Computing Galois Groups Arising From Automorphic Forms

Universiteit Leiden Université Paris-Saclay

Edward Coto Mora

Advised by Gaëtan Chenevier

ALGANT MASTER

Academic Year 2019/2020

Section I

Analize the compatible system of p-adic representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ which arise from certain cuspidal automorphic representations Π of $GL_{2n+1}(\mathbb{A})$.

Section I

Analize the compatible system of p-adic representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ which arise from certain cuspidal automorphic representations Π of $GL_{2n+1}(\mathbb{A})$.

$$\Pi = \bigotimes_{p}{}' \Pi_p$$

Section I

Analize the compatible system of p-adic representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ which arise from certain cuspidal automorphic representations Π of $GL_{2n+1}(\mathbb{A})$.

$$\Pi = \bigotimes_{p}{}' \Pi_p$$

(St) - There exists a finite place s.t. Π_q is the Steinberg representation, and Π_p is unramified for all $p \neq q \longrightarrow$ Satake parameter's: ϕ_p.

Section I

Analize the compatible system of p-adic representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ which arise from certain cuspidal automorphic representations Π of $GL_{2n+1}(\mathbb{A})$.

$$\Pi = \bigotimes_p{}' \Pi_p$$

(St) - There exists a finite place s.t. Π_q is the Steinberg representation, and Π_p is unramified for all $p \neq q \longrightarrow$ Satake parameter's: ϕ_p.

(Coh) - The infinitesimal character of Π_∞ is the infinitesimal character of the trivial representation of $GL_{2n+1}(\mathbb{R})$

Section I

Analize the compatible system of p-adic representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ which arise from certain cuspidal automorphic representations Π of $GL_{2n+1}(\mathbb{A})$.

$$\Pi = \bigotimes_p{}' \Pi_p$$

(St) - There exists a finite place s.t. Π_q is the Steinberg representation, and Π_p is unramified for all $p \neq q \longrightarrow$ Satake parameter's: ϕ_p.

(Coh) - The infinitesimal character of Π_∞ is the infinitesimal character of the trivial representation of $GL_{2n+1}(\mathbb{R})$

- $R_l(x)$ the characteristic polynomial of ϕ_{Π_l} factors as $R_l(x) = P_l(x)(x-1)$, with $P_l(x)$ palindromic in $\mathbb{Z}[\frac{1}{l}][x]$.

Theorem

There exists a compatible system of p-adic representations

$$\rho_p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_{2n+1}(\mathbb{Q}_p)$$

such that for all $p \neq q$ the image of ρ_p is contained in a split orthogonal group $SO_{2n+1}(\mathbb{Q}_p)$.

Section II

Examine an example of an automorphic representations π which was constructed on an anisotropic form of G_2.

Section II

Examine an example of an automorphic representations π which was constructed on an anisotropic form of G_2.

(Gross, Savin) π lifts to an automorphic representation σ of Sp_6.

Section II

Examine an example of an automorphic representations π which was constructed on an anisotropic form of G_2.

(Gross, Savin) π lifts to an automorphic representation σ of Sp_6.

(Arthur) σ lifts to an automorphic representation of II. This lift is cuspidal, and satisfies the (St) condition.

Section II

Examine an example of an automorphic representations π which was constructed on an anisotropic form of G_2.

(Gross, Savin) π lifts to an automorphic representation σ of Sp_6.

(Arthur) σ lifts to an automorphic representation of II. This lift is cuspidal, and satisfies the (St) condition.

Proposition

The splitting fields of $P_2(x)$ and $P_3(x)$, the characteristic polynomials associated to the corresponding Satake parameters π_2, π_3, have the Galois group isomorphic to D_6 and are algebraically independent.

Section III

We further analyze the Galois representations that arise from Π, the automorphic representation which lifts from π .

Section III

We further analyze the Galois representations that arise from Π, the automorphic representation which lifts from π .

Theorem

There exists a compatible system of p-adic representations

$$\rho_p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_7(\mathbb{Q}_p)$$

such that for all $p \neq 5$ the Zariski closure of the image is $G_2(\mathbb{Q}_p)$.

Section III

We further analyze the Galois representations that arise from Π, the automorphic representation which lifts from π .

Theorem

There exists a compatible system of p-adic representations

$$\rho_p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_7(\mathbb{Q}_p)$$

such that for all $p \neq 5$ the Zariski closure of the image is $G_2(\mathbb{Q}_p)$.

Theorem (Kay Magaard, Gordan Savin)

There is a set of primes S of density 1, such that for all $p \in S$, there exists an extension of $\mathbb{Q}$ with $G_2(p)$ as its Galois group which ramifies only at 5 and p.

Suppose that Π is cuspidal automorphic representations of $GL_{2n+1}(\mathbb{A})$ such that:

$$\Pi = \bigotimes_p{}' \Pi_p$$

Suppose that Π is cuspidal automorphic representations of $GL_{2n+1}(\mathbb{A})$ such that:

$$\Pi = \bigotimes_p{}' \Pi_p$$

(St) - There exists a finite place s.t. Π_q is the Steinberg representation, and Π_p is unramified for all $p \neq q \longrightarrow$ Satake parameter's: ϕ_{Π_p}.

(Coh) - The infinitesimal character of Π_∞ is the infinitesimal character of the trivial representation of $GL_m(\mathbb{R})$

Suppose that Π is cuspidal automorphic representations of $GL_{2n+1}(\mathbb{A})$ such that:

$$\Pi = \bigotimes_p{}' \Pi_p$$

(St) - There exists a finite place s.t. Π_q is the Steinberg representation, and Π_p is unramified for all $p \neq q \longrightarrow$ Satake parameter's: ϕ_{Π_p}.

(Coh) - The infinitesimal character of Π_∞ is the infinitesimal character of the trivial representation of $GL_m(\mathbb{R})$

- $R_l(x)$ the characteristic polynomial of ϕ_{Π_l} factors as $R_l(x) = P_l(x)(x-1)$, with $P_l(x)$ palindromic in $\mathbb{Z}[\frac{1}{l}][x]$.

(In particular Π is self dual.)

The work of Harris-Taylor and Taylor-Yoshida yields:

For every prime p there exists a semisimple continuous representation

$$\rho_p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_{2n+1}(\bar{\mathbb{Q}}_p)$$

such that:

- ρ_p *is unramified at all primes* $l \neq p, q$.
- $R_l(X)$ *is the characteristic polynomial of* $\rho_p(Fr_l)$.
- *For all* $p \neq q$ *the representation* ρ_p *is irreducible.*

Proposition

If $p \neq q$ then ρ_p is defined over $\mathbb{Q}_p$.

$$\rho_p^{\mathbb{Q}} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_{2n+1}(\mathbb{Q}_p)$$

Proposition

If $p \neq q$ then ρ_p is defined over $\mathbb{Q}_p$.

$$\rho_p^{\mathbb{Q}} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_{2n+1}(\mathbb{Q}_p)$$

Outline of the proof.

- Let Γ be the image of ρ_p and consider the algebra $A = \mathbb{Q}_p[\Gamma] \subset M_m(\bar{\mathbb{Q}}_p)$.

Proposition

If $p \neq q$ then ρ_p is defined over $\mathbb{Q}_p$.

$$\rho_p^{\mathbb{Q}} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_{2n+1}(\mathbb{Q}_p)$$

Outline of the proof.

- Let Γ be the image of ρ_p and consider the algebra $A = \mathbb{Q}_p[\Gamma] \subset M_m(\bar{\mathbb{Q}}_p)$.
- A is simple. So $A \cong M_r(D)$ for some division algebra D. Observe $A \otimes \bar{\mathbb{Q}} = M_m(\bar{\mathbb{Q}_p})$,

Proposition

If $p \neq q$ then ρ_p is defined over $\mathbb{Q}_p$.

$$\rho_p^{\mathbb{Q}} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_{2n+1}(\mathbb{Q}_p)$$

Outline of the proof.

- Let Γ be the image of ρ_p and consider the algebra $A = \mathbb{Q}_p[\Gamma] \subset M_m(\bar{\mathbb{Q}}_p)$.
- A is simple. So $A \cong M_r(D)$ for some division algebra D. Observe $A \otimes \bar{\mathbb{Q}} = M_m(\bar{\mathbb{Q}_p})$,
- $trd(\rho_p(Fr_l)) \in \mathbb{Q}$ for $l \neq p$ implies D is a central simple algebra over $\mathbb{Q}_p$.

Proposition

If $p \neq q$ then ρ_p is defined over $\mathbb{Q}_p$.

$$\rho_p^{\mathbb{Q}} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_{2n+1}(\mathbb{Q}_p)$$

Outline of the proof.

- Let Γ be the image of ρ_p and consider the algebra $A = \mathbb{Q}_p[\Gamma] \subset M_m(\bar{\mathbb{Q}}_p)$.
- A is simple. So $A \cong M_r(D)$ for some division algebra D. Observe $A \otimes \bar{\mathbb{Q}} = M_m(\bar{\mathbb{Q}_p})$,
- $trd(\rho_p(Fr_l)) \in \mathbb{Q}$ for $l \neq p$ implies D is a central simple algebra over $\mathbb{Q}_p$.
- D^r is a sum of the two eigenspaces for $\rho_p(c)$. And $Tr(\rho_p(c)) = \pm 1$.

Proposition

If $p \neq q$ then ρ_p is defined over $\mathbb{Q}_p$.

$$\rho_p^{\mathbb{Q}} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_{2n+1}(\mathbb{Q}_p)$$

Outline of the proof.

- Let Γ be the image of ρ_p and consider the algebra $A = \mathbb{Q}_p[\Gamma] \subset M_m(\bar{\mathbb{Q}}_p)$.
- A is simple. So $A \cong M_r(D)$ for some division algebra D. Observe $A \otimes \bar{\mathbb{Q}} = M_m(\bar{\mathbb{Q}_p})$,
- $trd(\rho_p(Fr_l)) \in \mathbb{Q}$ for $l \neq p$ implies D is a central simple algebra over $\mathbb{Q}_p$.
- D^r is a sum of the two eigenspaces for $\rho_p(c)$. And $Tr(\rho_p(c)) = \pm 1$.
- $D = \mathbb{Q}_p$ and $m = r$, thus $A \cong M_m(\mathbb{Q}_p)$.

Proposition

If $p \neq q$ then the image of ρ_p is contained in a split orthogonal group $SO_{2n+1}(\mathbb{Q}_p)$.

Proposition

If $p \neq q$ then the image of ρ_p is contained in a split orthogonal group $SO_{2n+1}(\mathbb{Q}_p)$.

Outline of the proof.

- ρ_p is self dual and irreducible, thus it has an unique (up to scalar multiple) invariant non-degenerate bilinear form.

Proposition

If $p \neq q$ then the image of ρ_p is contained in a split orthogonal group $SO_{2n+1}(\mathbb{Q}_p)$.

Outline of the proof.

- ρ_p is self dual and irreducible, thus it has an unique (up to scalar multiple) invariant non-degenerate bilinear form.
- Since m is odd, the form has to be orthogonal.

Proposition

If $p \neq q$ then the image of ρ_p is contained in a split orthogonal group $SO_{2n+1}(\mathbb{Q}_p)$.

Outline of the proof.

- ρ_p is self dual and irreducible, thus it has an unique (up to scalar multiple) invariant non-degenerate bilinear form.
- Since m is odd, the form has to be orthogonal.
- Since ρ_p is defined over $\mathbb{Q}_p$, the orthogonal form can be re-scaled so that it is also defined over $\mathbb{Q}_p$.

Proposition

If $p \neq q$ then the image of ρ_p is contained in a split orthogonal group $SO_{2n+1}(\mathbb{Q}_p)$.

Outline of the proof.

- ρ_p is self dual and irreducible, thus it has an unique (up to scalar multiple) invariant non-degenerate bilinear form.
- Since m is odd, the form has to be orthogonal.
- Since ρ_p is defined over $\mathbb{Q}_p$, the orthogonal form can be re-scaled so that it is also defined over $\mathbb{Q}_p$.
- Finally since the determinant of $\rho_p(Fr_l) = 1$ for all primes $l \neq p, q$ and these elements are dense in the image the image is contained in $SO_{2n+1}(\mathbb{Q}_p)$.

Proposition

If $p \neq q$ then the image of ρ_p is contained in a split orthogonal group $SO_{2n+1}(\mathbb{Q}_p)$.

Outline of the proof.

- ρ_p is self dual and irreducible, thus it has an unique (up to scalar multiple) invariant non-degenerate bilinear form.
- Since m is odd, the form has to be orthogonal.
- Since ρ_p is defined over $\mathbb{Q}_p$, the orthogonal form can be re-scaled so that it is also defined over $\mathbb{Q}_p$.
- Finally since the determinant of $\rho_p(Fr_l) = 1$ for all primes $l \neq p, q$ and these elements are dense in the image the image is contained in $SO_{2n+1}(\mathbb{Q}_p)$.
- There are two isomorphism classes of odd orthogonal groups over $\mathbb{Q}_p$, but only the split isomorphism class contains the regular unipotent conjugacy

Section II - Automorphic representation of $G_2(\mathbb{A})$

Let G be the unique form over $\mathbb{Q}$, of the exceptional Lie group of type G_2 such that $G(\mathbb{R})$ is compact and $G(\mathbb{Q}_p)$ is split for all primes p.

Section II - Automorphic representation of $G_2(\mathbb{A})$

Let G be the unique form over $\mathbb{Q}$, of the exceptional Lie group of type G_2 such that $G(\mathbb{R})$ is compact and $G(\mathbb{Q}_p)$ is split for all primes p.

Savin and Gross proved the existence of an automorphic representation π of $G(\mathbb{A})$ satisying:

(i) $\pi_\infty \cong \mathbb{C}$

(ii) π_5 *is the Steinberg Representation*

(iii) π_l *is unramified for all primes* $l \neq 5$.

The characteristic polynomial $R_l(x)$ *of the Satake parameter* $s_l \in G_2(\mathbb{C})$ *of* π_l, *acting on the 7-dimensional representation has coefficients in* $\mathbb{Z}[\frac{1}{l}]$.

Moreover π *lifts to an automorphic representation* σ *on* $Sp_6(\mathbb{A})$

Lansky and Pollack have calculated the polynomial $R_l(x)$ for $l = 2$ and 3:

$$R_2(x) = x^7 + \frac{1}{4}x^6 - x^5 - \frac{13}{16}x^4 + \frac{13}{16}x^3 + x^2 - \frac{1}{4}x - 1$$

$$R_3(x) = x^7 + \frac{29}{3^3}x^6 - \frac{175}{3^5}x^5 - \frac{1099}{3^6}x^4 + \frac{1099}{3^6}x^3 + \frac{175}{3^5}x^2 - \frac{29}{3^3}x - 1$$

Lansky and Pollack have calculated the polynomial $R_l(x)$ for $l = 2$ and 3:

$$R_2(x) = x^7 + \frac{1}{4}x^6 - x^5 - \frac{13}{16}x^4 + \frac{13}{16}x^3 + x^2 - \frac{1}{4}x - 1$$

$$R_3(x) = x^7 + \frac{29}{3^3}x^6 - \frac{175}{3^5}x^5 - \frac{1099}{3^6}x^4 + \frac{1099}{3^6}x^3 + \frac{175}{3^5}x^2 - \frac{29}{3^3}x - 1$$

After factoring $R_l(x) = P_l(X)(x - 1)$, the two palindromic polynomials $P_l(x)$ are reduced to:

$$Q_2(y) = y^3 + \frac{5}{4}y^2 - \frac{11}{4}y - \frac{49}{16}$$

$$Q_3(y) = y^3 - \frac{2}{3^3}y^2 - \frac{572}{3^5}y - \frac{520}{3^6}$$

Proposition

The local components π_2 and π_3 are tempered. The splitting fields of $P_2(x)$ and $P_3(x)$ have the Galois group isomorphic to D_6 and are algebraically independent.

Proposition

The local components π_2 and π_3 are tempered. The splitting fields of $P_2(x)$ and $P_3(x)$ have the Galois group isomorphic to D_6 and are algebraically independent.

Outline of the proof.

- $\Delta_l > 0$ so the polynomials $Q_l(y)$ have 3 real roots each.

Proposition

The local components π_2 and π_3 are tempered. The splitting fields of $P_2(x)$ and $P_3(x)$ have the Galois group isomorphic to D_6 and are algebraically independent.

Outline of the proof.

- $\Delta_l > 0$ so the polynomials $Q_l(y)$ have 3 real roots each.
- Moreover the roots are in the segment $(-2, 2)$.

Proposition

The local components π_2 and π_3 are tempered. The splitting fields of $P_2(x)$ and $P_3(x)$ have the Galois group isomorphic to D_6 and are algebraically independent.

Outline of the proof.

- $\Delta_l > 0$ so the polynomials $Q_l(y)$ have 3 real roots each.
- Moreover the roots are in the segment $(-2, 2)$.
- The roots of $Q(y)$ lie in the interval $(-2, 2)$ if and only if, the roots of $P(x)$ are pairs of complex conjugates on the unit circle.

Proposition

The local components π_2 and π_3 are tempered. The splitting fields of $P_2(x)$ and $P_3(x)$ have the Galois group isomorphic to D_6 and are algebraically independent.

Outline of the proof.

- $\Delta_l > 0$ so the polynomials $Q_l(y)$ have 3 real roots each.
- Moreover the roots are in the segment $(-2, 2)$.
- The roots of $Q(y)$ lie in the interval $(-2, 2)$ if and only if, the roots of $P(x)$ are pairs of complex conjugates on the unit circle.
- Since Δ_2 and Δ_3 are not rational squares, it follows that the Galois group of $Q_2(y)$ and $Q_3(y)$ is S_3.

Savin and Gross has also shown that π lifts to a cuspidal automorphic representation σ on $Sp_6(\mathbb{A})$ satisfying:

(1) *σ_∞ is a holomorphic discrete series representation.*

(2) *σ_5 is the Steinberg representation.*

(3) *σ_l is an unramified representation, a lift from $G_2(\mathbb{Q}_l)$, for $l \neq 5$.*

(4) *σ_2 and σ_3 are tempered with Satake parameters given by $R_2(x)$ and $R_3(x)$.*

Proposition (Arthur)

Let σ be a cuspidal automorphic representation on Sp_{2n}, such that σ_q is the Steinberg representation for a prime q. Then σ lifts to Π an automorphic representation of GL_{2n+1}.

Proposition (Arthur)

Let σ be a cuspidal automorphic representation on Sp_{2n}, such that σ_q is the Steinberg representation for a prime q. Then σ lifts to Π an automorphic representation of GL_{2n+1}.

- Then Π_q is the Steinberg Representation.
- Π is cuspidal.
- Moreover Π is a functorial lift of σ.

So far we have achieve the following:

Theorem

There exists a compatible system of p-adic representations

$$\rho_p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_7(\mathbb{Q}_p)$$

such that for all $p \neq q$ the image of ρ_p is contained in a split orthogonal group $SO_7(\mathbb{Q}_p)$.

For $l \neq q$, let E_l denote the splitting field of $P_l(x)$.

We know $Gal(E_3/\mathbb{Q}) \cong D_6$.

For $l \neq q$, let E_l denote the splitting field of $P_l(x)$.

We know $Gal(E_3/\mathbb{Q}) \cong D_6$.

Corollary

Let G be the Zarisky closure of the image of ρ_p. Then $G(\mathbb{Q}_p) = G_2(\mathbb{Q}_p)$ for all primes $p \neq q, 3$.

For $l \neq q$, let E_l denote the splitting field of $P_l(x)$.

We know $Gal(E_3/\mathbb{Q}) \cong D_6$.

Corollary

Let G be the Zarisky closure of the image of ρ_p. Then $G(\mathbb{Q}_p) = G_2(\mathbb{Q}_p)$ for all primes $p \neq q, 3$.

Outline of the Proof.

- G is a reductive group.

For $l \neq q$, let E_l denote the splitting field of $P_l(x)$.

We know $Gal(E_3/\mathbb{Q}) \cong D_6$.

Corollary

Let G be the Zarisky closure of the image of ρ_p. Then $G(\mathbb{Q}_p) = G_2(\mathbb{Q}_p)$ for all primes $p \neq q, 3$.

Outline of the Proof.

- G is a reductive group.
- Π locally lift from G_2 implies a a condition on the coefficients of $Q_l(x)$ of the form $a^2 = c^2 + 2b + 4$. Thus the rank of G is at most 2.

For $l \neq q$, let E_l denote the splitting field of $P_l(x)$.

We know $Gal(E_3/\mathbb{Q}) \cong D_6$.

Corollary

Let G be the Zarisky closure of the image of ρ_p. Then $G(\mathbb{Q}_p) = G_2(\mathbb{Q}_p)$ for all primes $p \neq q, 3$.

Outline of the Proof.

- G is a reductive group.
- Π locally lift from G_2 implies a a condition on the coefficients of $Q_l(x)$ of the form $a^2 = c^2 + 2b + 4$. Thus the rank of G is at most 2.
- The connected component G^0 of 1 contains the regular unipotent class.

- Thus G^0 is either $G_2(\mathbb{Q}_p)$ or $PGL_2(\mathbb{Q}_p)$.

- Thus G^0 is either $G_2(\mathbb{Q}_p)$ or $PGL_2(\mathbb{Q}_p)$.
- These two groups are self-normalizing in $SO_7(\mathbb{Q}_p)$, implies $G(\mathbb{Q}_p) \cong G_2(\mathbb{Q}_l)$ or $PGL_2(\mathbb{Q}_p) \cong G_2(\mathbb{Q}_l)$.

- Thus G^0 is either $G_2(\mathbb{Q}_p)$ or $PGL_2(\mathbb{Q}_p)$.
- These two groups are self-normalizing in $SO_7(\mathbb{Q}_p)$, implies $G(\mathbb{Q}_p) \cong G_2(\mathbb{Q}_l)$ or $PGL_2(\mathbb{Q}_p) \cong G_2(\mathbb{Q}_l)$.
- Now if the latter happens, for every $l \neq p, q$, the roots of $P_l(x)$ are z^i, where $-3 \leq i \leq 3$, for some $z \in \mathbb{C}^\times$.

Section III - Main Theorem

We get the following:

We get the following:

Theorem

There exists a compatible system of p-adic representations

$$\rho_p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_7(\mathbb{Q}_p)$$

such that for all $p \neq 5$ the Zariski closure of the image is $G_2(\mathbb{Q}_p)$.

We get the following:

Theorem

There exists a compatible system of p-adic representations

$$\rho_p : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_7(\mathbb{Q}_p)$$

such that for all $p \neq 5$ the Zariski closure of the image is $G_2(\mathbb{Q}_p)$.

We want:

Theorem

There exists an extension of $\mathbb{Q}$ with $G_2(p)$ as the Galois group, ramified at 5 and p only, for a set of primes p of density 1.

Theorem (Larsen:)

$G_2(p)$ appears as a quotient of the image for a set of primes p of density one.

Theorem

There exists an extension of $\mathbb{Q}$ with $G_2(p)$ as the Galois group, ramified at 5 and p only, for a set of primes p of density 1.

Theorem

There exists an infinite sequence of primes $l_1, l_2, \ldots$ such that $Gal(E_{l_j}/\mathbb{Q}) \cong D_6$ and the fields E_j are linearly independent, i.e. the composite of any n of them has degree 12^n

Theorem

Let $C_1, \ldots, C_n$ be semi-simple, regular, conjugacy classes in $G_2(\mathbb{Q})$. Assume that the Galois groups of the splitting fields E_{C_i} of the characteristic polynomials $P_{C_i}(x)$ are all isomorphic to the dihedral group D_6 and that they are linearly independent, i.e. the composite of all these fields has degree 12^n. Assume that for almost all primes p we are given $g_i \in C_i(\mathbb{Q}_p), i = 1, \ldots, n$, and a maximal compact subgroup U_p in $G_2(\mathbb{Q}_p)$ containing g_i. Then, for a set of primes of density at least

$$1 - 2(\frac{5}{6})^n + 4(\frac{4}{6})^n$$

the group U_p is hyperspecial and the projections of g_i generate the reductive quotient of U_p isomorphic to $G_2(p)$.