1 Explicit deformation spaces (Alex)

1.1 Set-up

References, Gouvea chapter 5. [1, 24, 25].

We have so far discussed the existence of the universal deformation and some of its properties, now we want to really get our hands on this functor. We do this by relating the residual representation to field extensions.

As usual, $S \ni p, \infty$ a finite set of places and $\mathbf{Q}_S/\mathbf{Q}$ the maximal extension unramified outside of S. Let

$$\Pi = G_{\mathbf{Q},S} = \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q}).$$

We assume that $C(\bar{\rho}) = k$ (or that $\bar{\rho}$ is absolutely irreducible).

We can let $\Pi_0 = \ker(\bar{\rho}) \subseteq \Pi$ and $K = \ker(\Pi_0)$ so that we have

$$\begin{tikzcd}
\mathbf{Q}_S \arrow[d, dash, "\Pi_0"'] \arrow[dd, dash, bend left, "G_{\mathbf{Q},S}"] \\
K \arrow[d, dash, "\Pi/\Pi_0 \to \mathrm{im}\,\bar{\rho}"'] \\
\mathbf{Q}
\end{tikzcd}$$

Figure 1.1

If

$$\rho \colon \Pi \to \mathrm{GL}_n(\mathcal{R})$$

is the universal deformation of $\bar{\rho}$ then we can consider

$$\Gamma_n(\mathcal{R}) = \ker(\mathrm{GL}_n(\mathcal{R}) \to \mathrm{GL}_n(k))$$

which has the property that

$$\rho(\gamma) \in \Gamma_n(\mathcal{R}),\ \forall \gamma \in \Pi_0.$$

So we can restrict

$$\rho|_{\Pi_0} \colon \Pi_0 \to \Gamma_n(\mathcal{R}).$$

Proposition 1.2 *Group theoretically $\Gamma_n(\mathcal{R})$ is a pro-p-group.*

Proof. This is as

$$\mathcal{R} = \varprojlim_k \mathcal{R}/\mathfrak{m}^k$$

so

$$\Gamma_n(\mathcal{R}) = \varprojlim_k \Gamma_n(\mathcal{R}/\mathfrak{m}^k)$$

now we can induct using that

$$\Gamma_n(R/\mathfrak{m}) = \Gamma_n(k) = \{1\}$$

is trivially a p-group.

Now each transition map

$$\Gamma_n(R/\mathfrak{m}^k) \to \Gamma_n(R/\mathfrak{m}^{k-1})$$

has image a p-group and the kernel is

$$G_r \coloneqq 1 + M_n(\mathfrak{m}^{k-1}/\mathfrak{m}^k)$$

which is isomorphic to
$$M_n(\mathfrak{m}^{k-1}/\mathfrak{m}^k).$$
■

So in fact the map
$$\rho|_{\Pi_0}\colon \Pi_0 \to \Gamma_n(\mathcal{R})$$
factors through the maximal (continuous) pro-p quotient of Π_0, call this P.

This quotient is the galois group of, L, the maximal pro-p-extension of K, which is unramified above all primes of K above S, call this set S_1.
$$P = \mathrm{Gal}(L/K).$$

Now letting
$$\tilde{\Pi} = \mathrm{Gal}(L/\mathbf{Q})$$
we have the exact sequence
$$0 \to P \to \tilde{\Pi} \to \mathrm{im}(\bar{\rho}) \to 0.$$

So to understand deformations of $\bar{\rho}$ we have to understand maps
$$P \to \Gamma_n(R)$$
and then how to extend to $\tilde{\Pi}$ so that they deform $\bar{\rho}$.

In order to get a handle on this we make the following assumption:

Definition 1.3 Tame residual representations. A residual representation is **tame** if
$$p \nmid \# \mathrm{im}(\bar{\rho}).$$
◊

The significance of this is that
$$\tilde{\Pi}$$
is a profinite group with a normal p-Sylow subgroup P.

1.2 Some group theory

Now we recall / learn for the first time some group theoretic results that will be our workhorses today.

If G is a profinite group with a normal Sylow p-subgroup P of finite index that is topologically finitely generated.

Proposition 1.4 Schur-Zassenhaus. *With the above notation G contains a subgroup A mapping isomorphically onto G/P (any two such subgroups are conjugate by an element of P).*

This says that for Sylow p-subgroups all extensions are split (i.e. semidirect products).

Moreover if we let $\overline{P}$ be the #

Definition 1.5 Frattini quotient. Let P be a pro-p-group, then
$$\overline{P}$$
is the maximal elementary abelian p-group quotient (recall this is the additive group of a (possibly infinite) vector space over $\mathbf{F}_p$). ◊

This can equivalently be defined as the quotient by the Frattini subgroup, $\Phi(P)$ of P, which is the intersection of all maximal subgroups, and can be obtained as the set of all non-generators (the elements that can be removed from any generating set).

Example 1.6 If P is the cyclic group $\mathbf{Z}/p^2$ we have the maximal sub $p\mathbf{Z}/p^2$ and the quotient $\mathbf{Z}/p$. Or the Heisenberg group

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

we get Frattini subgroup

$$\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and quotient

$$\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

□

Proposition 1.7 Burnside's basis theorem. *If $x_1, \dots, x_d \in P$ generate the quotient $\overline{P}$ then they generate P.*

So we can understand generators of P by understanding those of $\overline{P}$!

In fact Boston has strengthened this to

Theorem 1.8 *Let G be a profinite group with a normal p-Sylow subgroup P of finite index in G and A a subgroup of G that maps isomorphically to G/P (note A is finite). Then if A acts on P and $\overline{P}$ by conjugation (so that $\overline{P}$ is a $\mathbf{F}_p[A]$-module) and*

$$\overline{V} \subset \overline{P}$$

is an $\mathbf{F}_p[A]$-submodule. Then there is an A-invariant subgroup $V \subseteq P$ which maps onto $\overline{V}$ and has $\dim_{\mathbf{F}_p} \overline{V}$ generators.

Example 1.9 If $\overline{V}$ is just $\mathbf{F}_p$ (written multiplicatively) then an invariant submodule is an

$$\overline{x} \in \overline{P}$$

for which

$$a^{-1}\overline{x}a = \overline{x}^{\phi(a)}$$

for some character

$$\phi \colon A \to \mathbf{F}_p^\times$$

this then lifts to

$$x \in P : a^{-1}xa = x^{\phi'(a)}$$

where $\phi' = \mathrm{teich} \circ \phi \colon A \to \mathbf{Z}_p^\times$. □

and also shows

Lemma 1.10 *Up to isomorphism there is precisely one semidirect product of P and A with given A action on $\overline{P}$.*

Let $H \subseteq \mathrm{GL}_n(k)$.

Definition 1.11 A $k[H]$-module V is prime to adjoint if $\mathrm{Ad}(H) = M_n(k)$ and V have no irreducible subrepresentations in common. ◊

Let

$$Z_S = \left\{x \in K^\times : (x) = I^p \text{ for some } I, x_v = y_v^p \in K_v \forall v \in S_1\right\}$$

a group for which

$$Z_S \supseteq K^{\times p}$$

so

$$B_S = Z_S / K^{\times p}$$

which is an elementary abelian p-group.

As Galois H acts on $Z_S, K^{\times p}$ we have that B_S is a $\mathbf{F}_p[H]$-module.

For a pro-p-group P Let $d(P), r(P)$ be ranks of minimal sets of generators and relations for P, i.e. the cardinality of a minimal set of generators of P and relations when viewing P as a quotient of a free pro-p-group.

Write $\delta(F) = 1$ if $\mu_p \subseteq F$, $\delta(F) = 0$ otw. The significance of these is related to the fact that for certain local fields this is exactly the relation rank!

Theorem 1.12 Koch, H., Galoissche Theorie der p-Erweiterungen..

$$r(P) = \left(\sum_{v \in S_1} \delta(K_v)\right) - \delta(K) + \dim_{\mathbf{F}_p} B_S$$

$$d(P) = r_2(K) + 1 + r(P)$$

so P is topologically f.g.

If $p \nmid h_K$ global class field theory gives a map from the idele class group of L to P which induces a map on Frattini quotients and leads to: the exact sequence of $\mathbf{F}_p[H]$-modules

$$0 \to B_S \to \overline{O_K^\times} \to \bigoplus_{v \in S_1} \overline{O_{K_v}^\times} \to \overline{P} \to 0.$$

Theorem 1.13 Boston-Mazur. *If $p \nmid \#H$ then as $\mathbf{F}_p[H]$-modules*

$$\bigoplus_{v \in S_1} \overline{O}_v^\times \cong \mathbf{F}_p[H] \oplus \left(\bigoplus_{l \in S} \mathrm{Ind}_{H_l}^H \mu_p\right)$$

sum over decomposition subgroups

$$\overline{O}_K^\times \oplus \mathbf{F}_p \cong \mu_p \oplus \mathrm{Ind}_{H_\infty}^H \mathbf{F}_p$$

$H_\infty = \langle \bar{\cdot} \rangle$.

Assume $\bar{\rho}$ tame now. P is normal pro-p-Sylow subgroup of $\tilde{\Pi}$, and some $A \twoheadrightarrow G/P = H$ so $\tilde{\Pi} = H \rtimes P$. As $\Gamma_n(W(k))$ is pro-p by Schur-Zassenhaus we have

$$H_1 \subseteq \mathrm{GL}_n(W(k))$$

with $H \cong H_1$ so we can find a lift

$$\rho_1 \colon \tilde{H} \to \mathrm{GL}_n(W(k))$$

which induces an isomorphism

$$A \xrightarrow{\sim} H_1$$

we denote

$$\sigma\colon A \to \mathrm{GL}_n(W(k)).$$

Given a coefficient ring R we have

$$W(k) \to R$$

so

$$\sigma_R\colon A \to \mathrm{GL}_n(R) \supseteq \Gamma_n(R)$$

and A acts on $\Gamma_n(R)$ via conjugation.

Let

$$E_{\bar\rho}\colon \mathcal{C} \to \mathsf{Set}$$

$$E_{\bar\rho}(R) = \mathrm{Hom}_A(P, \Gamma_n(R)).$$

Then we have a natural morphism

$$E_{\bar\rho} \to D_{\bar\rho}$$

given by

$$\phi \in E_{\bar\rho}(R) \mapsto \tilde\Pi = A \rtimes P \xrightarrow{\sigma_R,\phi} \mathrm{GL}_n(R).$$

Theorem 1.14 Boston. *$R_{\bar\rho}$ is representable.*

1. *IF $C(\bar\rho) = k$ then*
$$E_{\bar\rho} \xrightarrow{\sim} D_{\bar\rho}$$
2. *Otherwise this morphism is smooth and induces an isomorphism of tangent spaces.*

Theorem 1.15 Boston. *Let p be odd, and*

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

odd, absolutely irreducible and tame, $H = \mathrm{im}(\bar\rho)$. Let

$$K = \mathbf{Q}_S^{\ker\bar\rho}$$

$$V = \mathrm{coker}\left(\mu_p(K) \to \prod_{v\in S_1} \mu_p(K_v)\right)$$

both V, B_S are $\mathbf{F}_p[H]$ modules, suppose $p \nmid h_K$ and V, B_S are relatively prime to $\mathrm{Ad}(\bar\rho)$ as $\mathbf{F}_p[H]$-modules, then

$$R(\bar\rho) \cong \mathbf{Z}_p[[T_1, T_2, T_3]],$$

moreover ρ can be described explicitly.Using Theorem 1.13 we have that $\overline{P}$ is generated by

1. *$\overline{x}$ fixed by H*
2. *$\overline{y}$ with $\overline{y}^c = \overline{y}^{-1}$*
3. *other elements generating a prime-to-adjoint $\mathbf{F}_p[H]$-module.*

by Theorem 1.8 we get that P is generated by some x fixed by H and y s.t. $y^c = y^{-1}$ and other prime-to-adjoint gens. So the dimension of the tangent space is 3 and we the universal deformation to

$$\mathbf{Z}_p[[T_1, T_2, T_3]]$$

via

$$x \mapsto \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_1 \end{pmatrix}$$

$$y \mapsto \begin{pmatrix} (1+T_2T_3)^{\frac{1}{2}} & T_2 \\ T_3 & (1+T_2T_3)^{\frac{1}{2}} \end{pmatrix}$$

other generators mapping to 0.

Where do these matrices come from? We are trying to write down the universal matrices which are fixed by conjugation by any element, or are inverted after conjugation by complex conjugation.

For the first the only matrices in the center are multiples of the identity which gives the form of x. For the second if we take

$$c = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

then $cyc^{-1} = y^{-1}$ has the following consequence. The condition gives $\det y = \pm 1$. As cyc^{-1} is y with the off diagonal elements negated assuming $\det = 1$ the inverse is the same with the diagonal terms swapped: we see that the two terms on the diagonal must be equal and we can choose the off diagonal terms to be whatever we like, call them T_2, T_3. Writing out what $\det = 1$ means for equal diagonal terms shows both are $(1+T_2T_3)^{\frac{1}{2}}$.

I'm confused about why we have $\det = 1$ though. *References

References

[1] Conrad, Brian David. *Arithmetic algebraic geometry*. Vol. 9. American Mathematical Soc., 2001.

[24] Boston, Nigel. *Explicit deformation of Galois representations*. Inventiones mathematicae 103.1 (1991): 181-196.

[25] Boston, Nigel, and Barry Mazur. *Explicit universal deformations of Galois representations*. Algebraic Number Theory—in honor of K. Iwasawa. Mathematical Society of Japan, 1989.