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

As an $\mathbb{F}_p[H]$-module

$$\bar{\rho} = \operatorname{Ind}_{H_\infty}^{H} \mathbb{F}_p \oplus \mathbb{F}_p \oplus V \oplus B_S \qquad \operatorname{ad}_{\bar{\rho}} \underset{\mathbb{F}_p[H]}{=} \operatorname{ad}^0_{\bar{\rho}} \oplus \mathbb{F}_p$$

H_∞ = subgp of H gen. by a comp. conjugation

06.06.18

Correction:

<u>H3:</u> $D_{\bar{\rho}}(k[\varepsilon])$ is a finite dimensional k-vector space

<u>"Proof"</u>: Take $\rho : G \longrightarrow GL_n(k[\varepsilon])$

$$\rho|_{\ker\bar{\rho}} : \ker\bar{\rho} \longrightarrow \Gamma_n(k[\varepsilon])$$

$\operatorname{Hom}_{cont}(\ker\bar{\rho}, \Gamma_n(k[\varepsilon]))$ is a finite set because of p-finiteness.

$\uparrow$ not injective in general

$D_{\bar{\rho}}(k[\varepsilon])$

<u>Inflation - restriction exact sequence</u>

Take a topological group G, $P \trianglelefteq G$ a normal subgroup. $H = G/P$. Then there is an exact sequence : (M a G-Module)

$$1 \longrightarrow H^1(H, M^P) \xrightarrow{\text{Inf}} H^1(G,M) \xrightarrow{\text{Res}} H^1(P,M)^H \longrightarrow H^2(H,M^P) \longrightarrow H^2(G,M)$$

Lemma. If G, M are finite then $H^i(G,M)$ is annihilated by $(\cdot \# G)$, $(\cdot \# M)$.

In particular if $\gcd(\# G, \# M) = 1$, then $H^i(G,M) = 0$ $\forall i \in \mathbb{N}$.

Lemma. G, P, H as before. Assume $H^i(H, M^P) = 0$ $\forall i \in \mathbb{N}$. Then

$$H^k(G,M) \cong H^k(P,M)^H \quad \forall k \in \mathbb{N}.$$

To prove H3, one identifies $D_{\bar\rho}(k[\varepsilon]) \cong H^1(G, Ad_{\bar\rho})$

Take $M = Ad_{\bar\rho}$, $P = \ker \bar\rho$.

$$1 \longrightarrow \underbrace{H^1(H, (Ad_{\bar\rho})^{P})}_{\text{finite set because}} \longrightarrow H^1(G, Ad_{\bar\rho}) \longrightarrow H^1(P, Ad_{\bar\rho})^H$$

acts trivially

finite set because H, $Ad_{\bar\rho}$ are finite

$P \underset{\text{open}}{\trianglelefteq} G \Rightarrow H = P/G$ finite.

$$H^1(P, Ad_{\bar\rho})^H = \underbrace{\mathrm{Hom}_H(P, Ad_{\bar\rho})}_{\text{finite set by } \Phi_p:\ p\text{-finiteness}}$$

A few results on cohomology of pro-p groups:

Def. Take I a set. $L(I)$ = free group generated by $\{x_i\}_{i\in I}$ ("variables").

The free profinite group (topologically) "generated" by $\{x_i\}_{i\in I}$ is

$$\varprojlim_{\substack{\text{finite quotients} \\ \text{s.t. } U \text{ contains} \\ \text{almost all } x_i\text{'s}}} L(I)/U$$

The free pro-p group (top.) generated by $\{x_i\}_{i\in I}$ is $\varprojlim_{\substack{\text{quotient } p\text{-group} \\ \text{s.t. } U \text{ contains almost} \\ \text{all } x_i\text{'s}}} L(I)/U$

Lemma. G a pro-p group.

(1) If G is free, then $H^2(G, \mathbb{F}_p) = 0$.

(2) If $H^1(G, \mathbb{F}_p)$, $H^2(G, \mathbb{F}_p)$ are finite, then: (a) the minimal number of (top.) generators for G is $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) =: d_1$

(b) if $0 \to R \to F \to G \to 0$, then the minimal number of generators for R is $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$.

(F: free pro-p group on d_1 generators)

Literature: Ribes - Zalesskii

Explicit universal deformation pairs for some tame residual presentations:

Fix $\bar{\rho}: G_{\mathbb{Q},S} \longrightarrow GL_2(\mathbb{F}_p)$, $p>2$, $\bar{\rho}$ tame, absolutely irreducible.

$$\begin{tikzcd} L \arrow[d, dash, "P"] \\ K \arrow[d, dash, "H \cong \operatorname{im}\bar{\rho}"] \\ \mathbb{Q} \end{tikzcd} \qquad G$$

$G = P \rtimes H$ because $\bar{\rho}$ is tame.

$\bar{P} :=$ Frattini quotient of P

We proved:

$$D_{\bar{\rho}} \xrightarrow{\cong} \operatorname{Hom}_H(P, \Gamma_2(\cdot)) \text{ is a natural isomorphism.}$$

Theorem. (Koch) (1) if $p \nmid cl(K)$ = class number of K, then one has an exact sequence:

$$0 \to B_S \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p \longrightarrow \bigoplus_{\underbrace{v \in S_1}_{\text{non-archimedian places!}}} \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^p \longrightarrow \bar{P} \to 0.$$

of $\mathbb{F}_p[H]$-modules.

$$B_S := \{x \in K^\times \mid (x) \text{ is a } p\text{-power of a fractional ideal, } x_v \text{ is a } p\text{-power for every } v \in S_1\} / (K^\times)^p$$

(2) (Koch + Boston + Mazur) Boston + Mazur: "Explicit universal deform. of Gal-rep."

Boston + Ullom:

$$\bigoplus_{v \in S_1} \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^p \cong \mathbb{F}_p[H] \oplus \Big(\bigoplus_{v \in S_1} \underbrace{\mu_p(K_v)}_{\circlearrowleft \text{ galoisaction}}\Big)$$

(3) $$\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p \oplus \overset{\text{trivial action by } H}{\mathbb{F}_p} \cong \underbrace{\mu_p(K)}_{\circlearrowleft \text{ Galois action}} \oplus \underbrace{\operatorname{Ind}_{H_\infty}^H \mathbb{F}_p}_{\text{trivial action of } H_\infty.}$$

H_∞ = subgroup of H generated by a complex conjugation.

<u>Exercise</u>: $$\mathbb{F}_p[H] \underset{\mathbb{F}_p[H_\infty]\text{-module}}{\cong} \operatorname{Ind}_{H_\infty}^H \underbrace{\mathbb{F}_p}_{\text{trivial } H_\infty \text{ action}} \oplus \operatorname{Ind}_{H_\infty}^H \tilde{\mathbb{F}}_p \quad (\bar{\rho} \text{ odd})$$

if c is a complex conjugation, then $c1 = -1$. = definition of $\tilde{\mathbb{F}}_p = \mathbb{F}_p$ (as sets)

$$\cong \operatorname{Ind}_1^H \mathbb{F}_p \ (\bar{\rho} \text{ even})$$

The category of $\mathbb{F}_p[H]$-modules is semisimple because $\bar{p}$ is tame.

Corollary: ($\bar{p}$ odd)
$$\bar{P} \cong_{\mathbb{F}_p[H]} \mathrm{Ind}_{H_\infty}^{H} \tilde{\mathbb{F}}_p \oplus \mathbb{F}_p \oplus B_S \oplus \underbrace{\mathrm{coker}\Big(\mu_p(K) \to \bigoplus_{v \in S_1} \mu_p(K_v)\Big)}_{=: V_S}$$

By 1+2+3 one has
$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p \oplus \mathbb{F}_p \to \bigoplus_{v \in S_1} \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^p \oplus B_S \oplus \mathbb{F}_p \to \bar{P} \to 0$$

$$\leadsto \quad \bar{P} \underset{[1]}{\cong} \mathbb{F}_p[H] \oplus V_S \oplus B_S \oplus \mathbb{F}_p \Big/ \mathrm{Ind}_{H_\infty}^{H} \mathbb{F}_p$$

Def. We say $\bar{\rho}$ is regular, if it is odd, absolutely irreducible, and if V_S, B_S are prime-to-adjoint, $p \nmid \mathrm{cl}(K)$ (class number of K)

Remark.
$$\mathrm{Ad}_{\bar{\rho}} \cong_{\mathbb{F}_p(H)} \underbrace{\mathrm{Ad}^0_{\bar{\rho}}}_{\text{trace 0 matrices}} \oplus \underbrace{\mathbb{F}_p}_{\text{scalar matrices}}$$

As an $\mathbb{F}_p[H]$-module, $\bar{P}$ is generated by
* x s.t. $h \cdot x = x$ $\forall h \in H$ (gen. of $\mathbb{F}_p$) - lift_p
* y st. $c\, y = y^{-1}$ with c complex conj. (gens of $\mathrm{Ind}_{H_\infty}^{H} \tilde{\mathbb{F}}_p$)
* some generators prime to adjoint

Theorem. If $\bar{\rho}$ is tame and regular, then the universal def pair is
$$R^{univ}(\bar{\rho}) \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$$

ρ^{univ} is the representation such that
$$\rho^{univ}|_P : x \longmapsto \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_1 \end{pmatrix}, \quad y \longmapsto \begin{pmatrix} \sqrt{1+T_2T_3} & T_2 \\ T_3 & \sqrt{1+T_2T_3} \end{pmatrix}$$
kernel ...

$p > 2 \Rightarrow \sqrt{\ }$ works..

Proof. Recall: $\bar{\rho}$ odd $\Rightarrow$ $d_1 - d_2 = 3$
$$d_1 - d_2 = \dim_{\mathbb{F}_p} H^1(G, \mathrm{Ad}_{\bar{\rho}}) - \dim_{\mathbb{F}_p} H^2(G, \mathrm{Ad}_{\bar{\rho}})$$

If $d_1 = 0 \Rightarrow d_2 = 0. \Rightarrow R^{univ}(\bar{\rho}) = \mathbb{Z}_p[[T_1, T_2, T_3]]$

Inflation-Restriction exact sequence:
$$1 \to \underbrace{\cancel{H^1(H, \mathrm{Ad}_{\bar{\rho}})}}_{0} \to H^1(G, \mathrm{Ad}_{\bar{\rho}}) \xrightarrow{\cong} H^1(P, \mathrm{Ad}_{\bar{\rho}})^H \to \underbrace{\cancel{H^2(H, \mathrm{Ad}_{\bar{\rho}})}}_{0}$$

$\gcd(\# H, \# \mathrm{Ad}_{\bar{\rho}}) = 1.$

$$H^1(G, Ad_{\bar\rho}) \cong H^1(P, Ad_{\bar\rho})^H \cong Hom_H(P, Ad_{\bar\rho}) \cong Hom_H(\bar P, Ad_{\bar\rho})$$

$$Hom_H(\bar P, Ad_{\bar\rho}) \cong Hom_H(Ind_{H_\infty}^H \tilde{\mathbb{F}}_p \oplus \mathbb{F}_p \oplus \underbrace{V_s \oplus B_s}_{\text{prime to adjoint}}, Ad_{\bar\rho})$$

$$\cong Hom_H(Ind_{H_\infty}^H \tilde{\mathbb{F}}_p, Ad_{\bar\rho}) \oplus Hom_H(\mathbb{F}_p, Ad_{\bar\rho})$$

- $Hom_H(Ind_{H_\infty}^H \tilde{\mathbb{F}}_p, Ad_{\bar\rho}) \underset{\text{Frobenius reciprocity}}{\cong} Hom_{H_\infty}(\tilde{\mathbb{F}}_p, \underbrace{Ad_{\bar\rho}}_{\mathbb{F}_p[H_\infty] \text{ module by restriction}})$

- $\dim_{\mathbb{F}_p} Hom_{H_\infty}(\tilde{\mathbb{F}}_p, Ad_{\bar\rho}) = 2$

$y \mapsto M \in Ad_{\bar\rho}$ $\quad M^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} M \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$y^c = y^{-1}$
$\| $
cyc^{-1}

$\left(\underset{\text{odd}}{\bar\rho(c)} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right)$

- $Hom_H(\mathbb{F}_p, Ad_{\bar\rho}) \quad \rightarrow \quad \dim_{\mathbb{F}_p} Hom_H(\mathbb{F}_p, Ad_{\bar\rho}) = 1.$

$\|$

$\underbrace{Ad^0_{\bar\rho}}_{} \oplus \mathbb{F}_p$

$\bar\rho$ abs. irreducible $\Rightarrow$ does not contain any $\mathbb{F}_p$ with trivial action

$\Rightarrow \dim_{\mathbb{F}_p} Hom_H(P, Ad_{\bar\rho}) = 3$

We prove that $\rho^{univ}|_P$ has the required form: 1) $\underset{H\text{-invariant}}{X} \longmapsto \underset{H\text{-invariant}}{\rho^{univ}(X)} \in \Gamma_2(R^{univ}) \Rightarrow \rho(X)$ is a scalar

$\underset{\text{up to automorphism}}{\rightsquigarrow} \quad \rho(x) = \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_1 \end{pmatrix}$

2) $y \mapsto \rho^{univ}(y) \in \Gamma_2(R^{univ})$
$\quad$ s.t. $\rho^{univ}(c)\rho^{univ}(y)\rho^{univ}(c) = \rho^{univ}(y)^{-1}$ $\quad \Rightarrow \rho(y) = \begin{pmatrix} \sqrt{1+T_2T_3} & T_2 \\ T_3 & \sqrt{1+T_2T_3} \end{pmatrix}$

$cy = y^{-1}$

3) z prime to adjoint $\Rightarrow \rho^{univ}(z)$ generates a prime to adjoint H-subm. of $\Gamma_2(R^{univ}) \Rightarrow$ this subgroup is trivial $\Rightarrow \rho(z) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

<u>Remarks</u>: ρ^{univ} well-def. because x, y generate a free pro-p subgroup of P (Koch: $H^2(\langle x,y\rangle, \mathbb{F}_p) = 0$).

galrep
13. 06. 18

Preliminaries :

Poiton - Tate exact sequence:

Fix K a number field, S finite set of places. ; M a $G_{K,S}$-module.

For $v \in S$, one has

$$\begin{tikzcd} G_{K_v} \arrow[rr, hook] \arrow[dr, hook] & & G_{K,S} \\ & G_K \arrow[ur] & \end{tikzcd}$$

assumption ... check beginning of lecture.

Then there is a map $\mathrm{Res}: H^i(G_{K,S}, M) \longrightarrow \bigoplus_{v\in S} H^i(G_{K_v}, M)$

M finite order and $\# M$ not divisible by the primes underlying S.

Then : (Poiton - Tate exact sequence)

$$0 \longrightarrow H^0(G_{K,S}, M) \longrightarrow \bigoplus_{v\in S} H^0(G_{K_v}, M) \longrightarrow H^2(G_{K,S}, M')^*$$

$$\hookrightarrow H^1(G_{K,S}, M) \longrightarrow \bigoplus_{v\in S} H^1(G_{K_v}, M) \longrightarrow H^1(G_{K,S}, M')^*$$

$$\hookrightarrow H^2(G_{K,S}, M) \longrightarrow \bigoplus_{v\in S} H^2(G_{K_v}, M) \longrightarrow H^0(G_{K,S}, M')^* \longrightarrow 0.$$

$\mathcal{O}_S^* :=$ ring of S-units of $K = \{ a \in K^\times \mid v(a) \geq 0 \ \forall v \notin S \}$

$M' = \mathrm{Hom}(M, \mathcal{O}_S^*)$

A a discrete torsion abelian group, $A^* = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ "Pontryagin dual"

Today: $\mathbb{F}_p$ with trivial $G_{K,S}$-action, $\mathbb{F}_p' = \mu_p$.

Def. The i-th Tate - Shafarevich group $(i=1,2)$ is $Ш^i_S(K, M) := \ker\left(H^i(G_{K,S}, M) \to \bigoplus_{v\in S} H^i(G_{K_v}, M)\right)$

Remark: if $\# \mu_p(K) = p$, then

$$Ш^1_S(K, \mu_p) \underset{\substack{\text{trivial}\\ \text{action}}}{=} \ker\left(\mathrm{Hom}_{cont}(G_{K,S}, \mu_p) \longrightarrow \bigoplus_{v\in S} \mathrm{Hom}_{cont}(G_{K_v}, \mu_p)\right)$$

$$\underset{\substack{\text{Kummer}\\ \text{theory}}}{=} \ker\left(\mathcal{O}_S^\times / \mathcal{O}_S^{\times p} \longrightarrow \bigoplus_{v\in S} \mathcal{O}_{K_v}^\times / \mathcal{O}_{K_v}^{\times p} \right) = B_S$$

as defined earlier.

Lemma. $Ш^1_S(K, M) = Ш^2_S(K, M')^*$.

Ring of S-integers $\mathcal{O}_S = \{ a \in K \mid v(a) \geq 0 \ \forall v \notin S \}$

$Cl_S(K) :=$ ideal class group $:= Cl(K) \big/$ subgroup generated by prime ideals in S

Lemma. $Ш^1_S(K, \mu_p) = \mathrm{Hom}(Cl_S(K), \mu_p)$

every hom. factors through the "p-elementary S-ideal class group"

$$Cl_S(K) \big/ Cl_S(K)^p$$

For this lecture we write $Cl_S(K)$ for $Cl_S(K) \big/ Cl_S(K)^p$.

Vandiver's conjecture: In the following we take $K = \mathbb{Q}(\zeta_p)$
ζ primitive p-th root of unity

$$\begin{array}{ccl} \mathbb{Q}(\zeta_p) & = & K \\ | & & \\ \mathbb{Q}(\zeta_p + \zeta_p^{-1}) & =: & K^+ \\ 2 | & & \leftarrow \text{totally real} \\ \mathbb{Q} & & \end{array}$$

$H \cong \mathbb{Z}/(p-1)\mathbb{Z}$

$h = \# Cl(K)$

$h^+ = \# Cl(K^+)$

One shows $h^+ \mid h$ and sets $h^- := \dfrac{h}{h^+}$.

Question: p-divisibility of h?
Divisibility of h^- is well-understood. (Washington's book: "Introduction to cyclotomic fields")

About h^+, one has

(Vandiver's Conjecture) $p \nmid h^+$.

We rewrite the statement in terms of the structure of $Cl_S(K)$ as $\mathbb{F}_p[H]$-module
$S = \{p, \infty\}$

Notation: take $\nu : H \longrightarrow \mathbb{F}_p^\times$ and M any $\mathbb{F}_p[H]$-module, then

$$M_\nu = \text{largest submodule of } M \text{ on which } H \text{ acts via } \nu \text{ of } M$$
$$\| $$
$$\{m \in M \mid h \cdot m = \nu(h) \cdot m\}$$

(well-defined because $p \nmid \# H$ and Maschke's theorem)

$$M = \bigoplus_{\nu \text{ character of } H} M_\nu$$

; Since $H = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, the characters of H are the powers of the $\underbrace{\text{mod } p \text{ cyclic character}}_{w : H \longrightarrow \mathbb{F}_p^\times}$

We write $\mathbb{F}_p^\nu$ for the 1-dim. $\mathbb{F}_p$-vector space on which H acts via ν and also

$$M(i) = M \otimes \mathbb{F}_p^{\omega^i} \quad (\text{"Take twist"})$$

$Cl_S(K)$ is an $\mathbb{F}_p[H]$-module, so

$$Cl_S(K) = \bigoplus_{i \in \mathbb{Z}} Cl_S(K)_{w^i}$$
$$\cup\!|$$
$$Cl_S(K^+) = \bigoplus_{i \in \mathbb{Z} \text{ even}} Cl_S(K)_{w^i}$$

The odd part is understood.

Vandiver's conjecture $\iff \forall i \in 2\mathbb{Z} : Cl_S(K)_{w^i} = 0$.

Deformations of reducible Galois representations:

Mézard's notes, original: Böckle - Mézard "The prime-to-adjoint principle and unobstructed Galois deformations in the Borel case"

Fix $\bar\rho : G_{\mathbb{Q},S} \longrightarrow GL_2(\mathbb{F}_p)$ such that:

* $\bar\rho$ is upper triangle: $\mathrm{im}\,\bar\rho \subseteq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \Rightarrow \bar\rho(g) = \begin{pmatrix} \chi_1(g) & * \\ 0 & \chi_2(g) \end{pmatrix}$

for some characters $\chi_1, \chi_2 : G_{\mathbb{Q},S} \longrightarrow \mathbb{F}_p^\times$

Since $S = \{p, \infty\}$ we must have $\chi_1 = w^i,\ \chi_2 = w^j$

$$\left(\begin{array}{l} \text{Kronecker-Weber: } G_{\mathbb{Q}}^{ab} \underset{\prod_\ell \chi_{cyc,\ell}}{\cong} \prod_\ell \mathbb{Z}_\ell^\times \\[2ex] G_{\mathbb{Q},S} \overset{\chi_{cyc}}{\cong} \mathbb{Z}_p^\times \end{array} \right)$$

We also assume that $*\ \det\bar\rho = \omega$ $\quad (\iff i+j \equiv 1(p-1))$

$*\ C_k(\bar\rho) = k$

One has a diagram:

$$\begin{array}{lcl}
 & \mathbb{Q}_S & \\
\ker\bar\rho & | & \\
 & L & = \text{largest } \overset{\text{pro-}p}{\text{extension}} \text{ of } K \text{ unramified outside } S \\
 & | & \\
 & K & = \mathbb{Q}_S^{\ker\bar\rho} \\
p\text{-Sylow of } \operatorname{im}\bar\rho & | & \\
 & F & \cong \operatorname{im}\bar\rho \\
H & | & \\
 & \mathbb{Q} &
\end{array}$$

$\det\bar\rho = \omega \underset{\text{exercise}}{\Longrightarrow} F = \mathbb{Q}(\zeta_p)$

Hint: $\begin{pmatrix} \omega^i & * \\ 0 & \omega^j \end{pmatrix}^{p-1} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$

Remark: $*\ Ad_{\bar\rho} \underset{\mathbb{F}_p[H]}{\cong} Ad^0_{\bar\rho} \oplus \mathbb{F}_p \cong \mathbb{F}_p^{\varphi} \oplus \mathbb{F}_p^{\varphi^{-1}} \oplus \mathbb{F}_p \oplus \mathbb{F}_p$

where $\varphi = \chi_1\chi_2^{-1}$.

$*\quad Ш_S^i(K, \mathbb{F}_p^{\varphi})$ carries an action of H.

$$Ш_S^i(K, \mathbb{F}_p^{\varphi}) \cong \bigoplus_{i\in\mathbb{Z}} Ш_S^i(K, \mathbb{F}_p^{\varphi})_{\omega^i}$$

Lemma. The following are equivalent:

(1) $Ш_S^2(F, \mathbb{F}_p)$ is prime-to-adjoint

(2) $Ш_S^2(F, \mathbb{F}_p^{\nu})^H = 0$ for $\nu \in \{1, \varphi, \varphi^{-1}\}$

(3) $Ш_2^S(\mathbb{Q}, \mathbb{F}_p^{\nu}) = 0$ for $\nu \in \{1, \varphi, \varphi^{-1}\}$

Proof. (1) $\iff$ (2): The $G_{F,S}$-action on $\mathbb{F}_p^{\nu}$ is trivial

$$\Rightarrow Ш_S^2(F, \mathbb{F}_p^{\nu})^H = \left(Ш_S^2(F, \mathbb{F}_p)^{\nu}\right)^H = Ш_S^2(F, \mathbb{F}_p)_{\nu^{-1}}$$

$(M^{\nu} := M \otimes \mathbb{F}_p^{\nu},\ (M^{\nu})^H = M_{\nu^{-1}})$

Remark: M is prime-to-adjoint $\iff M_{\varphi} = M_{\varphi^{-1}} = M_1 = 0$.

$\Rightarrow \left(Ш_S^2(F, \mathbb{F}_p^{\nu})\right)^H = 0\ \forall \nu \in \{1, \varphi, \varphi^{-1}\} \iff Ш_S^2(F, \mathbb{F}_p)_{\nu^{-1}} = 0\ \forall \nu \in \{1, \varphi, \varphi^{-1}\}$

$\iff Ш_S^2(F, \mathbb{F}_p)$ is prime-to-adjoint

(2) <=> (3): $$H^2(G_{\mathbb{Q},S}, \mathbb{F}_p^{\nu}) \cong H^2(G_{F,S}, \mathbb{F}_p^{\nu})^H$$

(last time) because $G_{\mathbb{Q},S} / G_{F,S} = H$

$p \nmid \# H$

By the def of Ш:

one has $$Ш_S^2(G_{\mathbb{Q},S}, \mathbb{F}_p^{\nu}) \cong Ш_S^2(G_{F,S}, \mathbb{F}_p^{\nu})^H.$$

Proposition 1. $Ш_S^2(F, \mathbb{F}_p)$ is prime-to-adjoint $\iff Cl_S(F)_{\omega\nu} = 0$ for $\nu \in \{1, \varphi, \varphi^{-1}\}$

Proof. $Ш_S^1(F, \mu_p) = \mathrm{Hom}(Cl_S(F), \mu_p)$ $\quad (\mu_p = \mathbb{F}_p(1))$

trivial $G_{F,S}$-module $\quad$ twist

$= \mathrm{Hom}(Cl_S(F), \mathbb{F}_p)(1)$

$$Ш_S^2(F, \mathbb{F}_p) \cong Ш_S^1(F, \mu_p)^* \cong \left(\mathrm{Hom}(Cl_S(F), \mu_p)(1)\right)^* \underset{p\text{-elementary}}{\cong} Cl_S(F)(-1)$$

$$Ш_S^2(F, \mathbb{F}_p)_{\nu} \cong (Cl_S(F)(-1))_{\nu} = Cl_S(F)_{\omega\nu}.$$ ∎

Theorem. (Böckle, Mezard)

Vandiver's conjecture holds $\iff \forall \bar\rho$ as before: $R^{univ}(\bar\rho) \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$

20.06.18

(non-diagonal $\bar\rho: G_{\mathbb{Q},S} \to GL_2(\mathbb{F}_p)$, reducible)

s.t. $\bar\rho = W$ and $c_k(\bar\rho) = k$.

Proof. "=>": Recall $Ad_{\bar\rho} \cong \mathbb{F}_p^{\varphi} \oplus \mathbb{F}_p^{\varphi^{-1}} \oplus \mathbb{F}_p \oplus \mathbb{F}_p$ $\qquad \varphi = \omega^{i-j}$

action via φ

$(F = \mathbb{Q}(\zeta_p))$

<u>Remark</u>:

$$Ш_S^2(F, \mathbb{F}_p) \text{ prime-to-adjoint} \underset{\text{Prop. 1}}{\iff} Cl_S(F)_{\omega\nu} = 0 \ \forall \nu \in \{1, \varphi, \varphi^{-1}\}$$

$Cl_S(F)_{\omega} = 0$ (known result, 6.16 Washington's book)

$\iff Cl_S(F)_{\omega^{i-j+1}} = 0, \ Cl_S(F)_{\omega^{j-i-1}} = 0$

ν: Character of H $\quad (\nu \in \{1, \varphi, \varphi^{-1}\}\,!)$ $\qquad H = \mathrm{Gal}(F/\mathbb{Q})$

Poisen-Tate:

$$\underbrace{Ш^2_S(F,\mathbb{F}_p)_\nu}_{} \to H^2(G_{F,S}, \mathbb{F}_p)_\nu \longrightarrow H^2(G_{F_p}, \mathbb{F}_p)_\nu \longrightarrow H^0(G_{F,S}, \mu_p)^*_\nu \longrightarrow 0$$

we assumed Vandiver's conjecture

$\rightsquigarrow \quad Cl_S(F)_{\omega\nu} = 0$ for $\nu \in \{\varphi, \varphi^{-1}\}$

isomorphism

$$H^0(G_{F,S}, \mu_p)^*_\nu \xrightarrow[\sim]{\mathrm{Res}} H^0(G_{F_p}, \mu_p)^* \cong H^2(G_{F_p}, \mathbb{F}_p)$$

local Tate duality

$\cong$ one has isomorphism

$\underset{\text{by remark}}{\Longrightarrow} \quad Ш^2_S(F,\mathbb{F}_p)_\nu = 0 \quad \underset{\text{sequence}}{\Longrightarrow} \quad H^2(G_{F,S},\mathbb{F}_p)_\nu = 0.$

We want $H^2(G_{\mathbb{Q},S}, \mathrm{Ad}\bar\rho) = 0$.

We mentioned $\quad H^2(G_{\mathbb{Q},S}, \mathbb{F}_p^\nu) \cong H^2(G_{F,S}, \mathbb{F}_p^\nu)^H$

Fix $\nu \in \{1, \varphi, \varphi^{-1}\}$, then $\quad H^2(G_{\mathbb{Q},S}, \mathbb{F}_p^\nu) \cong H^2(G_{F,S}, \mathbb{F}_p^\nu)^H$

$$\| $$

$$\underset{\substack{\uparrow \\ \text{previous} \\ \text{step in the proof}}}{0 =} H^2(G_{F,S}, \mathbb{F}_p)_{\nu^{-1}} = \left(H^2(G_{F,S}, \mathbb{F}_p)^\nu\right)^H$$

$$H^2(G_{\mathbb{Q},S}, \mathrm{Ad}\bar\rho) = \bigoplus_{\nu = 1,1,\varphi,\varphi^{-1}} H^2(G_{\mathbb{Q},S}, \mathbb{F}_p^\nu) = 0$$

$\rightsquigarrow$ The deformation problem for $\bar\rho$ is unobstructed.

$\Rightarrow \quad R^{univ}(\bar\rho) \cong \mathbb{Z}_p[\![T_1, T_2, \dots, T_d]\!]$, $\quad d = \dim H^1(G_{\mathbb{Q},S}, \mathrm{Ad}\bar\rho)$

Recall the decomposition

$$\bar P \cong \mathrm{Ind}_{H_\infty}^{H} \vec{\mathbb{F}}_p \oplus \mathbb{F}_p \oplus \overbrace{\mathrm{coker}(\mu_p(F) \to \mu_p(F_p))}^{=0} \oplus B_S \qquad B_S \cong Ш^2_S(F,\mathbb{F}_p)^*$$

$$P \left(\begin{array}{c} L \\ | \\ K \\ | \\ F \\ | \, H \\ \mathbb{Q} \end{array} \right.$$

look earlier for definitions

B_S is prime-to-adjoint because $Ш^2_S(F,\mathbb{F}_p)$ is.

(One shows: M $\mathbb{F}_p[H]$-module is p.t.a. $\Leftrightarrow$ M^* is p.t.a.

$M_\nu \cong M^*_{\nu^{-1}}$)

Now one computes $H^1(G_{\mathbb{Q},S}, Ad\bar{\rho}) = H^1(G_{F,S}, Ad\bar{\rho})^H = \mathrm{Hom}_H(G_{F,S}, Ad\bar{\rho})^{\text{galrep}}$

$= \mathrm{Hom}_H(\mathrm{Ind}_{H_\infty}^H \tilde{\mathbb{F}}_p \oplus \mathbb{F}_p, Ad\bar{\rho})$ is 3-dimensional.

$\Rightarrow d = 3$.

"$\Leftarrow$": Assume: $H^2(G_{\mathbb{Q},S}, Ad\bar{\rho}) = 0$ for all $\bar{\rho}$ with the given form.

Take one such $\bar{\rho}$: $\bar{\rho} \cong \begin{pmatrix} \omega^i & * \\ 0 & \omega^j \end{pmatrix}$ where $i+j \equiv 1 \ (p-1)$

$$0 = H^2(G_{\mathbb{Q},S}, Ad\bar{\rho}) = \bigoplus_{\substack{\nu = 1,1,\\ \varphi,\varphi^{-1}}} H^2(G_{\mathbb{Q},S}, \mathbb{F}_p^{\nu}) \Rightarrow Ш^2_S(F, \mathbb{F}_p^{\nu}) = 0.$$

$\underset{\text{Prop. 1.}}{\Longrightarrow}$ $Cl_S(F)_{\omega\nu} = 0$ $\varphi = \omega^{i-j} \equiv \omega^{1-2j}$

$\varphi^{-1} = \omega^{j-i} = \omega^{2j-1}$

$\Rightarrow Cl_S(F)_{\omega^{2j}} = 0.$

We said: Vandiver's conjecture holds $\Leftrightarrow Cl_S(F)_{\omega^{2j}} = 0 \ \forall j$.

If $\exists \bar{\rho} \sim \begin{pmatrix} \omega^{1-j} & * \\ 0 & \omega^j \end{pmatrix}$ for some j, then $Cl_S(F)_{\omega^{2j}} = 0$.

It remains to show: such a $\bar{\rho}$ exists for all j.

<u>Remarks</u>: $\mathrm{Ind}_{H_\infty}^H \mathbb{F}_p = \tilde{\mathbb{F}}_p \oplus \bigoplus_{\substack{k \in \{1,\dots,p-1\} \\ \text{odd}}} \mathbb{F}_p^{\omega^k}$ Fix j. Then for $k = 2j-1$,

one has a nontrivial H-homomorphism $\mathrm{Ind}_{H_\infty}^H \mathbb{F}_p \longrightarrow \mathbb{F}_p^{\omega^k}$

In particular a map $P \longrightarrow \mathbb{F}_p^{\omega^k}$.

One defines a representation

$$\begin{tikzcd} \bar{\rho}: G_{\mathbb{Q},S} \arrow[r] & GL_2(\mathbb{F}_p) \\ P \rtimes H \arrow[u, two heads] \arrow[ur] & \end{tikzcd}$$

$P \rtimes H \longrightarrow \underbrace{B_2(\mathbb{F}_p)}_{\text{upper triangle matrices}} \hookrightarrow GL_2(\mathbb{F}_p)$

$\quad\quad\quad\quad\quad\quad \parallel\!\!\parallel$

$\quad\quad\quad\quad\quad\quad N \rtimes T$

unipotent part $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ diagonal matrices $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

$\Rightarrow$ enough to give maps $P \to N$, $H \to T$ with $P \to N$ equivariant under H-action

One sets $H \longrightarrow T$ as $\begin{pmatrix} \omega^{1-j} & 0 \\ 0 & \omega^j \end{pmatrix}$

$P \longrightarrow N$ $\begin{pmatrix} 1 & \omega^k \\ 0 & 1 \end{pmatrix}$

(take $P \to \mathbb{F}_p^{\omega^k}$)

$\boxtimes$

* Full case: $\operatorname{im}\bar\rho \supseteq SL_2(\mathbb{F}_p)$ $\quad (\bar\rho : G_{\mathbb{Q},S} \longrightarrow GL_2(\mathbb{F}_p))$

One can give an explicit universal deformation

* Swinnerton-Dyer: for $\mathbb{F}_p$-coeff. these are all the possibilities (Dickson)
* Dimension conjecture: For arbitrary G profinite group, $\bar\rho$, then $\dim R(\bar\rho)/_{p\mathbb{Z}_p} = d^1 - d^2$

  Galois groups (G_K local field, $G_{K,S}$ global)

  $\Lambda = \mathbb{Z}_p \rightsquigarrow m_\Lambda = p\mathbb{Z}_p$

conjecture false (Sprang, "Counterex. to Gouvea's dim.-conjecture)

Main application of deformation theory:

studying Galois repres. that come from "automorphic" objects.

* Hecke characters and Galois characters

K global field

Def. The ring of adeles of K is the restricted product $\mathbb{A}_K = \prod'_{v \in P_K} (K_v, \mathcal{O}_v)$

$$:= \left\{ (\alpha_v)_v \in \prod_{v \in P_K} K_v \;\middle|\; \alpha_v \in \mathcal{O}_v \text{ for all but finitely many } v \right\}$$

Topology: basis of opens is given by $\prod_{v \in P_K} A_v$ where $A_v = \mathcal{O}_v$ for almost all v, $A_v \subseteq K_v$ open for all v.

There is an embedding
$$K \hookrightarrow \mathbb{A}_K$$
$$x \longmapsto (x_v)_v$$
look at $x\mathcal{O}_v$, it has a finite number of prime divisors. ($\rightsquigarrow$ well-defined)

Invertible elements $\mathbb{I}_K := \mathbb{A}_K^\times$ "Ideles"

One has $\mathbb{I}_K = \prod'_{v \in P_K} (K_v^\times, \mathcal{O}_v^\times)$ (topology of restricted product $\neq$ subspace topology in $\mathbb{A}_K$)

One has an embedding $K^\times \hookrightarrow \mathbb{I}_K$

$$C_K := \mathbb{A}_K^\times / K^\times \qquad \text{"idele class group"}$$

Global class field theory gives a map $C_K \longrightarrow Gal(K^{ab}/K)$ inducing an isomorphism

$$\hat{C}_K^{prof.} \xrightarrow{\sim} Gal(K^{ab}/K).$$

$G_K = Gal(\bar{K}/K)$

K: number field, not global

In particular $\{$finite order characters of $G_K\}$

$\updownarrow$ 1:1

$\{$finite order character of $C_K\}$

Also $\{$cont. characters $G_K \to$ prof. group$\}$ $\overset{1:1}{\longleftrightarrow}$ $\{$cont. characters $C_K \to$ prof. group$\}$

<u>We call</u>:

* a p-adic character of G_K is a continuous character $G_K \longrightarrow \overline{\mathbb{Q}}_p^\times$
* a Hecke character is a continuous character $C_K \longrightarrow \mathbb{C}^\times$
* a p-adic Hecke character is a continuous character $C_K \longrightarrow \overline{\mathbb{Q}}_p^\times$

χ: p-adic Hecke character $C_K \longrightarrow \overline{\mathbb{Q}}_p^\times$

$$\prod_{\nu \in P_K} (K_\nu^\times, \mathcal{O}_\nu^\times) = \mathbb{A}_K^\times \nearrow$$

$\rightsquigarrow \chi = (\chi_\nu)_\nu$ where $\chi_\nu : K_\nu^\times \longrightarrow \overline{\mathbb{Q}}_p^\times$

If $\nu \nmid p$, then χ_ν is a finite order character:

* archimedean places: $\mathbb{R}^\times \longrightarrow \overline{\mathbb{Q}}_p^\times$ or $\mathbb{C}^\times \longrightarrow \overline{\mathbb{Q}}_p^\times$
* non-archimedean places: $\nmid p$.

$$\begin{tikzcd} K_\nu^\times \arrow[rr] \arrow[dr, hook] & & \overline{\mathbb{Q}}_p^\times \\ & \mathcal{O}_F^\times \arrow[ur] & \end{tikzcd}$$

$F \mid \mathbb{Q}_p$ finite

27.06.18

Start with a Hecke character $\chi : C_K \longrightarrow \mathbb{C}^\times$, $\chi = (\chi_\nu)_\nu$

$\chi_\nu : K_\nu^\times \longrightarrow \mathbb{C}^\times$ (p-adic: $\chi = (\chi_\nu)_\nu : K_\nu^\times \longrightarrow \overline{\mathbb{Q}}_p^\times$)
$\nu \mid \ell, \nu \nmid p, \mathcal{O}_\nu^\times$

ν non-archimedean: χ_ν is determined by its value on a uniformizer $\pi_\nu \in \mathcal{O}_\nu$ and by

$\chi_\nu|_{\mathcal{O}_\nu^\times}$, $\mathcal{O}_\nu^\times \cong \underset{\substack{\uparrow \\ \text{finite group}}}{M} \times$ pro-p-group

One shows: $\chi_\nu | \mathcal{O}_\nu^\times$ is of finite order.

χ_ν on $\pi_\nu^{\mathbb{Z}}$, all characters are of the form $|\pi_\nu|_\nu^s$ for some $s \in \mathbb{C}$.

Since $\prod_\nu \chi_\nu(K^\times) = 1$, then one has that s must be independent of ν; and also

for ν archimedian either $\begin{cases} K_\nu^\times = \mathbb{R}^\times = \mathbb{R}_{>0}^\times \{\pm 1\} \\ K_\nu^\times = \mathbb{C}^\times \end{cases}$

maybe wrong

Def. A Hecke-character χ is algebraic iff $\exists n_1, \dots, n_d \in \mathbb{Z}$ $(d := [K:\mathbb{Q}])$ s.t.

$$\chi|_{(K \otimes_{\mathbb{Q}} \mathbb{R})^\times} = \sigma_{1,\infty}^{n_1} \cdots \sigma_{d,\infty}^{n_d}$$

($\sigma_{1,\infty}, \dots, \sigma_{d,\infty}$ are the embeddings $K \hookrightarrow \mathbb{C}$)

Def. A p-adic Hecke-Character $\chi : C_K \longrightarrow \overline{\mathbb{Q}_p}^\times$ is algebraic iff. $\exists\, U \underset{\text{open}}{\leq} (K \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times$:

$$\chi|_K = \sigma_{1,p}^{n_1} \cdots \sigma_{d,p}^{n_d} \quad \text{for some } n_1, \dots, n_d \in \mathbb{Z},\ d = [K:\mathbb{Q}]$$

($\sigma_{1,p}, \dots, \sigma_{d,p}$ are the embeddings $K \hookrightarrow \overline{\mathbb{Q}_p}$)

Def. Let χ be an algebraic Hecke-Character. Then $w := \underbrace{\chi|_{(K \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times}}_{= \sigma_{1,\infty}^{n_1} \cdots \sigma_{d,\infty}^{n_d}}$ is the weight of χ.

We define $d_{w,\infty} : C_K \longrightarrow \mathbb{C}^\times$ by $d_{w,\infty}|_{(K \otimes_{\mathbb{Q}} \mathbb{R})^\times} = w$, trivial on $K_\nu^\times$ $\forall \nu \neq \infty$.

$d_{w,p} : C_K \longrightarrow \overline{\mathbb{Q}_p}^\times$ by $d_{w,p}|_{(K \otimes_{\mathbb{Q}} \mathbb{R})^\times} = \sigma_{1,p}^{n_1} \cdots \sigma_{d,p}^{n_d}$, trivial on $K_\nu^\times$ for $\nu \neq p$.

Fix from the beginning $\overline{\mathbb{Q}_p} \cong \mathbb{C}$ (as fields); $\sigma_{i,p}$ is the embedding corresponding to $\sigma_{i,\infty}$.

From χ we define a p-adic Hecke-character:

First consider $\underbrace{\chi \cdot d_{w,\infty}^{-1} : C_K \longrightarrow \mathbb{C}^\times}_{(*)\ \text{takes values in some number field}}$

(*) $\underline{K=\mathbb{Q}}: \chi: C_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \cong \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^{\times} \longrightarrow \mathbb{C}^{\times}$

In this case an algebraic Hecke character is $\chi = d_{W,\infty} \cdot \underbrace{\eta}_{\text{some finite order character}}$

Then $\chi d_{W,\infty}^{-1} = \eta$ finite order character $\Rightarrow$ takes values in a number field.

(General case: more complicated / next time)

Then one can look at $\chi d_{W,\infty}^{-1}$ as a $\overline{\mathbb{Q}}_p^{\times}$-valued character (take an embedding $M \hookrightarrow \overline{\mathbb{Q}}_p$)

and define $\chi_p = \underbrace{\chi \cdot d_{W,\infty}^{-1}}\cdot \underbrace{d_{W,p}}: C_K \longrightarrow \overline{\mathbb{Q}}_p$

$\mathbb{Q}_p$-valued character.

Now we have a family $\{\chi_\nu\}_\nu$ of p-adic Hecke-characters. Via $\widehat{C}_K \xrightarrow{\cong} G_K^{ab}$ one gets for every ν a character $\psi_\nu: G_K \longrightarrow \overline{K}_\nu^{\times}$.

The collection $\{\psi_\nu\}_\nu$ is a compatible family of Galois characters. Assume that χ is unramified outside of $S \ni \infty$

Def.

1). χ_ν ν-adic Hecke-character; We say χ_ν is unramified at a place w of K if

$$\chi_\nu(\mathcal{O}_w^{\times}) = 1$$

2) ψ_ν a ν-adic Galois-character; we say ψ_ν is unramified at w if $\psi_\nu(I_w) = 1$.

<u>Fact 1</u>: If χ_ν is unramified at w, then the galois character attached to χ_ν by class field theory is unramified at w (and vice versa)

1) The character ψ_ν is unramified outside $S \cup \{\nu\}$ (S a set independent of ν)

2) For $w \notin S$ the image $\psi_\nu(\text{Frob}\ w)$ is "independent" of $\nu (\nmid w)$

any lift of Frobenius

1) follows from Fact 1.

2) One computes: $\psi_v(\mathrm{Frob}_w) = \chi_v(\pi_w) = \chi(\pi_w)\cdot \underbrace{d_{w,\infty}^{-1}(\pi_w)}_{=1} \cdot \underbrace{d_{w,v}(\pi_w)}_{=1} = \chi(\pi_w) \in \overline{\mathbb{Q}}_p$

independent of choice of uniformizer — uniformizer at w

w place at K, $w \notin S$

$v \notin S \cup \{w\}$

(fix v, $v|p$)

$$\begin{tikzcd}
\text{algebraic Hecke characters} \arrow[r] \arrow[d, "\text{previous constructions}"'] & \text{compatible family of galois characters} \arrow[d, "\text{take } v\text{-adic member}"] \\
p\text{-adic Hecke character} \arrow[r, "\text{not surjective}"'] & p\text{-adic galois character} \\
\text{p-adic, algebraic Hecke character unramified outside } S \arrow[u, hook] \arrow[r, "\text{CFT}"'] & \text{p-adic galois character unramified outside } S \arrow[u, hook]
\end{tikzcd}$$

__Deforming p-adically:__

Fix $p>0$, K p-adic field, L number field, $\mathcal{O}_K$ ring of integers in K, k residue field.

$L_\infty := L\otimes_{\mathbb{Q}}\mathbb{R}$, $L_\infty^\times \supseteq (\hat{L_\infty})^\circ$

$L_p := L\otimes_{\mathbb{Q}}\mathbb{Q}_p \supseteq \mathcal{O}_{L,p} := \mathcal{O}_L\otimes_{\mathbb{Z}}\mathbb{Z}_p \supseteq \mathcal{O}_{L,p}^\times$.

H = abelian profinite group with an open subgroup isomorphic to $\mathbb{Z}_p^n$ for some n

$\hat{\mathcal{C}}_{W(k)}$ = category of local complete noetherian $W(k)$-algebras with residue field k.

Fix a character $\overline{\chi}: H \longrightarrow k^\times$.

We know that the deformation functor $\hat{\mathcal{C}}_{W(k)} \longrightarrow \underline{\mathrm{Set}}$ for $\overline{\chi}$ is representable by some ring

$$R_H \in \hat{\mathcal{C}}_{W(k)}$$

__Remarks:__ (1) If $H \cong H_1\times H_2$, then one can represent deformations of $\chi|_{H_1}$, $\chi|_{H_2}$ and $R_H \cong R_{H_1}\hat{\otimes}_{W(k)} R_{H_2}$

(2) Structure theorem for abelian profinite groups $\Rightarrow$ $H \cong \underbrace{H^1}_{\text{finite group}} \times \mathbb{Z}_p^n$