# SERRE'S CONJECTURE AND BASE CHANGE FOR $GL(2)$

HARUZO HIDA

## 1. Quaternion class sets

A quaternion algebra $B$ over a field $F$ is a simple algebra of dimension 4 central over a field $F$. A prototypical example is the $2 \times 2$ matrix algebra $M_2(F)$ over $F$ and the Hamilton quaternion algebra over $\mathbb{R}$ given by $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ such that $ij = k = -ji$, $jk = i = -ki$ and $ki = j = -ik$ with $i^2 = j^2 = k^2 = -1$. Of course, its rational version $H = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ makes perfect sense and gives an example of quaternion algebras over $\mathbb{Q}$. The algebra $H$ has a reduced norm map $N : H^\times \to \mathbb{Q}^\times$ and the reduced trace map $\mathrm{Tr} : H \to \mathbb{Q}$ given by $N(x) = x\overline{x} \in \mathbb{Q}^\times$ and $\mathrm{Tr}(x) = x + \overline{x}$ for $\overline{x} = a - bi - cj - dk$ if $x = a + bi + cj + dk$. It is easy to check that $X^2 - \mathrm{Tr}(x)X + N(x)$ is the minimal equation $x$ satisfies in $B$ if $x \notin \mathbb{Q}$. Since $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$, $N^{-1}(1)$ is a finite set.

Pick a quaternion algebra $B$ over $\mathbb{Q}$ and suppose that $B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$. Such a quaternion algebra is called a definite quaternion algebra. These algebras were intensely studied in the late 19th to the early 20th century by a handful of outstanding German algebraists along with class field theory. One of the hope they (particularly E. Artin) had was to create a theory parallel to class field theory in a nonabelian setting, but unfortunately, they only found a new proof of class field theory (Weil's book: "basic number theory"), returning to the abelian setting. By a result of Hasse at the time, any set $\Sigma_B$ of odd number of primes, there exists a unique isomorphism class of definite quaternion algebras $B_{/\mathbb{Q}}$ such that $B_\ell = B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is a division algebra if and only if $\ell \in \Sigma_B$.

When a totally real number field $F$ with integer ring $O$ is given, two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $O$ in $F$ are called equivalent (written as $\mathfrak{a} \sim \mathfrak{b}$) if $\mathfrak{a} = \alpha\mathfrak{b}$ for an element $\alpha \in F_+^\times$, where $F_+^\times$ are made up of elements whose conjugates in $\mathbb{R}$ are all positive (totally positive). The equivalence classes $Cl_F$ form a finite group under ideal multiplication. For a relative setting of field extensions $F/E$, we have the norm map $N_{F/E} : F^\times \to E^\times$ (and the trace map) which induces the norm map of class group $N_{F/E} : Cl_F \to Cl_E$. Any fractional $E$-ideal $\mathfrak{a}$ can be extended to a fractional $F$-ideal by $\mathfrak{a} \mapsto \mathfrak{a}O$, getting a homomorphism $i_{F/E} : Cl_E \to Cl_F$. The norm map $N_{F/E}$ and

*Date*: July 4, 2006.

A colloquium talk at Columbia university on 4/19/2006 and a number theory seminar talk at Boston university 4/24/06; The author is partially supported by the NSF grant: DMS 0244401 and DMS 0456252.

$i_{F/E}$ are a sort of dual under Kummer's theory for cyclotomic fields $F/E$, and this duality has been exploited much by Iwasawa theorists.

The algebra $B$ has a maximal order $R$, which is maximal among subrings of $B$ free of rank 4 over $\mathbb{Z}$. A finite submodule $\mathfrak{a} \subset B$ is called a fractional right ideal if $\mathfrak{a}R \subset \mathfrak{a}$ and $\mathbb{Q}\mathfrak{a} = B$. We can think of an equivalence between right fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $B$. In other words, $\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \mathfrak{a} = \alpha\mathfrak{b}$ (left multiplication) for $\alpha \in B^\times$. The resulting set $Cl_B$ of equivalence classes is a finite set (not a group, because $\mathfrak{a}^{-1}$ is a left ideal). Even we take a totally real field extension $F/E$, we do not have a good definition of the norm map of $Cl_{B_F} \to Cl_{B_E}$ for $B_F = B \otimes_{\mathbb{Q}} F$ and $B_E = B \otimes_{\mathbb{Q}} E$. Since $B_E \subset B_F$ naturally, we still have $\iota_{F/E} : Cl_{B_E} \to Cl_{B_F}$.

## 2. Hecke operators

We have the reduced norm map $N : B_F^\times \to F^\times$, which induces maps

$$\{\text{right fractional ideals of } B_F\} \to \{\text{fractional ideals of } F\}$$

and $Cl_{B_F} \to Cl_F$. Write $\mathcal{M}_F$ for the space of functions $f : Cl_{B_F} \to \mathbb{C}$. Then we have Hecke operators $T(\mathfrak{n})$ for nonzero $O$-ideals $\mathfrak{n}$. Take a right ideal $\mathfrak{x}$ with $N(\mathfrak{x}) = \mathfrak{n}$. Then $\mathfrak{a}\mathfrak{x} \in Cl_{B_F}$, and we have

$$f|T(\mathfrak{n})(\mathfrak{a}) = \sum_{\mathfrak{x}: N(\mathfrak{x})=\mathfrak{n}} f(\mathfrak{a}\mathfrak{x}).$$

A marvelous fact Eichler found in the 1950s to 60s is that as modules with an action of Hecke operators $T(n)$, $\mathcal{M}_{\mathbb{Q}}$ is isomorphic to a subspace of modular forms on $\Gamma_0(d(B))$ of weight 2, where $d(B) = \prod_{\ell \in \Sigma_B} \ell$. This is generalized to any field $F$ by Jacquet-Langlands; so, $\mathcal{M}_F$ as a Hecke module is equivalent to a subspace of Hilbert modular forms over $F$ of weight 2.

We write $\mathbb{T}_F$ for the $\mathbb{C}$-subalgebra of $\mathrm{End}(\mathcal{M}_F)$ generated by Hecke operators. Then $\mathbb{T}_F$ is a commutative semi-simple algebra, and $\mathcal{M}_F \cong \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_F, \mathbb{C})$ as $\mathbb{T}_F$-modules. Since $\mathbb{T}_F$ is a Frobenius algebra (or a Gorenstein ring), we have $\mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_F, \mathbb{C}) \cong \mathbb{T}_F$ as $\mathbb{T}_F$-module; so, $\mathcal{M}_F \cong \mathbb{T}_F$ as $\mathbb{T}_F$-modules.

The reduced norm map $N : B_F^\times \to F^\times$ induces a map $\nu : Cl_{B_F} \to Cl_F$. We write $Cl^{(1)}_{B_F} := \nu^{-1}([O])$ for the kernel of this map ($[O] \in Cl_F$). We can think of the space $\mathcal{M}^{(1)}_F$ of functions on $Cl^{(1)}_{B_F}$ with values in $\mathbb{C}$, on which we have Hecke operators $T(\mathfrak{n})$ as long as $[\mathfrak{n}] = 1$ in $Cl_F$. Write $\mathbb{T}^{(1)}_F$ for the $\mathbb{C}$-subalgebra of $\mathrm{End}(\mathcal{M}^{(1)}_F)$ generated by Hecke operators. Then $\mathbb{T}^{(1)}_F$ is again a commutative semi-simple algebra. If $B_{\mathfrak{l}} = B \otimes_{\mathbb{Q}} F_{\mathfrak{l}}$ is a division algebra for at least one prime $\mathfrak{l}$, by the study of $L$-distinguishability of Langlands-Labesse (combined with the strong multiplicity one for $GL(2)$), we have a duality pairing $(\cdot,\cdot) : \mathbb{T}^{(1)}_F \times \mathcal{M}^{(1)}_F \to \mathbb{C}$ such that $(TT', f) = (T, f|T')$ for all $T, T' \in \mathbb{T}^{(1)}_F$ and $f \in \mathcal{M}^{(1)}_F$. Thus again we have $\mathcal{M}^{(1)}_F \cong \mathbb{T}^{(1)}_F$ as $\mathbb{T}_F$-modules.

## 3. A conjecture on Galois permutation representations

Suppose $F/\mathbb{Q}$ is a Galois extension with Galois group $G$. Then $G$ acts on $B_F = B \otimes_{\mathbb{Q}} F$ through the right factor $F$. We choose a maximal order $R_F$ of $B_F$ so that it is stable under $G$. Then the Galois group $G$ naturally acts on the finite set $Cl^{(1)}_{B_F}$ and hence on $\mathcal{M}^{(1)}_F$ by the pull back action. Since $\mathbb{T}^{(1)}_F$ acts on $\mathcal{M}^{(1)}_F$, we can let $g \in G$ act on $\mathbb{T}^{(1)}_F$ by $T \mapsto g \circ T \circ g^{-1}$; thus $g(T(\mathfrak{n})) = T(g(\mathfrak{n}))$. Thus $G$ acts on the finite set $\mathrm{Spec}(\mathbb{T}^{(1)}_F)(\mathbb{C}) = \mathrm{Hom}_{\mathbb{C}\text{-alg}}(\mathbb{T}^{(1)}_F, \mathbb{C})$ canonically. Here is a conjecture

**Conjecture 3.1.** *Suppose that $B_\mathfrak{l}$ is a division algebra for all primes $\mathfrak{l}$ of $F$ over $d(B)$. Then there exists a bijection $\iota : Cl^{(1)}_{B_F} \xrightarrow{\sim} \mathrm{Spec}(\mathbb{T}^{(1)}_F)(\mathbb{C})$ such that $\iota(g(a)) = g\iota(a)$ for all $g \in G$.*

Since $\mathbb{T}^{(1)}_F$ is commutative semi-simple, $\mathbb{T}^{(1)}_F \cong \mathbb{C}[\mathrm{Spec}(\mathbb{T}^{(1)}_F)(\mathbb{C})]$ as $\mathbb{C}[G]$-modules. As described in an exercise in Serre's book on linear representations of finite groups (II.13, Exercise 13.5), if $\mathbb{C}[\mathrm{Spec}(\mathbb{T}^{(1)}_F)(\mathbb{C})] \cong \mathcal{M}^{(1)}_F = \mathbb{C}[Cl^{(1)}_{B_F}]$ as $G$-modules, the two sets $\mathrm{Spec}(\mathbb{T}^{(1)}_F)(\mathbb{C})$ and $Cl^{(1)}_{B_F}$ are equivalent as $H$-sets for all cyclic subgroups $H \subset G$. Since we can make the isomorphism $\mathbb{T}^{(1)}_F \cong \mathcal{M}^{(1)}_F$ already stated $G$-equivariant (easily), we have

**Theorem 3.2.** *If $G$ is cyclic, the conjecture holds.*

## 4. Galois representations

Pick a prime $p$. By the effort of Shimura, Deligne, Carayol, Wiles, Blasius-Rogawski and R. Taylor, with each $P \in \mathrm{Spec}(\mathbb{T}_F)(\mathbb{C})$ regarded as a $\mathbb{C}$-algebra homomorphism $P : \mathbb{T}_F \to \mathbb{C}$, we can now attach a unique semi-simple $p$-adic Galois representation $\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to GL_2(\overline{\mathbb{Q}}_p)$ such that

- (G1) $\rho_P$ is unramified outside $p \cdot d(B_F)$ and $\mathrm{Tr}(\rho_P(Frob_\mathfrak{l})) = P(T(\mathfrak{l}))$ for $\mathfrak{l} \nmid p \cdot d(B_F)$, where $d(B_F)$ is the product of primes at which $B_F$ is a division algebra;
- (G2) If $\mathfrak{l} | d(B_F)$, $\rho_P$ restricted to the decomposition group $\mathrm{Gal}(\overline{F}/F_\mathfrak{l})$ is not semi-simple, and $\rho_P|_{\mathrm{Gal}(\overline{F}_\mathfrak{l}/F_\mathfrak{l})} \cong \left(\begin{smallmatrix} \alpha\chi & * \\ 0 & \alpha \end{smallmatrix}\right)$ for all $\mathfrak{l} | d(B_F)$, where $\chi$ is the $p$-adic cyclotomic character and $\alpha = P(T(\mathfrak{l}))$. In particular, $\rho_P$ is ramified at $\mathfrak{l} | d(B_F)$.

Start with $\rho_P$ for $P \in \mathrm{Spec}(\mathbb{T}_\mathbb{Q})(\mathbb{C})$, Langlands functoriality predicts the existence of $\widehat{P} \in \mathrm{Spec}(\mathbb{T}_F)(\mathbb{C})$ such that $\rho_{\widehat{P}} \cong \rho_P|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$. To prove the existence of $\widehat{P}$ is the problem of base-change. Define the inner conjugate $\rho^g_P(\sigma) = \rho_P(\widetilde{g}\sigma\widetilde{g}^{-1})$ taking an extension $\widetilde{g}$ of $g \in G$. Then we have $\rho_{g(P)} \cong \rho^g_P$. Thus if $H^2(G, \mathbb{Q}/\mathbb{Z})$ vanishes and $P$ is fixed by $G$, $\rho_P$ extends to a Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (I. Schur). The associated projective representation $\overline{\rho}_P : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to PGL_2(\overline{\mathbb{Q}}_p)$ (that is, $\rho_P$ modulo center) always extends to a unique projective representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Since $Cl^{(1)}_F$ is basically associated to the kernel of the reduced norm; so, it is associated to the derived group $B^{(1)}$ of the multiplicative group $B^\times$ as an algebraic

group over $\mathbb{Q}$. Since $B^{(1)}$ is an inner form of $SL(2)$, its Langlands dual group is $PGL(2)$. Thus each $Q \in \mathrm{Spec}(\mathbb{T}^{(1)}(\mathbb{C}))$ gives rise to a unique projective representation $\overline{\rho}_Q : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to PGL_2(\overline{\mathbb{Q}}_p)$.

## 5. Base-change with Steinberg primes

We now count the number of projective modular irreducible representations with the properties specified by (G1–2) up to character twists. Then over $\mathbb{Q}$, (forgetting about Eisenstein part), the number is given by $|Cl^{(1)}_{B_{\mathbb{Q}}}| - 1$. If Serre's conjecture holds, by the characteristic 0 lifting result of Wiles-Taylor, this number is the number of all such representations. Suppose that $d(B_F)$ is made up of all primes above primes in $\Sigma_B$. Then it is easy to check (under one more mild assumption on $\Sigma_B$) that $\iota$ sends $Cl^{(1)}_{B_{\mathbb{Q}}}$ injectively into $Cl^{(1)}_{B_F}$. Thus under the conjecture, the number of $G$-invariant modular projective representation with the specified properties over $F$ exceeds the number of restrictions to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ of such projective representations defined over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The restriction of Galois representations as above to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ is injective by a result of Ribet (or Faltings' solution of the Tate conjecture for abelian varieties). We conclude that the base-change problem is solved for $F/\mathbb{Q}$ for projective representations. If $H^q(G, \mathbb{Q}_2/\mathbb{Z}_2) = 0$ for $q = 1, 2$ (we call such group 2-simply connected), for a given compatible central character, we can lift a projective representation to a true representation uniquely. Since the 2-simple connectedness holds if $|G|$ is odd, by Theorem 3.2, we reprove the following theorem of Langlands:

**Theorem 5.1.** *Suppose that $d(B_F)$ is made up of all primes above primes in $\Sigma_B$. If $G$ is cyclic of odd order, for any $P \in \mathrm{Spec}(\mathbb{T}_{\mathbb{Q}})(\mathbb{C})$, we can find a unique point $\widehat{P} \in \mathrm{Spec}(\mathbb{T}_F)(\mathbb{C})$ such that $\rho_{\widehat{P}} \cong \rho_P|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$.*

We can do this counting process of projective representations with specific local properties among modular Galois representations. Since Langlands has already solved the base-change problem for soluble extensions $F/E$, we conclude

**Theorem 5.2.** *Suppose that $d(B_F)$ is made up of all primes above primes in $\Sigma_B$. Then the two sets $\mathrm{Spec}(\mathbb{T}^{(1)}_F)(\mathbb{C})$ and $Cl^{(1)}_{B_F}$ are equivalent as $H$-sets for all soluble subgroups $H \subset G$.*

In other word, solution of the base-change problem implies the conjecture, and the conjecture implies the solution of the base-change problem for a Hecke eigenform which is Steinberg at sufficiently many places.

## 6. General base-change

The solution of the conjecture basically suffices to solve the base-change problem for more general Hecke eigenform $f$. By introducing a ray class set $Cl^{(1)}_U = B^\times \backslash B^\times B^1(\mathbb{A}^{(\infty)})U/U$ for a suitable open compact subgroups $U \subset B^\times(\mathbb{A}^{(\infty)})$, we can

formulate the conjecture in this setting of the "ray" class set. Once this is done, pick any holomorphic Hecke eigenform $f$ (of weight 2 without complex multiplication) which generates an automorphic representation $\pi$ locally principal everywhere. We cannot shift $\pi$ to any definite quaternion algebra. However, by the level raising argument of Ribet-Wiles-Taylor, we can find a mod $p$ Hecke eigenform $g$ with $g \equiv f$ mod $p$ which is new at specific prime $\Sigma_B = \{q\}$ (if one wants, one can make $\Sigma_B$ with any given odd cardinality). Then $g$ can be lifted to $F/\mathbb{Q}$ under the generalized conjecture. Thus, by the Galois deformation theory (of Taylor-Wiles and Fujiwara over $F$) combined with level-lowering (of Jarvis), we can find the base-change Hilbert modular form $\widehat{f}$. Since weight 2 forms are $p$-adically dense in the space of $p$-adic modular forms, even if $f$ has weight $k \neq 2$, approximating $f$ by weight 2 forms, we can lift $f$ to a $p$-adic Hilbert modular form $\widehat{f}$ by the weight 2-result. Thus if $f$ has one ordinary prime $p$, $\widehat{f}$ is classical if $k \geq 2$ (by the classicity theorem of ordinary Hecke eigenform).

In summary, the quaternion algebras (which were studied in the hope of getting nonabelian class field theory) finally find some place in Langlands' functoriality conjecture.

Department of Mathematics, UCLA, Los Angeles CA 90095-1555, U.S.A.