N of G of finite index such that $|G/N|$ is a power of p.

Let $G^{(p),\mathrm{ab}}$ be the quotient of $G^{(p)}$ by the closure of its commutator subgroup. Since G satisfies the finiteness condition (Φ_p), it follows that $G^{(p),\mathrm{ab}}$ is a finitely generated $\mathbb{Z}_p$-module.

Let $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ be the completed group ring of $G^{(p),\mathrm{ab}}$ over $W(\mathbb{F})$. So $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] = \varprojlim_H W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$, where the inverse limit is taken over open normal subgroups H of $G^{(p),\mathrm{ab}}$ and $W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$ is the group ring of $G^{(p),\mathrm{ab}}/H$ over $W(\mathbb{F})$.

Let $\bar{\chi} : G \to \mathbb{F}^\times$ be a character.

Let $G^{(p)}$ be the pro-p completion of G i.e. $G^{(p)} = \varprojlim_N G/N$, where the inverse limit is taken over all closed normal subgroups N of G of finite index such that $|G/N|$ is a power of p.

Let $G^{(p),\mathrm{ab}}$ be the quotient of $G^{(p)}$ by the closure of its commutator subgroup. Since G satisfies the finiteness condition (Φ_p), it follows that $G^{(p),\mathrm{ab}}$ is a finitely generated $\mathbb{Z}_p$-module.

Let $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ be the completed group ring of $G^{(p),\mathrm{ab}}$ over $W(\mathbb{F})$. So $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] = \varprojlim_H W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$, where the inverse limit is taken over open normal subgroups H of $G^{(p),\mathrm{ab}}$ and $W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$ is the group ring of $G^{(p),\mathrm{ab}}/H$ over $W(\mathbb{F})$.

Let $\bar{\chi} : G \to \mathbb{F}^\times$ be a character.

Let $G^{(p)}$ be the pro-p completion of G i.e. $G^{(p)} = \varprojlim_N G/N$, where the inverse limit is taken over all closed normal subgroups N of G of finite index such that $|G/N|$ is a power of p.

Let $G^{(p),\mathrm{ab}}$ be the quotient of $G^{(p)}$ by the closure of its commutator subgroup. Since G satisfies the finiteness condition (Φ_p), it follows that $G^{(p),\mathrm{ab}}$ is a finitely generated $\mathbb{Z}_p$-module.

Let $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ be the completed group ring of $G^{(p),\mathrm{ab}}$ over $W(\mathbb{F})$. So $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] = \varprojlim_H W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$, where the inverse limit is taken over open normal subgroups H of $G^{(p),\mathrm{ab}}$ and $W(\mathbb{F})[G^{(p),\mathrm{ab}}/H]$ is the group ring of $G^{(p),\mathrm{ab}}/H$ over $W(\mathbb{F})$.

As $G^{(p),\mathrm{ab}}$ is a finitely generated $\mathbb{Z}_p$-module, $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ is a CNL $W(\mathbb{F})$-algebra.

Let $\gamma : G \to G^{(p),\mathrm{ab}}$ be the natural projection and if $u \in G^{(p),\mathrm{ab}}$, then denote by $[u]$ the corresponding element in the group ring.

We have a character

$$\eta_0 : G \to W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]^\times$$

such that $\eta_0(g) = [\gamma(g)]$.
Denote the Teichmuller lift of $\bar{\chi}$ to $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ by χ_0.

Theorem

The universal deformation ring of $\bar{\chi} : G \to \mathbb{F}^\times$ is $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ and the universal deformation of $\bar{\chi}$ is given by

$$\chi_0\eta_0 : G \to W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]^\times.$$

As $G^{(p),\mathrm{ab}}$ is a finitely generated $\mathbb{Z}_p$-module, $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ is a CNL $W(\mathbb{F})$-algebra.

Let $\gamma : G \to G^{(p),\mathrm{ab}}$ be the natural projection and if $u \in G^{(p),\mathrm{ab}}$, then denote by $[u]$ the corresponding element in the group ring.

We have a character

$$\eta_0 : G \to W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]^\times$$

such that $\eta_0(g) = [\gamma(g)]$.
Denote the Teichmuller lift of $\bar{\chi}$ to $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ by χ_0.

Theorem

The universal deformation ring of $\bar{\chi} : G \to \mathbb{F}^\times$ is $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ and the universal deformation of $\bar{\chi}$ is given by

$$\chi_0\eta_0 : G \to W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]^\times.$$

As $G^{(p),\mathrm{ab}}$ is a finitely generated $\mathbb{Z}_p$-module, $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ is a CNL $W(\mathbb{F})$-algebra.

Let $\gamma : G \to G^{(p),\mathrm{ab}}$ be the natural projection and if $u \in G^{(p),\mathrm{ab}}$, then denote by $[u]$ the corresponding element in the group ring.

We have a character

$$\eta_0 : G \to W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]^\times$$

such that $\eta_0(g) = [\gamma(g)]$.
Denote the Teichmuller lift of $\bar{\chi}$ to $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ by χ_0.

Theorem

The universal deformation ring of $\bar{\chi} : G \to \mathbb{F}^\times$ is $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ and the universal deformation of $\bar{\chi}$ is given by

$$\chi_0\eta_0 : G \to W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]^\times.$$

As $G^{(p),\text{ab}}$ is a finitely generated $\mathbb{Z}_p$-module, $W(\mathbb{F})[[G^{(p),\text{ab}}]]$ is a CNL $W(\mathbb{F})$-algebra.

Let $\gamma : G \to G^{(p),\text{ab}}$ be the natural projection and if $u \in G^{(p),\text{ab}}$, then denote by $[u]$ the corresponding element in the group ring.

We have a character

$$\eta_0 : G \to W(\mathbb{F})[[G^{(p),\text{ab}}]]^\times$$

such that $\eta_0(g) = [\gamma(g)]$.
Denote the Teichmuller lift of $\bar{\chi}$ to $W(\mathbb{F})[[G^{(p),\text{ab}}]]$ by χ_0.

Theorem

The universal deformation ring of $\bar{\chi} : G \to \mathbb{F}^\times$ is $W(\mathbb{F})[[G^{(p),\text{ab}}]]$ and the universal deformation of $\bar{\chi}$ is given by

$$\chi_0\eta_0 : G \to W(\mathbb{F})[[G^{(p),\text{ab}}]]^\times.$$

As $G^{(p),\mathrm{ab}}$ is a finitely generated $\mathbb{Z}_p$-module, $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ is a CNL $W(\mathbb{F})$-algebra.

Let $\gamma : G \to G^{(p),\mathrm{ab}}$ be the natural projection and if $u \in G^{(p),\mathrm{ab}}$, then denote by $[u]$ the corresponding element in the group ring.

We have a character

$$\eta_0 : G \to W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]^\times$$

such that $\eta_0(g) = [\gamma(g)]$.
Denote the Teichmuller lift of $\bar{\chi}$ to $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ by χ_0.

Theorem

The universal deformation ring of $\bar{\chi} : G \to \mathbb{F}^\times$ is $W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]$ and the universal deformation of $\bar{\chi}$ is given by

$$\chi_0\eta_0 : G \to W(\mathbb{F})[[G^{(p),\mathrm{ab}}]]^\times.$$

Proof of the theorem

If R is a CNL $W(\mathbb{F})$-algebra, then denote the Teichmuller lift of $\bar{\chi}$ to $R^\times$ by χ_R.

If $\chi : G \to R^\times$ is a lift of $\bar{\chi}$, then $\chi = \chi' \chi_R$ for some lift χ' of the trivial character.

So χ' takes values in $1 + m_R$ which is an abelian pro-p group. Hence, χ' factors through $G^{(p),\mathrm{ab}}$ giving a character

$$\chi'' : G^{(p),\mathrm{ab}} \to 1 + m_R.$$

So χ'' extends to a morphism $f_\chi : W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] \to R$.

Thus we have

$$\chi = f_\chi \circ \chi_0 \eta_0$$

which proves the theorem.

Proof of the theorem

If R is a CNL $W(\mathbb{F})$-algebra, then denote the Teichmuller lift of $\bar{\chi}$ to $R^\times$ by χ_R.

If $\chi : G \to R^\times$ is a lift of $\bar{\chi}$, then $\chi = \chi' \chi_R$ for some lift χ' of the trivial character.

So χ' takes values in $1 + m_R$ which is an abelian pro-p group. Hence, χ' factors through $G^{(p),\mathrm{ab}}$ giving a character

$$\chi'' : G^{(p),\mathrm{ab}} \to 1 + m_R.$$

So χ'' extends to a morphism $f_\chi : W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] \to R$.

Thus we have

$$\chi = f_\chi \circ \chi_0 \eta_0$$

which proves the theorem.

Proof of the theorem

If R is a CNL $W(\mathbb{F})$-algebra, then denote the Teichmuller lift of $\bar{\chi}$ to $R^\times$ by χ_R.

If $\chi : G \to R^\times$ is a lift of $\bar{\chi}$, then $\chi = \chi'\chi_R$ for some lift χ' of the trivial character.

So χ' takes values in $1 + m_R$ which is an abelian pro-p group. Hence, χ' factors through $G^{(p),\mathrm{ab}}$ giving a character

$$\chi'' : G^{(p),\mathrm{ab}} \to 1 + m_R.$$

So χ'' extends to a morphism $f_\chi : W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] \to R$.

Thus we have

$$\chi = f_\chi \circ \chi_0\eta_0$$

which proves the theorem.

Proof of the theorem

If R is a CNL $W(\mathbb{F})$-algebra, then denote the Teichmuller lift of $\bar{\chi}$ to $R^\times$ by χ_R.

If $\chi : G \to R^\times$ is a lift of $\bar{\chi}$, then $\chi = \chi'\chi_R$ for some lift χ' of the trivial character.

So χ' takes values in $1 + m_R$ which is an abelian pro-p group. Hence, χ' factors through $G^{(p),\mathrm{ab}}$ giving a character

$$\chi'' : G^{(p),\mathrm{ab}} \to 1 + m_R.$$

So χ'' extends to a morphism $f_\chi : W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] \to R$.

Thus we have

$$\chi = f_\chi \circ \chi_0\eta_0$$

which proves the theorem.

Proof of the theorem

If R is a CNL $W(\mathbb{F})$-algebra, then denote the Teichmuller lift of $\bar{\chi}$ to $R^\times$ by χ_R.

If $\chi : G \to R^\times$ is a lift of $\bar{\chi}$, then $\chi = \chi' \chi_R$ for some lift χ' of the trivial character.

So χ' takes values in $1 + m_R$ which is an abelian pro-p group. Hence, χ' factors through $G^{(p),\mathrm{ab}}$ giving a character

$$\chi'' : G^{(p),\mathrm{ab}} \to 1 + m_R.$$

So χ'' extends to a morphism $f_\chi : W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] \to R$.

Thus we have

$$\chi = f_\chi \circ \chi_0 \eta_0$$

which proves the theorem.

Proof of the theorem

If R is a CNL $W(\mathbb{F})$-algebra, then denote the Teichmuller lift of $\bar{\chi}$ to $R^\times$ by χ_R.

If $\chi : G \to R^\times$ is a lift of $\bar{\chi}$, then $\chi = \chi' \chi_R$ for some lift χ' of the trivial character.

So χ' takes values in $1 + m_R$ which is an abelian pro-p group. Hence, χ' factors through $G^{(p),\mathrm{ab}}$ giving a character

$$\chi'' : G^{(p),\mathrm{ab}} \to 1 + m_R.$$

So χ'' extends to a morphism $f_\chi : W(\mathbb{F})[[G^{(p),\mathrm{ab}}]] \to R$.

Thus we have

$$\chi = f_\chi \circ \chi_0 \eta_0$$

which proves the theorem.

Examples

- If $G = G_{\mathbb{Q},\{p,\infty\}}$, then $G^{(p),\text{ab}} = \mathbb{Z}_p$ and $R^{\text{univ}}_{\bar{\chi}} \simeq \mathbb{Z}_p[[T]]$.
- Suppose ℓ is a prime such that $p \mid \ell - 1$ and p^e is the highest power of p dividing $\ell - 1$.
  If $G = G_{\mathbb{Q},\{p,\ell,\infty\}}$, then $G^{(p),\text{ab}} = \mathbb{Z}_p \times (\mathbb{Z}/p^e\mathbb{Z})$ and
  $$R^{\text{univ}}_{\bar{\chi}} \simeq \frac{\mathbb{Z}_p[[T,X]]}{((1+X)^{p^e} - 1)}.$$
- In general, if S is a finite set of primes of $\mathbb{Q}$ and $G = G_{\mathbb{Q},S}$, then $G^{(p),\text{ab}} = \mathbb{Z}_p \times \prod_{i=1}^{n}(\mathbb{Z}/p^{e_i}\mathbb{Z})$ for some $n \geq 0$ and
  $$R^{\text{univ}}_{\bar{\chi}} \simeq \frac{\mathbb{Z}_p[[T,X_1,\cdots,X_n]]}{((1+X_1)^{p^{e_1}} - 1,\cdots,(1+X_n)^{p^{e_n}} - 1)}.$$

Examples

- If $G = G_{\mathbb{Q},\{p,\infty\}}$, then $G^{(p),\mathrm{ab}} = \mathbb{Z}_p$ and $R^{\mathrm{univ}}_{\bar{\chi}} \simeq \mathbb{Z}_p[[T]]$.

- Suppose ℓ is a prime such that $p \mid \ell - 1$ and p^e is the highest power of p dividing $\ell - 1$.
  If $G = G_{\mathbb{Q},\{p,\ell,\infty\}}$, then $G^{(p),\mathrm{ab}} = \mathbb{Z}_p \times (\mathbb{Z}/p^e\mathbb{Z})$ and

$$R^{\mathrm{univ}}_{\bar{\chi}} \simeq \frac{\mathbb{Z}_p[[T,X]]}{((1+X)^{p^e} - 1)}.$$

- In general, if S is a finite set of primes of $\mathbb{Q}$ and $G = G_{\mathbb{Q},S}$, then $G^{(p),\mathrm{ab}} = \mathbb{Z}_p \times \prod_{i=1}^{n} (\mathbb{Z}/p^{e_i}\mathbb{Z})$ for some $n \geq 0$ and

$$R^{\mathrm{univ}}_{\bar{\chi}} \simeq \frac{\mathbb{Z}_p[[T,X_1,\cdots,X_n]]}{((1+X_1)^{p^{e_1}} - 1, \cdots, (1+X_n)^{p^{e_n}} - 1)}.$$

Examples

- If $G = G_{\mathbb{Q},\{p,\infty\}}$, then $G^{(p),\mathrm{ab}} = \mathbb{Z}_p$ and $R^{\mathrm{univ}}_{\bar{\chi}} \simeq \mathbb{Z}_p[[T]]$.
- Suppose ℓ is a prime such that $p \mid \ell - 1$ and p^e is the highest power of p dividing $\ell - 1$.
  If $G = G_{\mathbb{Q},\{p,\ell,\infty\}}$, then $G^{(p),\mathrm{ab}} = \mathbb{Z}_p \times (\mathbb{Z}/p^e\mathbb{Z})$ and

$$R^{\mathrm{univ}}_{\bar{\chi}} \simeq \frac{\mathbb{Z}_p[[T,X]]}{((1+X)^{p^e} - 1)}.$$

- In general, if S is a finite set of primes of $\mathbb{Q}$ and $G = G_{\mathbb{Q},S}$, then $G^{(p),\mathrm{ab}} = \mathbb{Z}_p \times \prod_{i=1}^{n} (\mathbb{Z}/p^{e_i}\mathbb{Z})$ for some $n \geq 0$ and

$$R^{\mathrm{univ}}_{\bar{\chi}} \simeq \frac{\mathbb{Z}_p[[T, X_1, \cdots, X_n]]}{((1+X_1)^{p^{e_1}} - 1, \cdots, (1+X_n)^{p^{e_n}} - 1)}.$$

Examples

- If $G = G_{\mathbb{Q},\{p,\infty\}}$, then $G^{(p),\mathrm{ab}} = \mathbb{Z}_p$ and $R^{\mathrm{univ}}_{\bar{\chi}} \simeq \mathbb{Z}_p[[T]]$.
- Suppose ℓ is a prime such that $p \mid \ell - 1$ and p^e is the highest power of p dividing $\ell - 1$.
  If $G = G_{\mathbb{Q},\{p,\ell,\infty\}}$, then $G^{(p),\mathrm{ab}} = \mathbb{Z}_p \times (\mathbb{Z}/p^e\mathbb{Z})$ and

$$R^{\mathrm{univ}}_{\bar{\chi}} \simeq \frac{\mathbb{Z}_p[[T, X]]}{((1+X)^{p^e} - 1)}.$$

- In general, if S is a finite set of primes of $\mathbb{Q}$ and $G = G_{\mathbb{Q},S}$, then $G^{(p),\mathrm{ab}} = \mathbb{Z}_p \times \prod_{i=1}^{n}(\mathbb{Z}/p^{e_i}\mathbb{Z})$ for some $n \geq 0$ and

$$R^{\mathrm{univ}}_{\bar{\chi}} \simeq \frac{\mathbb{Z}_p[[T, X_1, \cdots, X_n]]}{((1+X_1)^{p^{e_1}} - 1, \cdots, (1+X_n)^{p^{e_n}} - 1)}.$$

Generators and relations

Denote the maximal ideal of $R_{\bar{\rho}}^{\text{univ}}$ by $\mathfrak{m}$ and let $r = \dim_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2)) = \dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}))$.

So, we have an exact sequence:

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

We would like to determine r and J in order to determine the structure of $R_{\bar{\rho}}^{\text{univ}}$.

Observe that $\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}) = \text{Hom}(R_{\bar{\rho}}^{\text{univ}}, \mathbb{F}[\epsilon]) = D_{\bar{\rho}}(\mathbb{F}[\epsilon])$.

G acts on $M_n(\mathbb{F})$ by conjugation by ρ i.e. action of $g \in G$ on $M \in M_n(\mathbb{F})$ is given by $g.M := \rho(g)M\rho(g)^{-1}$. We call this representation *adjoint representation of* ρ and denote it by $\text{Ad}(\rho)$.

Generators and relations

Denote the maximal ideal of $R_{\bar{\rho}}^{\text{univ}}$ by $\mathfrak{m}$ and let $r = \dim_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2)) = \dim_{\mathbb{F}}(\mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}))$.

So, we have an exact sequence:

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

We would like to determine r and J in order to determine the structure of $R_{\bar{\rho}}^{\text{univ}}$.

Observe that $\mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}) = \mathrm{Hom}(R_{\bar{\rho}}^{\text{univ}}, \mathbb{F}[\epsilon]) = D_{\bar{\rho}}(\mathbb{F}[\epsilon])$.

G acts on $M_n(\mathbb{F})$ by conjugation by ρ i.e. action of $g \in G$ on $M \in M_n(\mathbb{F})$ is given by $g.M := \rho(g)M\rho(g)^{-1}$. We call this representation *adjoint representation of* ρ and denote it by $\mathrm{Ad}(\rho)$.

Generators and relations

Denote the maximal ideal of $R_{\bar{\rho}}^{\text{univ}}$ by $\mathfrak{m}$ and let $r = \dim_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2)) = \dim_{\mathbb{F}}(\mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}))$.

So, we have an exact sequence:

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

We would like to determine r and J in order to determine the structure of $R_{\bar{\rho}}^{\text{univ}}$.

Observe that $\mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}) = \mathrm{Hom}(R_{\bar{\rho}}^{\text{univ}}, \mathbb{F}[\epsilon]) = D_{\bar{\rho}}(\mathbb{F}[\epsilon])$.

G acts on $M_n(\mathbb{F})$ by conjugation by ρ i.e. action of $g \in G$ on $M \in M_n(\mathbb{F})$ is given by $g.M := \rho(g)M\rho(g)^{-1}$. We call this representation *adjoint representation of* ρ and denote it by $\mathrm{Ad}(\rho)$.

Generators and relations

Denote the maximal ideal of $R_{\bar{\rho}}^{\text{univ}}$ by $\mathfrak{m}$ and let $r = \dim_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2)) = \dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}))$.

So, we have an exact sequence:

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

We would like to determine r and J in order to determine the structure of $R_{\bar{\rho}}^{\text{univ}}$.

Observe that $\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}) = \text{Hom}(R_{\bar{\rho}}^{\text{univ}}, \mathbb{F}[\epsilon]) = D_{\bar{\rho}}(\mathbb{F}[\epsilon])$.

G acts on $M_n(\mathbb{F})$ by conjugation by ρ i.e. action of $g \in G$ on $M \in M_n(\mathbb{F})$ is given by $g.M := \rho(g)M\rho(g)^{-1}$. We call this representation *adjoint representation of* ρ and denote it by $\text{Ad}(\rho)$.

Generators and relations

Denote the maximal ideal of $R_{\bar{\rho}}^{\text{univ}}$ by $\mathfrak{m}$ and let $r = \dim_{\mathbb{F}}(\mathfrak{m}/(p,\mathfrak{m}^2)) = \dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p,\mathfrak{m}^2),\mathbb{F}))$.

So, we have an exact sequence:

$$0 \to J \to W(\mathbb{F})[[X_1,\cdots,X_r]] \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

We would like to determine r and J in order to determine the structure of $R_{\bar{\rho}}^{\text{univ}}$.

Observe that $\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p,\mathfrak{m}^2),\mathbb{F}) = \text{Hom}(R_{\bar{\rho}}^{\text{univ}},\mathbb{F}[\epsilon]) = D_{\bar{\rho}}(\mathbb{F}[\epsilon])$.

G acts on $M_n(\mathbb{F})$ by conjugation by ρ i.e. action of $g \in G$ on $M \in M_n(\mathbb{F})$ is given by $g.M := \rho(g)M\rho(g)^{-1}$. We call this representation *adjoint representation of* ρ and denote it by $\text{Ad}(\rho)$.

Generators and relations

Denote the maximal ideal of $R_{\bar{\rho}}^{\text{univ}}$ by $\mathfrak{m}$ and let $r = \dim_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2)) = \dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}))$.

So, we have an exact sequence:

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

We would like to determine r and J in order to determine the structure of $R_{\bar{\rho}}^{\text{univ}}$.

Observe that $\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}) = \text{Hom}(R_{\bar{\rho}}^{\text{univ}}, \mathbb{F}[\epsilon]) = D_{\bar{\rho}}(\mathbb{F}[\epsilon])$.

G acts on $M_n(\mathbb{F})$ by conjugation by ρ i.e. action of $g \in G$ on $M \in M_n(\mathbb{F})$ is given by $g.M := \rho(g)M\rho(g)^{-1}$. We call this representation *adjoint representation of* ρ and denote it by $\text{Ad}(\rho)$.

Generators and relations

Denote the maximal ideal of $R_{\bar{\rho}}^{\text{univ}}$ by $\mathfrak{m}$ and let $r = \dim_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2)) = \dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}))$.

So, we have an exact sequence:

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

We would like to determine r and J in order to determine the structure of $R_{\bar{\rho}}^{\text{univ}}$.

Observe that $\text{Hom}_{\mathbb{F}}(\mathfrak{m}/(p, \mathfrak{m}^2), \mathbb{F}) = \text{Hom}(R_{\bar{\rho}}^{\text{univ}}, \mathbb{F}[\epsilon]) = D_{\bar{\rho}}(\mathbb{F}[\epsilon])$.

G acts on $M_n(\mathbb{F})$ by conjugation by ρ i.e. action of $g \in G$ on $M \in M_n(\mathbb{F})$ is given by $g.M := \rho(g)M\rho(g)^{-1}$. We call this representation *adjoint representation of* ρ and denote it by $\text{Ad}(\rho)$.

Let $\rho : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be a set-theoretic lift of $\bar{\rho}$. Then there exists a function $f_\rho : G \to M_n(\mathbb{F})$ such that $\rho(g) = (1 + \epsilon f_\rho(g))\bar{\rho}(g)$.

Now ρ is a representation if and only if $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$.

Now $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$ if and only if

$$f_\rho(gg') = f_\rho(g) + \bar{\rho}(g) f_\rho(g') \bar{\rho}(g)^{-1} \text{ for all } g, g' \in G.$$

So ρ is a representation if and only if f_ρ is a 1-cocyle taking values in $\mathrm{Ad}(\bar{\rho})$.

Let $\rho, \rho' : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be two lifts of $\bar{\rho}$. They are equivalent if and only if there exists an $M \in M_n(\mathbb{F})$ such that

$$(Id + \epsilon M)\rho(Id - \epsilon M) = \rho'.$$

Let $\rho : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be a set-theoretic lift of $\bar{\rho}$. Then there exists a function $f_\rho : G \to M_n(\mathbb{F})$ such that $\rho(g) = (1 + \epsilon f_\rho(g))\bar{\rho}(g)$.

Now ρ is a representation if and only if $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$.

Now $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$ if and only if

$$f_\rho(gg') = f_\rho(g) + \bar{\rho}(g) f_\rho(g') \bar{\rho}(g)^{-1} \text{ for all } g, g' \in G.$$

So ρ is a representation if and only if f_ρ is a 1-cocyle taking values in $\mathrm{Ad}(\bar{\rho})$.

Let $\rho, \rho' : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be two lifts of $\bar{\rho}$. They are equivalent if and only if there exists an $M \in M_n(\mathbb{F})$ such that

$$(Id + \epsilon M)\rho(Id - \epsilon M) = \rho'.$$

Let $\rho : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be a set-theoretic lift of $\bar{\rho}$. Then there exists a function $f_\rho : G \to M_n(\mathbb{F})$ such that $\rho(g) = (1 + \epsilon f_\rho(g))\bar{\rho}(g)$.

Now ρ is a representation if and only if $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$.

Now $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$ if and only if

$$f_\rho(gg') = f_\rho(g) + \bar{\rho}(g) f_\rho(g') \bar{\rho}(g)^{-1} \text{ for all } g, g' \in G.$$

So ρ is a representation if and only if f_ρ is a 1-cocyle taking values in $\mathrm{Ad}(\bar{\rho})$.

Let $\rho, \rho' : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be two lifts of $\bar{\rho}$. They are equivalent if and only if there exists an $M \in M_n(\mathbb{F})$ such that

$$(Id + \epsilon M)\rho(Id - \epsilon M) = \rho'.$$

Let $\rho : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be a set-theoretic lift of $\bar{\rho}$. Then there exists a function $f_\rho : G \to M_n(\mathbb{F})$ such that $\rho(g) = (1 + \epsilon f_\rho(g))\bar{\rho}(g)$.

Now ρ is a representation if and only if $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$.

Now $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$ if and only if

$$f_\rho(gg') = f_\rho(g) + \bar{\rho}(g) f_\rho(g')\bar{\rho}(g)^{-1} \text{ for all } g, g' \in G.$$

So ρ is a representation if and only if f_ρ is a 1-cocyle taking values in $\mathrm{Ad}(\bar{\rho})$.

Let $\rho, \rho' : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be two lifts of $\bar{\rho}$. They are equivalent if and only if there exists an $M \in M_n(\mathbb{F})$ such that

$$(Id + \epsilon M)\rho(Id - \epsilon M) = \rho'.$$

Let $\rho : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be a set-theoretic lift of $\bar{\rho}$. Then there exists a function $f_\rho : G \to M_n(\mathbb{F})$ such that $\rho(g) = (1 + \epsilon f_\rho(g))\bar{\rho}(g)$.

Now ρ is a representation if and only if $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$.

Now $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$ if and only if

$$f_\rho(gg') = f_\rho(g) + \bar{\rho}(g) f_\rho(g')\bar{\rho}(g)^{-1} \text{ for all } g, g' \in G.$$

So ρ is a representation if and only if f_ρ is a 1-cocyle taking values in $\mathrm{Ad}(\bar{\rho})$.

Let $\rho, \rho' : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be two lifts of $\bar{\rho}$. They are equivalent if and only if there exists an $M \in M_n(\mathbb{F})$ such that

$$(Id + \epsilon M)\rho(Id - \epsilon M) = \rho'.$$

Let $\rho : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be a set-theoretic lift of $\bar{\rho}$. Then there exists a function $f_\rho : G \to M_n(\mathbb{F})$ such that $\rho(g) = (1 + \epsilon f_\rho(g))\bar{\rho}(g)$.

Now ρ is a representation if and only if $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$.

Now $\rho(gg') = \rho(g)\rho(g')$ for all $g, g' \in G$ if and only if

$$f_\rho(gg') = f_\rho(g) + \bar{\rho}(g) f_\rho(g') \bar{\rho}(g)^{-1} \text{ for all } g, g' \in G.$$

So ρ is a representation if and only if f_ρ is a 1-cocyle taking values in $\mathrm{Ad}(\bar{\rho})$.

Let $\rho, \rho' : G \to \mathrm{GL}_n(\mathbb{F}[\epsilon])$ be two lifts of $\bar{\rho}$. They are equivalent if and only if there exists an $M \in M_n(\mathbb{F})$ such that

$$(Id + \epsilon M)\rho(Id - \epsilon M) = \rho'.$$

So if ρ and ρ' are equivalent, then

$$f_{\rho'}(g) = f_\rho(g) + M - \bar{\rho}(g) M \bar{\rho}(g)^{-1}$$

i.e. f_ρ and $f_{\rho'}$ differ by a coboundary.

On the other hand if f_ρ and $f_{\rho'}$ differ by a coboundary i.e. if there exists an $N \in M_n(\mathbb{F})$ such that

$$f_\rho(g) - f_{\rho'}(g) = \bar{\rho}(g) N \bar{\rho}(g)^{-1} - N,$$

then $(Id + \epsilon N)\rho(Id - \epsilon N) = \rho'$ which means that ρ and ρ' are equivalent.

This gives an isomorphism of $\mathbb{F}$-vector spaces between $D_{\bar{\rho}}(\mathbb{F}[\epsilon])$ and $H^1(G, \mathrm{Ad}(\bar{\rho}))$. Hence, it follows that

$$r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho}))).$$

So if ρ and ρ' are equivalent, then

$$f_{\rho'}(g) = f_\rho(g) + M - \bar{\rho}(g)M\bar{\rho}(g)^{-1}$$

i.e. f_ρ and $f_{\rho'}$ differ by a coboundary.

On the other hand if f_ρ and $f_{\rho'}$ differ by a coboundary i.e. if there exists an $N \in M_n(\mathbb{F})$ such that

$$f_\rho(g) - f_{\rho'}(g) = \bar{\rho}(g)N\bar{\rho}(g)^{-1} - N,$$

then $(Id + \epsilon N)\rho(Id - \epsilon N) = \rho'$ which means that ρ and ρ' are equivalent.

This gives an isomorphism of $\mathbb{F}$-vector spaces between $D_{\bar{\rho}}(\mathbb{F}[\epsilon])$ and $H^1(G, \mathrm{Ad}(\bar{\rho}))$. Hence, it follows that

$$r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho}))).$$

So if ρ and ρ' are equivalent, then

$$f_{\rho'}(g) = f_{\rho}(g) + M - \bar{\rho}(g)M\bar{\rho}(g)^{-1}$$

i.e. f_ρ and $f_{\rho'}$ differ by a coboundary.

On the other hand if f_ρ and $f_{\rho'}$ differ by a coboundary i.e. if there exists an $N \in M_n(\mathbb{F})$ such that

$$f_{\rho}(g) - f_{\rho'}(g) = \bar{\rho}(g)N\bar{\rho}(g)^{-1} - N,$$

then $(Id + \epsilon N)\rho(Id - \epsilon N) = \rho'$ which means that ρ and ρ' are equivalent.

This gives an isomorphism of $\mathbb{F}$-vector spaces between $D_{\bar{\rho}}(\mathbb{F}[\epsilon])$ and $H^1(G, \mathrm{Ad}(\bar{\rho}))$. Hence, it follows that

$$r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho}))).$$

So if ρ and ρ' are equivalent, then

$$f_{\rho'}(g) = f_{\rho}(g) + M - \bar{\rho}(g)M\bar{\rho}(g)^{-1}$$

i.e. f_{ρ} and $f_{\rho'}$ differ by a coboundary.

On the other hand if f_{ρ} and $f_{\rho'}$ differ by a coboundary i.e. if there exists an $N \in M_n(\mathbb{F})$ such that

$$f_{\rho}(g) - f_{\rho'}(g) = \bar{\rho}(g)N\bar{\rho}(g)^{-1} - N,$$

then $(Id + \epsilon N)\rho(Id - \epsilon N) = \rho'$ which means that ρ and ρ' are equivalent.

This gives an isomorphism of $\mathbb{F}$-vector spaces between $D_{\bar{\rho}}(\mathbb{F}[\epsilon])$ and $H^1(G, \mathrm{Ad}(\bar{\rho}))$. Hence, it follows that

$$r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho}))).$$

So if ρ and ρ' are equivalent, then

$$f_{\rho'}(g) = f_\rho(g) + M - \bar{\rho}(g)M\bar{\rho}(g)^{-1}$$

i.e. f_ρ and $f_{\rho'}$ differ by a coboundary.

On the other hand if f_ρ and $f_{\rho'}$ differ by a coboundary i.e. if there exists an $N \in M_n(\mathbb{F})$ such that

$$f_\rho(g) - f_{\rho'}(g) = \bar{\rho}(g)N\bar{\rho}(g)^{-1} - N,$$

then $(Id + \epsilon N)\rho(Id - \epsilon N) = \rho'$ which means that ρ and ρ' are equivalent.

This gives an isomorphism of $\mathbb{F}$-vector spaces between $D_{\bar{\rho}}(\mathbb{F}[\epsilon])$ and $H^1(G, \mathrm{Ad}(\bar{\rho}))$. Hence, it follows that

$$r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho}))).$$

So if ρ and ρ' are equivalent, then

$$f_{\rho'}(g) = f_\rho(g) + M - \bar{\rho}(g) M \bar{\rho}(g)^{-1}$$

i.e. f_ρ and $f_{\rho'}$ differ by a coboundary.

On the other hand if f_ρ and $f_{\rho'}$ differ by a coboundary i.e. if there exists an $N \in M_n(\mathbb{F})$ such that

$$f_\rho(g) - f_{\rho'}(g) = \bar{\rho}(g) N \bar{\rho}(g)^{-1} - N,$$

then $(Id + \epsilon N)\rho(Id - \epsilon N) = \rho'$ which means that ρ and ρ' are equivalent.

This gives an isomorphism of $\mathbb{F}$-vector spaces between $D_{\bar{\rho}}(\mathbb{F}[\epsilon])$ and $H^1(G, \mathrm{Ad}(\bar{\rho}))$. Hence, it follows that

$$r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho}))).$$

So if ρ and ρ' are equivalent, then

$$f_{\rho'}(g) = f_\rho(g) + M - \bar{\rho}(g)M\bar{\rho}(g)^{-1}$$

i.e. f_ρ and $f_{\rho'}$ differ by a coboundary.

On the other hand if f_ρ and $f_{\rho'}$ differ by a coboundary i.e. if there exists an $N \in M_n(\mathbb{F})$ such that

$$f_\rho(g) - f_{\rho'}(g) = \bar{\rho}(g)N\bar{\rho}(g)^{-1} - N,$$

then $(Id + \epsilon N)\rho(Id - \epsilon N) = \rho'$ which means that ρ and ρ' are equivalent.

This gives an isomorphism of $\mathbb{F}$-vector spaces between $D_{\bar{\rho}}(\mathbb{F}[\epsilon])$ and $H^1(G, \mathrm{Ad}(\bar{\rho}))$. Hence, it follows that

$$r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho}))).$$

So if ρ and ρ' are equivalent, then

$$f_{\rho'}(g) = f_\rho(g) + M - \bar{\rho}(g) M \bar{\rho}(g)^{-1}$$

i.e. f_ρ and $f_{\rho'}$ differ by a coboundary.

On the other hand if f_ρ and $f_{\rho'}$ differ by a coboundary i.e. if there exists an $N \in M_n(\mathbb{F})$ such that

$$f_\rho(g) - f_{\rho'}(g) = \bar{\rho}(g) N \bar{\rho}(g)^{-1} - N,$$

then $(Id + \epsilon N)\rho(Id - \epsilon N) = \rho'$ which means that ρ and ρ' are equivalent.

This gives an isomorphism of $\mathbb{F}$-vector spaces between $D_{\bar{\rho}}(\mathbb{F}[\epsilon])$ and $H^1(G, \mathrm{Ad}(\bar{\rho}))$. Hence, it follows that

$$r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho}))).$$

Denote $W(\mathbb{F})[[X_1, \cdots, X_r]]$ by R and its maximal ideal by m_R. The exact sequence above gives an exact sequence

$$0 \to J/m_RJ \to R/m_RJ \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

If γ is a set theoretic lift of $\rho^{\text{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\text{univ}})$ to $\mathrm{GL}_n(R/m_RJ)$, then it is easy to verify that the function

$$d : G \times G \to M_n(J/m_RJ) = \mathrm{Ad}(\bar{\rho}) \otimes J/m_RJ$$

given by

$$d(g_1, g_2) = \gamma(g_1g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} - Id$$

is a 2-cocycle with values in $\mathrm{Ad}(\bar{\rho}) \otimes J/m_RJ$.

Replacing γ by a different lift changes this cocycle by a coboundary. Hence, this gives a cohomology class

$$\mathcal{O}(\rho^{\text{univ}}) \in H^2(G, \mathrm{Ad}(\bar{\rho})) \otimes J/m_RJ.$$

Denote $W(\mathbb{F})[[X_1, \cdots, X_r]]$ by R and its maximal ideal by m_R. The exact sequence above gives an exact sequence

$$0 \to J/m_RJ \to R/m_RJ \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

If γ is a set theoretic lift of $\rho^{\text{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\text{univ}})$ to $\mathrm{GL}_n(R/m_RJ)$, then it is easy to verify that the function

$$d : G \times G \to M_n(J/m_RJ) = \mathrm{Ad}(\bar{\rho}) \otimes J/m_RJ$$

given by

$$d(g_1, g_2) = \gamma(g_1g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} - Id$$

is a 2-cocycle with values in $\mathrm{Ad}(\bar{\rho}) \otimes J/m_RJ$.

Replacing γ by a different lift changes this cocycle by a coboundary. Hence, this gives a cohomology class

$$\mathcal{O}(\rho^{\text{univ}}) \in H^2(G, \mathrm{Ad}(\bar{\rho})) \otimes J/m_RJ.$$

Denote $W(\mathbb{F})[[X_1, \cdots, X_r]]$ by R and its maximal ideal by m_R. The exact sequence above gives an exact sequence

$$0 \to J/m_RJ \to R/m_RJ \to R_{\bar{\rho}}^{\mathrm{univ}} \to 0.$$

If γ is a set theoretic lift of $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\mathrm{univ}})$ to $\mathrm{GL}_n(R/m_RJ)$, then it is easy to verify that the function

$$d : G \times G \to M_n(J/m_RJ) = \mathrm{Ad}(\bar{\rho}) \otimes J/m_RJ$$

given by

$$d(g_1, g_2) = \gamma(g_1g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} - Id$$

is a 2-cocycle with values in $\mathrm{Ad}(\bar{\rho}) \otimes J/m_RJ$.

Replacing γ by a different lift changes this cocycle by a coboundary. Hence, this gives a cohomology class

$$\mathcal{O}(\rho^{\mathrm{univ}}) \in H^2(G, \mathrm{Ad}(\bar{\rho})) \otimes J/m_RJ.$$

Denote $W(\mathbb{F})[[X_1, \cdots, X_r]]$ by R and its maximal ideal by m_R. The exact sequence above gives an exact sequence

$$0 \to J/m_RJ \to R/m_RJ \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

If γ is a set theoretic lift of $\rho^{\text{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\text{univ}})$ to $\mathrm{GL}_n(R/m_RJ)$, then it is easy to verify that the function

$$d : G \times G \to M_n(J/m_RJ) = \mathrm{Ad}(\bar{\rho}) \otimes J/m_RJ$$

given by

$$d(g_1, g_2) = \gamma(g_1 g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} - Id$$

is a 2-cocycle with values in $\mathrm{Ad}(\bar{\rho}) \otimes J/m_RJ$.

Replacing γ by a different lift changes this cocycle by a coboundary. Hence, this gives a cohomology class

$$\mathcal{O}(\rho^{\text{univ}}) \in H^2(G, \mathrm{Ad}(\bar{\rho})) \otimes J/m_RJ.$$

Denote $W(\mathbb{F})[[X_1, \cdots, X_r]]$ by R and its maximal ideal by m_R. The exact sequence above gives an exact sequence

$$0 \to J/m_R J \to R/m_R J \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

If γ is a set theoretic lift of $\rho^{\text{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\text{univ}})$ to $\mathrm{GL}_n(R/m_R J)$, then it is easy to verify that the function

$$d : G \times G \to M_n(J/m_R J) = \mathrm{Ad}(\bar{\rho}) \otimes J/m_R J$$

given by

$$d(g_1, g_2) = \gamma(g_1 g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} - Id$$

is a 2-cocycle with values in $\mathrm{Ad}(\bar{\rho}) \otimes J/m_R J$.

Replacing γ by a different lift changes this cocycle by a coboundary. Hence, this gives a cohomology class

$$\mathcal{O}(\rho^{\text{univ}}) \in H^2(G, \mathrm{Ad}(\bar{\rho})) \otimes J/m_R J.$$

Denote $W(\mathbb{F})[[X_1, \cdots, X_r]]$ by R and its maximal ideal by m_R. The exact sequence above gives an exact sequence

$$0 \to J/m_R J \to R/m_R J \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

If γ is a set theoretic lift of $\rho^{\text{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\text{univ}})$ to $\mathrm{GL}_n(R/m_R J)$, then it is easy to verify that the function

$$d : G \times G \to M_n(J/m_R J) = \mathrm{Ad}(\bar{\rho}) \otimes J/m_R J$$

given by

$$d(g_1, g_2) = \gamma(g_1 g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} - Id$$

is a 2-cocycle with values in $\mathrm{Ad}(\bar{\rho}) \otimes J/m_R J$.

Replacing γ by a different lift changes this cocycle by a coboundary. Hence, this gives a cohomology class

$$\mathcal{O}(\rho^{\text{univ}}) \in H^2(G, \mathrm{Ad}(\bar{\rho})) \otimes J/m_R J.$$

Denote $W(\mathbb{F})[[X_1, \cdots, X_r]]$ by R and its maximal ideal by m_R. The exact sequence above gives an exact sequence

$$0 \to J/m_R J \to R/m_R J \to R_{\bar{\rho}}^{\mathrm{univ}} \to 0.$$

If γ is a set theoretic lift of $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R_{\bar{\rho}}^{\mathrm{univ}})$ to $\mathrm{GL}_n(R/m_R J)$, then it is easy to verify that the function

$$d : G \times G \to M_n(J/m_R J) = \mathrm{Ad}(\bar{\rho}) \otimes J/m_R J$$

given by

$$d(g_1, g_2) = \gamma(g_1 g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} - Id$$

is a 2-cocycle with values in $\mathrm{Ad}(\bar{\rho}) \otimes J/m_R J$.

Replacing γ by a different lift changes this cocycle by a coboundary. Hence, this gives a cohomology class

$$\mathcal{O}(\rho^{\mathrm{univ}}) \in H^2(G, \mathrm{Ad}(\bar{\rho})) \otimes J/m_R J.$$

Consider the $\mathbb{F}$-linear map

$$\phi : \mathrm{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F}) \to H^2(G, \mathrm{Ad}(\bar{\rho}))$$

given by $\phi(f) = (1 \otimes f)(\mathcal{O}(\rho^{\mathrm{univ}}))$.

Suppose ϕ is not injective and let $f \in \ker(\phi)$. Let R' be the quotient of R by $\ker(f)$ and I be the quotient of $J/m_R J$ by $\ker(f)$.

So $I \simeq \mathbb{F}$ and this gives us an exact sequence:

$$0 \to I \to R' \to R_{\bar{\rho}}^{\mathrm{univ}} \to 0.$$

Denote the map $R' \to R_{\bar{\rho}}^{\mathrm{univ}}$ by ψ_2. As $f \in \ker(\phi)$, the obstruction to lifting ρ^{univ} to R' vanishes.
Hence, there is a deformation $\rho' : G \to \mathrm{GL}_n(R')$ of $\bar{\rho}$ to R' such that ρ' also lifts ρ^{univ}.

Consider the $\mathbb{F}$-linear map

$$\phi : \mathrm{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F}) \to H^2(G, \mathrm{Ad}(\bar{\rho}))$$

given by $\phi(f) = (1 \otimes f)(\mathcal{O}(\rho^{\mathrm{univ}}))$.

Suppose ϕ is not injective and let $f \in \ker(\phi)$. Let R' be the quotient of R by $\ker(f)$ and I be the quotient of $J/m_R J$ by $\ker(f)$.

So $I \simeq \mathbb{F}$ and this gives us an exact sequence:

$$0 \to I \to R' \to R_{\bar{\rho}}^{\mathrm{univ}} \to 0.$$

Denote the map $R' \to R_{\bar{\rho}}^{\mathrm{univ}}$ by ψ_2. As $f \in \ker(\phi)$, the obstruction to lifting ρ^{univ} to R' vanishes.
Hence, there is a deformation $\rho' : G \to \mathrm{GL}_n(R')$ of $\bar{\rho}$ to R' such that ρ' also lifts ρ^{univ}.

Consider the $\mathbb{F}$-linear map

$$\phi : \mathrm{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F}) \to H^2(G, \mathrm{Ad}(\bar{\rho}))$$

given by $\phi(f) = (1 \otimes f)(\mathcal{O}(\rho^{\text{univ}}))$.

Suppose ϕ is not injective and let $f \in \ker(\phi)$. Let R' be the quotient of R by $\ker(f)$ and I be the quotient of $J/m_R J$ by $\ker(f)$.

So $I \simeq \mathbb{F}$ and this gives us an exact sequence:

$$0 \to I \to R' \to R_{\bar{\rho}}^{\text{univ}} \to 0.$$

Denote the map $R' \to R_{\bar{\rho}}^{\text{univ}}$ by ψ_2. As $f \in \ker(\phi)$, the obstruction to lifting ρ^{univ} to R' vanishes.
Hence, there is a deformation $\rho' : G \to \mathrm{GL}_n(R')$ of $\bar{\rho}$ to R' such that ρ' also lifts ρ^{univ}.

Consider the $\mathbb{F}$-linear map

$$\phi : \mathrm{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F}) \to H^2(G, \mathrm{Ad}(\bar{\rho}))$$

given by $\phi(f) = (1 \otimes f)(\mathcal{O}(\rho^{\mathrm{univ}}))$.

Suppose ϕ is not injective and let $f \in \ker(\phi)$. Let R' be the quotient of R by $\ker(f)$ and I be the quotient of $J/m_R J$ by $\ker(f)$.

So $I \simeq \mathbb{F}$ and this gives us an exact sequence:

$$0 \to I \to R' \to R_{\bar{\rho}}^{\mathrm{univ}} \to 0.$$

Denote the map $R' \to R_{\bar{\rho}}^{\mathrm{univ}}$ by ψ_2. As $f \in \ker(\phi)$, the obstruction to lifting ρ^{univ} to R' vanishes.
Hence, there is a deformation $\rho' : G \to \mathrm{GL}_n(R')$ of $\bar{\rho}$ to R' such that ρ' also lifts ρ^{univ}.

Consider the $\mathbb{F}$-linear map

$$\phi : \mathrm{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F}) \to H^2(G, \mathrm{Ad}(\bar{\rho}))$$

given by $\phi(f) = (1 \otimes f)(\mathcal{O}(\rho^{\mathrm{univ}}))$.

Suppose ϕ is not injective and let $f \in \ker(\phi)$. Let R' be the quotient of R by $\ker(f)$ and I be the quotient of $J/m_R J$ by $\ker(f)$.

So $I \simeq \mathbb{F}$ and this gives us an exact sequence:

$$0 \to I \to R' \to R^{\mathrm{univ}}_{\bar{\rho}} \to 0.$$

Denote the map $R' \to R^{\mathrm{univ}}_{\bar{\rho}}$ by ψ_2. As $f \in \ker(\phi)$, the obstruction to lifting ρ^{univ} to R' vanishes.
Hence, there is a deformation $\rho' : G \to \mathrm{GL}_n(R')$ of $\bar{\rho}$ to R' such that ρ' also lifts ρ^{univ}.

Consider the $\mathbb{F}$-linear map

$$\phi : \mathrm{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F}) \to H^2(G, \mathrm{Ad}(\bar{\rho}))$$

given by $\phi(f) = (1 \otimes f)(\mathcal{O}(\rho^{\mathrm{univ}}))$.

Suppose ϕ is not injective and let $f \in \ker(\phi)$. Let R' be the quotient of R by $\ker(f)$ and I be the quotient of $J/m_R J$ by $\ker(f)$.

So $I \simeq \mathbb{F}$ and this gives us an exact sequence:

$$0 \to I \to R' \to R_{\bar{\rho}}^{\mathrm{univ}} \to 0.$$

Denote the map $R' \to R_{\bar{\rho}}^{\mathrm{univ}}$ by ψ_2. As $f \in \ker(\phi)$, the obstruction to lifting ρ^{univ} to R' vanishes.
Hence, there is a deformation $\rho' : G \to \mathrm{GL}_n(R')$ of $\bar{\rho}$ to R' such that ρ' also lifts ρ^{univ}.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\mathrm{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\mathrm{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho})))$.

So the universal property implies that ρ' is induced by a homomorphism $\psi_1 : R_{\bar{\rho}}^{\text{univ}} \to R'$.

As $\psi_2 \circ \psi_1 \circ \rho^{\text{univ}} = \rho^{\text{univ}}$, the universal property implies that $\psi_2 \circ \psi_1$ is identity and hence, the exact sequence above splits.

Since $\ker(\psi_2) \subset (p, m_{R'}^2)$ and $\psi_2 \circ \psi_1$ is identity, it follows that ψ_1 induces an isomorphism on mod p tangent spaces of $R_{\bar{\rho}}^{\text{univ}}$ and R'. Hence, ψ_1 is surjective.

As $\psi_2 \circ \psi_1$ is identity, it follows that ψ_2 is injective. This contradicts the fact that $\ker(\psi_2) = I \simeq \mathbb{F} \neq 0$.

Therefore, the map ϕ is injective. Injectivity of ϕ implies that

$$\dim_{\mathbb{F}}(\text{Hom}_{\mathbb{F}}(J/m_R J, \mathbb{F})) \leq \dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho}))).$$

So, by Nakayama's lemma, the minimal number of generators of J is at most $\dim_{\mathbb{F}}(H^2(G, \text{Ad}(\bar{\rho})))$.

In conclusion, we have:

Theorem

Let $r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho})))$ and $s = \dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho})))$. Then we have a presentation

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R^{\mathrm{univ}}_{\bar{\rho}},$$

such that the minimal number of generators of J is at most s.

If $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F})$ is an odd representation, then global Euler characteristic formula implies that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) - \dim_{\mathbb{F}}(H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

So we get that the Krull dimension of $R^{\mathrm{univ}}_{\bar{\rho}}$ is at least 4 if $\bar{\rho}$ is odd.

The representation $\bar{\rho}$ is called *unobstructed* if $H^2(G, \mathrm{Ad}(\bar{\rho})) = 0$. If $\bar{\rho}$ is unobstructed, then $R^{\mathrm{univ}}_{\bar{\rho}} \simeq W(\mathbb{F})[[X_1, \cdots, X_r]]$.

In conclusion, we have:

Theorem

Let $r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho})))$ and $s = \dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho})))$. Then we have a presentation

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\mathrm{univ}},$$

such that the minimal number of generators of J is at most s.

If $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F})$ is an odd representation, then global Euler characteristic formula implies that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) - \dim_{\mathbb{F}}(H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

So we get that the Krull dimension of $R_{\bar{\rho}}^{\mathrm{univ}}$ is at least 4 if $\bar{\rho}$ is odd.

The representation $\bar{\rho}$ is called *unobstructed* if $H^2(G, \mathrm{Ad}(\bar{\rho})) = 0$. If $\bar{\rho}$ is unobstructed, then $R_{\bar{\rho}}^{\mathrm{univ}} \simeq W(\mathbb{F})[[X_1, \cdots, X_r]]$.

In conclusion, we have:

Theorem

Let $r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho})))$ and $s = \dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho})))$. Then we have a presentation

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\mathrm{univ}},$$

such that the minimal number of generators of J is at most s.

If $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F})$ is an odd representation, then global Euler characteristic formula implies that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) - \dim_{\mathbb{F}}(H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

So we get that the Krull dimension of $R_{\bar{\rho}}^{\mathrm{univ}}$ is at least 4 if $\bar{\rho}$ is odd.

The representation $\bar{\rho}$ is called *unobstructed* if $H^2(G, \mathrm{Ad}(\bar{\rho})) = 0$. If $\bar{\rho}$ is unobstructed, then $R_{\bar{\rho}}^{\mathrm{univ}} \simeq W(\mathbb{F})[[X_1, \cdots, X_r]]$.

In conclusion, we have:

Theorem

Let $r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho})))$ and $s = \dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho})))$. Then we have a presentation

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\mathrm{univ}},$$

such that the minimal number of generators of J is at most s.

If $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F})$ is an odd representation, then global Euler characteristic formula implies that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) - \dim_{\mathbb{F}}(H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

So we get that the Krull dimension of $R_{\bar{\rho}}^{\mathrm{univ}}$ is at least 4 if $\bar{\rho}$ is odd.

The representation $\bar{\rho}$ is called *unobstructed* if $H^2(G, \mathrm{Ad}(\bar{\rho})) = 0$.
If $\bar{\rho}$ is unobstructed, then $R_{\bar{\rho}}^{\mathrm{univ}} \simeq W(\mathbb{F})[[X_1, \cdots, X_r]]$.

In conclusion, we have:

Theorem

Let $r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho})))$ and $s = \dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho})))$. Then we have a presentation

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R^{\mathrm{univ}}_{\bar{\rho}},$$

such that the minimal number of generators of J is at most s.

If $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F})$ is an odd representation, then global Euler characteristic formula implies that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) - \dim_{\mathbb{F}}(H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

So we get that the Krull dimension of $R^{\mathrm{univ}}_{\bar{\rho}}$ is at least 4 if $\bar{\rho}$ is odd.

The representation $\bar{\rho}$ is called *unobstructed* if $H^2(G, \mathrm{Ad}(\bar{\rho})) = 0$.
If $\bar{\rho}$ is unobstructed, then $R^{\mathrm{univ}}_{\bar{\rho}} \simeq W(\mathbb{F})[[X_1, \cdots, X_r]]$.

In conclusion, we have:

Theorem

Let $r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho})))$ and $s = \dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho})))$. Then we have a presentation

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\text{univ}},$$

such that the minimal number of generators of J is at most s.

If $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F})$ is an odd representation, then global Euler characteristic formula implies that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) - \dim_{\mathbb{F}}(H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

So we get that the Krull dimension of $R_{\bar{\rho}}^{\text{univ}}$ is at least 4 if $\bar{\rho}$ is odd.

The representation $\bar{\rho}$ is called *unobstructed* if $H^2(G, \mathrm{Ad}(\bar{\rho})) = 0$.
If $\bar{\rho}$ is unobstructed, then $R_{\bar{\rho}}^{\text{univ}} \simeq W(\mathbb{F})[[X_1, \cdots, X_r]]$.

In conclusion, we have:

Theorem

Let $r = \dim_{\mathbb{F}}(H^1(G, \mathrm{Ad}(\bar{\rho})))$ and $s = \dim_{\mathbb{F}}(H^2(G, \mathrm{Ad}(\bar{\rho})))$. Then we have a presentation

$$0 \to J \to W(\mathbb{F})[[X_1, \cdots, X_r]] \to R_{\bar{\rho}}^{\mathrm{univ}},$$

such that the minimal number of generators of J is at most s.

If $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F})$ is an odd representation, then global Euler characteristic formula implies that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) - \dim_{\mathbb{F}}(H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

So we get that the Krull dimension of $R_{\bar{\rho}}^{\mathrm{univ}}$ is at least 4 if $\bar{\rho}$ is odd.

The representation $\bar{\rho}$ is called *unobstructed* if $H^2(G, \mathrm{Ad}(\bar{\rho})) = 0$. If $\bar{\rho}$ is unobstructed, then $R_{\bar{\rho}}^{\mathrm{univ}} \simeq W(\mathbb{F})[[X_1, \cdots, X_r]]$.

Neat S_3 representations

Let $f(X) = X^3 + aX + 1 \in \mathbb{Q}[X]$ be a polynomial such that $27 + 4a^3$ is a prime p. Some examples of such primes are 23, 31, 59 and 283.

Let L be the splitting field of $f(X)$ over $\mathbb{Q}$. Since the discriminant of $f(X)$ is $-p$, $\mathbb{Q}(\sqrt{-p}) \subset L$.
So L is a totally complex extension of $\mathbb{Q}$ and $G_0 := \mathrm{Gal}(L/\mathbb{Q}) = S_3$.
Note that the extension $L/\mathbb{Q}$ is unramified outside p and ∞.

Fix an embedding $i : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ and let

$$\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation obtained by composing i with the natural surjective map $G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{Gal}(L/\mathbb{Q})$.

We call such a $\bar{\rho}$ a *neat* S_3 representation.

Neat S_3 representations

Let $f(X) = X^3 + aX + 1 \in \mathbb{Q}[X]$ be a polynomial such that $27 + 4a^3$ is a prime p. Some examples of such primes are 23, 31, 59 and 283.

Let L be the splitting field of $f(X)$ over $\mathbb{Q}$. Since the discriminant of $f(X)$ is $-p$, $\mathbb{Q}(\sqrt{-p}) \subset L$.
So L is a totally complex extension of $\mathbb{Q}$ and $G_0 := \mathrm{Gal}(L/\mathbb{Q}) = S_3$.
Note that the extension $L/\mathbb{Q}$ is unramified outside p and ∞.

Fix an embedding $i : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ and let

$$\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation obtained by composing i with the natural surjective map $G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{Gal}(L/\mathbb{Q})$.

We call such a $\bar{\rho}$ a *neat* S_3 representation.

Neat S_3 representations

Let $f(X) = X^3 + aX + 1 \in \mathbb{Q}[X]$ be a polynomial such that $27 + 4a^3$ is a prime p. Some examples of such primes are 23, 31, 59 and 283.

Let L be the splitting field of $f(X)$ over $\mathbb{Q}$. Since the discriminant of $f(X)$ is $-p$, $\mathbb{Q}(\sqrt{-p}) \subset L$.
So L is a totally complex extension of $\mathbb{Q}$ and $G_0 := \mathrm{Gal}(L/\mathbb{Q}) = S_3$.
Note that the extension $L/\mathbb{Q}$ is unramified outside p and ∞.

Fix an embedding $i : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ and let

$$\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation obtained by composing i with the natural surjective map $G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{Gal}(L/\mathbb{Q})$.

We call such a $\bar{\rho}$ a *neat* S_3 representation.

Neat S_3 representations

Let $f(X) = X^3 + aX + 1 \in \mathbb{Q}[X]$ be a polynomial such that $27 + 4a^3$ is a prime p. Some examples of such primes are 23, 31, 59 and 283.

Let L be the splitting field of $f(X)$ over $\mathbb{Q}$. Since the discriminant of $f(X)$ is $-p$, $\mathbb{Q}(\sqrt{-p}) \subset L$.
So L is a totally complex extension of $\mathbb{Q}$ and $G_0 := \mathrm{Gal}(L/\mathbb{Q}) = S_3$.
Note that the extension $L/\mathbb{Q}$ is unramified outside p and ∞.

Fix an embedding $i : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ and let

$$\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation obtained by composing i with the natural surjective map $G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{Gal}(L/\mathbb{Q})$.

We call such a $\bar{\rho}$ a *neat* S_3 representation.

Neat S_3 representations

Let $f(X) = X^3 + aX + 1 \in \mathbb{Q}[X]$ be a polynomial such that $27 + 4a^3$ is a prime p. Some examples of such primes are 23, 31, 59 and 283.

Let L be the splitting field of $f(X)$ over $\mathbb{Q}$. Since the discriminant of $f(X)$ is $-p$, $\mathbb{Q}(\sqrt{-p}) \subset L$.
So L is a totally complex extension of $\mathbb{Q}$ and $G_0 := \mathrm{Gal}(L/\mathbb{Q}) = S_3$.
Note that the extension $L/\mathbb{Q}$ is unramified outside p and ∞.

Fix an embedding $i : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ and let

$$\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation obtained by composing i with the natural surjective map $G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{Gal}(L/\mathbb{Q})$.

We call such a $\bar{\rho}$ a *neat* S_3 representation.

Neat S_3 representations

Let $f(X) = X^3 + aX + 1 \in \mathbb{Q}[X]$ be a polynomial such that $27 + 4a^3$ is a prime p. Some examples of such primes are 23, 31, 59 and 283.

Let L be the splitting field of $f(X)$ over $\mathbb{Q}$. Since the discriminant of $f(X)$ is $-p$, $\mathbb{Q}(\sqrt{-p}) \subset L$.
So L is a totally complex extension of $\mathbb{Q}$ and $G_0 := \text{Gal}(L/\mathbb{Q}) = S_3$.
Note that the extension $L/\mathbb{Q}$ is unramified outside p and ∞.

Fix an embedding $i : \text{Gal}(L/\mathbb{Q}) \to \text{GL}_2(\mathbb{F}_p)$ and let

$$\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \text{GL}_2(\mathbb{F}_p)$$

be the representation obtained by composing i with the natural surjective map $G_{\mathbb{Q},\{p,\infty\}} \to \text{Gal}(L/\mathbb{Q})$.

We call such a $\bar{\rho}$ a *neat* S_3 representation.

Neat S_3 representations

Let $f(X) = X^3 + aX + 1 \in \mathbb{Q}[X]$ be a polynomial such that $27 + 4a^3$ is a prime p. Some examples of such primes are 23, 31, 59 and 283.

Let L be the splitting field of $f(X)$ over $\mathbb{Q}$. Since the discriminant of $f(X)$ is $-p$, $\mathbb{Q}(\sqrt{-p}) \subset L$.
So L is a totally complex extension of $\mathbb{Q}$ and $G_0 := \mathrm{Gal}(L/\mathbb{Q}) = S_3$.
Note that the extension $L/\mathbb{Q}$ is unramified outside p and ∞.

Fix an embedding $i : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ and let

$$\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation obtained by composing i with the natural surjective map $G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{Gal}(L/\mathbb{Q})$.

We call such a $\bar{\rho}$ a *neat* S_3 representation.

Neat S_3 representations

Let $f(X) = X^3 + aX + 1 \in \mathbb{Q}[X]$ be a polynomial such that $27 + 4a^3$ is a prime p. Some examples of such primes are 23, 31, 59 and 283.

Let L be the splitting field of $f(X)$ over $\mathbb{Q}$. Since the discriminant of $f(X)$ is $-p$, $\mathbb{Q}(\sqrt{-p}) \subset L$.
So L is a totally complex extension of $\mathbb{Q}$ and $G_0 := \mathrm{Gal}(L/\mathbb{Q}) = S_3$.
Note that the extension $L/\mathbb{Q}$ is unramified outside p and ∞.

Fix an embedding $i : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ and let

$$\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation obtained by composing i with the natural surjective map $G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{Gal}(L/\mathbb{Q})$.

We call such a $\bar{\rho}$ a *neat* S_3 representation.

Theorem (Mazur)

If $\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is a neat S_3 representation, then $R^{\mathrm{univ}}_{\bar{\rho}} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

By global Euler characteristic formula, it suffices to prove that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},\{p,\infty\}}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

Now as a G_0-representation, $\mathrm{Ad}(\bar{\rho}) = 1 \oplus \epsilon \oplus \bar{\rho}'$, where ϵ is the non-trivial 1-dimensional sign representation and $\bar{\rho}'$ is the irreducible representation given by the embedding i above. So the dual of $\mathrm{Ad}(\bar{\rho})$ is itself.

By inflation-restriction sequence, this amounts to proving that $\dim_{\mathbb{F}}(H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0}) = 3$, where S' is the set of places of L lying above $\{p, \infty\}$ and $G_0 = \mathrm{Gal}(L/\mathbb{Q})$.

Since G_L acts trivially on $\mathrm{Ad}(\bar{\rho})$ and $\mathrm{Ad}(\bar{\rho})$ is self-dual, we get that

$$H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0} = \mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho})).$$

Theorem (Mazur)

If $\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is a neat S_3 representation, then $R^{\mathrm{univ}}_{\bar{\rho}} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

By global Euler characteristic formula, it suffices to prove that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},\{p,\infty\}}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

Now as a G_0-representation, $\mathrm{Ad}(\bar{\rho}) = 1 \oplus \epsilon \oplus \bar{\rho}'$, where ϵ is the non-trivial 1-dimensional sign representation and $\bar{\rho}'$ is the irreducible representation given by the embedding i above. So the dual of $\mathrm{Ad}(\bar{\rho})$ is itself.

By inflation-restriction sequence, this amounts to proving that $\dim_{\mathbb{F}}(H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0}) = 3$, where S' is the set of places of L lying above $\{p, \infty\}$ and $G_0 = \mathrm{Gal}(L/\mathbb{Q})$.

Since G_L acts trivially on $\mathrm{Ad}(\bar{\rho})$ and $\mathrm{Ad}(\bar{\rho})$ is self-dual, we get that

$$H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0} = \mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho})).$$

Theorem (Mazur)

If $\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is a neat S_3 representation, then $R_{\bar{\rho}}^{\mathrm{univ}} \simeq \mathbb{Z}_p[[X,Y,Z]]$.

By global Euler characteristic formula, it suffices to prove that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},\{p,\infty\}}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

Now as a G_0-representation, $\mathrm{Ad}(\bar{\rho}) = 1 \oplus \epsilon \oplus \bar{\rho}'$, where ϵ is the non-trivial 1-dimensional sign representation and $\bar{\rho}'$ is the irreducible representation given by the embedding i above. So the dual of $\mathrm{Ad}(\bar{\rho})$ is itself.

By inflation-restriction sequence, this amounts to proving that $\dim_{\mathbb{F}}(H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0}) = 3$, where S' is the set of places of L lying above $\{p,\infty\}$ and $G_0 = \mathrm{Gal}(L/\mathbb{Q})$.

Since G_L acts trivially on $\mathrm{Ad}(\bar{\rho})$ and $\mathrm{Ad}(\bar{\rho})$ is self-dual, we get that

$$H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0} = \mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho})).$$

Theorem (Mazur)

If $\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is a neat S_3 representation, then $R_{\bar{\rho}}^{\mathrm{univ}} \simeq \mathbb{Z}_p[[X,Y,Z]]$.

By global Euler characteristic formula, it suffices to prove that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},\{p,\infty\}}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

Now as a G_0-representation, $\mathrm{Ad}(\bar{\rho}) = 1 \oplus \epsilon \oplus \bar{\rho}'$, where ϵ is the non-trivial 1-dimensional sign representation and $\bar{\rho}'$ is the irreducible representation given by the embedding i above. So the dual of $\mathrm{Ad}(\bar{\rho})$ is itself.

By inflation-restriction sequence, this amounts to proving that $\dim_{\mathbb{F}}(H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0}) = 3$, where S' is the set of places of L lying above $\{p,\infty\}$ and $G_0 = \mathrm{Gal}(L/\mathbb{Q})$.

Since G_L acts trivially on $\mathrm{Ad}(\bar{\rho})$ and $\mathrm{Ad}(\bar{\rho})$ is self-dual, we get that

$$H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0} = \mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho})).$$

Theorem (Mazur)

If $\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is a neat S_3 representation, then $R^{\mathrm{univ}}_{\bar{\rho}} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

By global Euler characteristic formula, it suffices to prove that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},\{p,\infty\}}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

Now as a G_0-representation, $\mathrm{Ad}(\bar{\rho}) = 1 \oplus \epsilon \oplus \bar{\rho}'$, where ϵ is the non-trivial 1-dimensional sign representation and $\bar{\rho}'$ is the irreducible representation given by the embedding i above. So the dual of $\mathrm{Ad}(\bar{\rho})$ is itself.

By inflation-restriction sequence, this amounts to proving that $\dim_{\mathbb{F}}(H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0}) = 3$, where S' is the set of places of L lying above $\{p, \infty\}$ and $G_0 = \mathrm{Gal}(L/\mathbb{Q})$.

Since G_L acts trivially on $\mathrm{Ad}(\bar{\rho})$ and $\mathrm{Ad}(\bar{\rho})$ is self-dual, we get that

$$H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0} = \mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho})).$$

Theorem (Mazur)

If $\bar{\rho} : G_{\mathbb{Q},\{p,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is a neat S_3 representation, then $R^{\mathrm{univ}}_{\bar{\rho}} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

By global Euler characteristic formula, it suffices to prove that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},\{p,\infty\}}, \mathrm{Ad}(\bar{\rho}))) = 3.$$

Now as a G_0-representation, $\mathrm{Ad}(\bar{\rho}) = 1 \oplus \epsilon \oplus \bar{\rho}'$, where ϵ is the non-trivial 1-dimensional sign representation and $\bar{\rho}'$ is the irreducible representation given by the embedding i above. So the dual of $\mathrm{Ad}(\bar{\rho})$ is itself.

By inflation-restriction sequence, this amounts to proving that $\dim_{\mathbb{F}}(H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0}) = 3$, where S' is the set of places of L lying above $\{p, \infty\}$ and $G_0 = \mathrm{Gal}(L/\mathbb{Q})$.

Since G_L acts trivially on $\mathrm{Ad}(\bar{\rho})$ and $\mathrm{Ad}(\bar{\rho})$ is self-dual, we get that

$$H^1(G_{L,S'}, \mathrm{Ad}(\bar{\rho}))^{G_0} = \mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho})).$$

The class number of L is not divisible by p. So by class field theory, we have an exact sequence of $\mathbb{F}_p[G_0]$-modules

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \to \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \to G_{L,S'}^{\mathrm{ab},(p)}/(G_{L,S'}^{\mathrm{ab},(p)})^p \to 0.$$

Mazur proves that the first map in the exact sequence above is injective.

Now for every $\mathfrak{p} \mid p$, $L_\mathfrak{p}^\times$ does not contain a non-trivial p-th root of unity.
So as G_0-representations,

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \simeq \bar{\rho}' \quad \text{and} \quad \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \simeq 1 \oplus \epsilon \oplus \bar{\rho}'^{\oplus 2}.$$

Combining all this, we get that

$$\dim_\mathbb{F}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = \dim_\mathbb{F}(\mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho}))) = 3.$$

The class number of L is not divisible by p. So by class field theory, we have an exact sequence of $\mathbb{F}_p[G_0]$-modules

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \to \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \to G_{L,S'}^{\mathrm{ab},(p)}/(G_{L,S'}^{\mathrm{ab},(p)})^p \to 0.$$

Mazur proves that the first map in the exact sequence above is injective.

Now for every $\mathfrak{p} \mid p$, $L_\mathfrak{p}^\times$ does not contain a non-trivial p-th root of unity.
So as G_0-representations,

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \simeq \bar{\rho}' \quad \text{and} \quad \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \simeq 1 \oplus \epsilon \oplus \bar{\rho}'^{\oplus 2}.$$

Combining all this, we get that

$$\dim_\mathbb{F}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = \dim_\mathbb{F}(\mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho}))) = 3.$$

The class number of L is not divisible by p. So by class field theory, we have an exact sequence of $\mathbb{F}_p[G_0]$-modules

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \to \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \to G_{L,S'}^{\mathrm{ab},(p)}/(G_{L,S'}^{\mathrm{ab},(p)})^p \to 0.$$

Mazur proves that the first map in the exact sequence above is injective.

Now for every $\mathfrak{p} \mid p$, $L_\mathfrak{p}^\times$ does not contain a non-trivial p-th root of unity.

So as G_0-representations,

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \simeq \bar{\rho}' \quad \text{and} \quad \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \simeq 1 \oplus \epsilon \oplus \bar{\rho}'^{\oplus 2}.$$

Combining all this, we get that

$$\dim_{\mathbb{F}}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = \dim_{\mathbb{F}}(\mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho}))) = 3.$$

The class number of L is not divisible by p. So by class field theory, we have an exact sequence of $\mathbb{F}_p[G_0]$-modules

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \to \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \to G_{L,S'}^{\mathrm{ab},(p)}/(G_{L,S'}^{\mathrm{ab},(p)})^p \to 0.$$

Mazur proves that the first map in the exact sequence above is injective.

Now for every $\mathfrak{p} \mid p$, $L_\mathfrak{p}^\times$ does not contain a non-trivial p-th root of unity.

So as G_0-representations,

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \simeq \bar{\rho}' \quad \text{and} \quad \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \simeq 1 \oplus \epsilon \oplus \bar{\rho}'^{\oplus 2}.$$

Combining all this, we get that

$$\dim_\mathbb{F}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = \dim_\mathbb{F}(\mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho}))) = 3.$$

The class number of L is not divisible by p. So by class field theory, we have an exact sequence of $\mathbb{F}_p[G_0]$-modules

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \to \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \to G_{L,S'}^{\mathrm{ab},(p)}/(G_{L,S'}^{\mathrm{ab},(p)})^p \to 0.$$

Mazur proves that the first map in the exact sequence above is injective.

Now for every $\mathfrak{p} \mid p$, $L_\mathfrak{p}^\times$ does not contain a non-trivial p-th root of unity.
So as G_0-representations,

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \simeq \bar{\rho}' \quad \text{and} \quad \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \simeq 1 \oplus \epsilon \oplus \bar{\rho}'^{\oplus 2}.$$

Combining all this, we get that

$$\dim_\mathbb{F}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = \dim_\mathbb{F}(\mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho}))) = 3.$$

The class number of L is not divisible by p. So by class field theory, we have an exact sequence of $\mathbb{F}_p[G_0]$-modules

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \to \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \to G_{L,S'}^{\mathrm{ab},(p)}/(G_{L,S'}^{\mathrm{ab},(p)})^p \to 0.$$

Mazur proves that the first map in the exact sequence above is injective.

Now for every $\mathfrak{p} \mid p$, $L_\mathfrak{p}^\times$ does not contain a non-trivial p-th root of unity.
So as G_0-representations,

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \simeq \bar{\rho}' \quad \text{and} \quad \prod_{\mathfrak{p}|p} \mathcal{O}_{L_\mathfrak{p}}^\times/(\mathcal{O}_{L_\mathfrak{p}}^\times)^p \simeq 1 \oplus \epsilon \oplus \bar{\rho}'^{\oplus 2}.$$

Combining all this, we get that

$$\dim_\mathbb{F}(H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\bar{\rho}))) = \dim_\mathbb{F}(\mathrm{Hom}_{G_0}(\mathrm{Hom}(G_{L,S'}, \mathbb{F}_p), \mathrm{Ad}(\bar{\rho}))) = 3.$$

Suppose $p = 23$ and $\bar{\rho} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_{23})$ is the neat S_3-representation coming from the splitting field of the polynomial $X^3 - X + 1$.

$\bar{\rho}$ is the reduction of the 23-adic Galois representation $\rho_{23} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{Z}_{23})$ attached to Δ modulo 23.

Example from Chenevier's notes: Let E be the elliptic curve given by

$$y^2 + xy + y = x^3 - x^2 - x.$$

E has good reduction outside 17.

Let $S = \{5, 17, \infty\}$ and $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_5)$ be the representation arising from the action of $G_{\mathbb{Q},S}$ on $E[5]$.

Then $\bar{\rho}$ is surjective and moreover, $\bar{\rho}$ is unobstructed.

Suppose $p = 23$ and $\bar{\rho} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_{23})$ is the neat S_3-representation coming from the splitting field of the polynomial $X^3 - X + 1$.

$\bar{\rho}$ is the reduction of the 23-adic Galois representation $\rho_{23} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{Z}_{23})$ attached to Δ modulo 23.

Example from Chenevier's notes: Let E be the elliptic curve given by

$$y^2 + xy + y = x^3 - x^2 - x.$$

E has good reduction outside 17.

Let $S = \{5, 17, \infty\}$ and $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_5)$ be the representation arising from the action of $G_{\mathbb{Q},S}$ on $E[5]$.

Then $\bar{\rho}$ is surjective and moreover, $\bar{\rho}$ is unobstructed.

Suppose $p = 23$ and $\bar{\rho} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_{23})$ is the neat S_3-representation coming from the splitting field of the polynomial $X^3 - X + 1$.
$\bar{\rho}$ is the reduction of the 23-adic Galois representation $\rho_{23} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{Z}_{23})$ attached to Δ modulo 23.

Example from Chenevier's notes: Let E be the elliptic curve given by

$$y^2 + xy + y = x^3 - x^2 - x.$$

E has good reduction outside 17.

Let $S = \{5, 17, \infty\}$ and $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_5)$ be the representation arising from the action of $G_{\mathbb{Q},S}$ on $E[5]$.

Then $\bar{\rho}$ is surjective and moreover, $\bar{\rho}$ is unobstructed.

Suppose $p = 23$ and $\bar{\rho} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_{23})$ is the neat S_3-representation coming from the splitting field of the polynomial $X^3 - X + 1$.
$\bar{\rho}$ is the reduction of the 23-adic Galois representation $\rho_{23} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{Z}_{23})$ attached to Δ modulo 23.

Example from Chenevier's notes: Let E be the elliptic curve given by

$$y^2 + xy + y = x^3 - x^2 - x.$$

E has good reduction outside 17.

Let $S = \{5, 17, \infty\}$ and $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_5)$ be the representation arising from the action of $G_{\mathbb{Q},S}$ on $E[5]$.

Then $\bar{\rho}$ is surjective and moreover, $\bar{\rho}$ is unobstructed.

Suppose $p = 23$ and $\bar{\rho} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_{23})$ is the neat S_3-representation coming from the splitting field of the polynomial $X^3 - X + 1$.
$\bar{\rho}$ is the reduction of the 23-adic Galois representation $\rho_{23} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{Z}_{23})$ attached to Δ modulo 23.

Example from Chenevier's notes: Let E be the elliptic curve given by

$$y^2 + xy + y = x^3 - x^2 - x.$$

E has good reduction outside 17.

Let $S = \{5, 17, \infty\}$ and $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_5)$ be the representation arising from the action of $G_{\mathbb{Q},S}$ on $E[5]$.

Then $\bar{\rho}$ is surjective and moreover, $\bar{\rho}$ is unobstructed.

Suppose $p = 23$ and $\bar{\rho} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_{23})$ is the neat S_3-representation coming from the splitting field of the polynomial $X^3 - X + 1$.

$\bar{\rho}$ is the reduction of the 23-adic Galois representation $\rho_{23} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{Z}_{23})$ attached to Δ modulo 23.

Example from Chenevier's notes: Let E be the elliptic curve given by

$$y^2 + xy + y = x^3 - x^2 - x.$$

E has good reduction outside 17.

Let $S = \{5, 17, \infty\}$ and $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_5)$ be the representation arising from the action of $G_{\mathbb{Q},S}$ on $E[5]$.

Then $\bar{\rho}$ is surjective and moreover, $\bar{\rho}$ is unobstructed.

Suppose E is an elliptic curve over $\mathbb{Q}$, $p \geq 5$ and E has good reduction at p.

Let $S = \{\ell \mid E \text{ has bad reduction at } \ell\} \cup \{p, \infty\}$ and

$$\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation given by the action of $G_{\mathbb{Q},S}$ on $E[p]$.

Theorem (Flach)

Suppose we are in the setup as above and suppose the following hypotheses hold:

- $\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective,
- For every $q \in S$, $H^0(\mathbb{Q}_q, E[p] \otimes E[p]) = 0$,
- $p \nmid \Omega^{-1} L(\mathrm{Sym}^2(E), 2)$, where Ω is a transcendental period.

Then $R^{\mathrm{univ}}_{\bar{\rho}_p} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

A similar result for CM elliptic curves has been proved by Boston–Ullom.

Suppose E is an elliptic curve over $\mathbb{Q}$, $p \geq 5$ and E has good reduction at p.
Let $S = \{\ell \mid E \text{ has bad reduction at } \ell\} \cup \{p, \infty\}$ and

$$\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation given by the action of $G_{\mathbb{Q},S}$ on $E[p]$.

Theorem (Flach)

Suppose we are in the setup as above and suppose the following hypotheses hold:

- $\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective,
- For every $q \in S$, $H^0(\mathbb{Q}_q, E[p] \otimes E[p]) = 0$,
- $p \nmid \Omega^{-1} L(\mathrm{Sym}^2(E), 2)$, where Ω is a transcendental period.

Then $R^{\mathrm{univ}}_{\bar{\rho}_p} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

A similar result for CM elliptic curves has been proved by Boston–Ullom.

Suppose E is an elliptic curve over $\mathbb{Q}$, $p \geq 5$ and E has good reduction at p.
Let $S = \{\ell \mid E \text{ has bad reduction at } \ell\} \cup \{p, \infty\}$ and

$$\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation given by the action of $G_{\mathbb{Q},S}$ on $E[p]$.

Theorem (Flach)

Suppose we are in the setup as above and suppose the following hypotheses hold:

- $\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective,
- For every $q \in S$, $H^0(\mathbb{Q}_q, E[p] \otimes E[p]) = 0$,
- $p \nmid \Omega^{-1} L(\mathrm{Sym}^2(E), 2)$, where Ω is a transcendental period.

Then $R^{\mathrm{univ}}_{\bar{\rho}_p} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

A similar result for CM elliptic curves has been proved by Boston–Ullom.

Suppose E is an elliptic curve over $\mathbb{Q}$, $p \geq 5$ and E has good reduction at p.
Let $S = \{\ell \mid E \text{ has bad reduction at } \ell\} \cup \{p, \infty\}$ and

$$\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation given by the action of $G_{\mathbb{Q},S}$ on $E[p]$.

Theorem (Flach)

Suppose we are in the setup as above and suppose the following hypotheses hold:

- $\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective,
- For every $q \in S$, $H^0(\mathbb{Q}_q, E[p] \otimes E[p]) = 0$,
- $p \nmid \Omega^{-1} L(\mathrm{Sym}^2(E), 2)$, where Ω is a transcendental period.

Then $R^{\mathrm{univ}}_{\bar{\rho}_p} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

A similar result for CM elliptic curves has been proved by Boston–Ullom.

Suppose E is an elliptic curve over $\mathbb{Q}$, $p \geq 5$ and E has good reduction at p.
Let $S = \{\ell \mid E \text{ has bad reduction at } \ell\} \cup \{p, \infty\}$ and

$$\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation given by the action of $G_{\mathbb{Q},S}$ on $E[p]$.

Theorem (Flach)

Suppose we are in the setup as above and suppose the following hypotheses hold:

- $\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective,
- For every $q \in S$, $H^0(\mathbb{Q}_q, E[p] \otimes E[p]) = 0$,
- $p \nmid \Omega^{-1} L(\mathrm{Sym}^2(E), 2)$, where Ω is a transcendental period.

Then $R^{\mathrm{univ}}_{\bar{\rho}_p} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

A similar result for CM elliptic curves has been proved by Boston–Ullom.

Suppose E is an elliptic curve over $\mathbb{Q}$, $p \geq 5$ and E has good reduction at p.
Let $S = \{\ell \mid E \text{ has bad reduction at } \ell\} \cup \{p, \infty\}$ and

$$\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation given by the action of $G_{\mathbb{Q},S}$ on $E[p]$.

Theorem (Flach)

Suppose we are in the setup as above and suppose the following hypotheses hold:

- $\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective,
- For every $q \in S$, $H^0(\mathbb{Q}_q, E[p] \otimes E[p]) = 0$,
- $p \nmid \Omega^{-1} L(\mathrm{Sym}^2(E), 2)$, where Ω is a transcendental period.

Then $R^{\mathrm{univ}}_{\bar{\rho}_p} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

A similar result for CM elliptic curves has been proved by Boston–Ullom.

Suppose E is an elliptic curve over $\mathbb{Q}$, $p \geq 5$ and E has good reduction at p.
Let $S = \{\ell \mid E \text{ has bad reduction at } \ell\} \cup \{p, \infty\}$ and

$$\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation given by the action of $G_{\mathbb{Q},S}$ on $E[p]$.

Theorem (Flach)

Suppose we are in the setup as above and suppose the following hypotheses hold:

- $\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective,
- For every $q \in S$, $H^0(\mathbb{Q}_q, E[p] \otimes E[p]) = 0$,
- $p \nmid \Omega^{-1} L(\mathrm{Sym}^2(E), 2)$, where Ω is a transcendental period.

Then $R^{\mathrm{univ}}_{\bar{\rho}_p} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

A similar result for CM elliptic curves has been proved by Boston–Ullom.

Suppose E is an elliptic curve over $\mathbb{Q}$, $p \geq 5$ and E has good reduction at p.
Let $S = \{\ell \mid E \text{ has bad reduction at } \ell\} \cup \{p, \infty\}$ and

$$\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$$

be the representation given by the action of $G_{\mathbb{Q},S}$ on $E[p]$.

Theorem (Flach)

Suppose we are in the setup as above and suppose the following hypotheses hold:

- $\bar{\rho}_p : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective,
- For every $q \in S$, $H^0(\mathbb{Q}_q, E[p] \otimes E[p]) = 0$,
- $p \nmid \Omega^{-1} L(\mathrm{Sym}^2(E), 2)$, where Ω is a transcendental period.

Then $R^{\mathrm{univ}}_{\bar{\rho}_p} \simeq \mathbb{Z}_p[[X, Y, Z]]$.

A similar result for CM elliptic curves has been proved by Boston–Ullom.