CONSTRUCTION OF GALOIS COVERS OF CURVES WITH GROUPS OF SL_2-TYPE

CHIA-FU YU

ABSTRACT. We give a construction of étale Galois covers of algebraic curves over a field of positive characteristic with a prescribed system of finite groups of SL_2-type.

1. Introduction

In this note we give a construction of étale Galois covers of algebraic curves over a field of positive characteristic with a prescribed system of finite groups.

Consider a datum (p, ℓ, R) as follows:

- p and ℓ are different rational primes;
- R is the ring of integers of a finite product L of local fields over $\mathbb{Q}_\ell$.

The question studied here is

(Q) Can one find a smooth connected projective algebraic curve X over $\overline{\mathbb{F}}_p$ so that for any positive integer m there is a connected étale Galois cover $\pi_m : Y_m \to X$ with Galois group $G_m = \mathrm{SL}_2(R/\ell^m R)$? Furthermore, can one make the covers $\pi_m : Y_m \to X$ compatible with the projective system (G_m)?

We answer the question **(Q)** affirmatively, namely we prove the following

Theorem 1.1. *Given a datum $(p.\ell, R)$ as above, then there is a smooth connected projective curve X over $\overline{\mathbb{F}}_p$ and a compatible system of connected étale Galois covers $\pi_m : Y_m \to X$ with Galois group $\mathrm{SL}_2(R/\ell^m R)$.*

We find a totally real number field F of degree $d = \dim_{\mathbb{Q}_\ell} L$ so that (1) $O_F \otimes \mathbb{Z}_\ell \simeq R$ and (2) the prime p splits completely in F. Let $\mathbf{M}_F$ be the Hilbert modular variety associated to the totally real field F. The curve X is constructed in the reduction $\mathbf{M}_F \otimes \overline{\mathbb{F}}_p$ modulo p by vanishing $d-1$ Hasse invariants. The cover Y_m arises from the monodromy group for the ℓ^m-torsion subgroup of the universal family restricted on X.

The main tool is the ℓ-adic monodromy of Hecke invariant subvarieties in the moduli spaces of abelian varieties developed by Chai [1]. This technique confirms that the curves X and Y_m constructed as above are irreducible. The main theorem for Hilbert modular varieties is stated in Section 2.

The construction above provides a solution to the question **(Q)** when $d > 1$. In case of $d = 1$, one replaces R by $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ and proceeds the same construction. By replacing the covers Y_m by $Y_m/(1 \times \mathrm{SL}_2(\mathbb{Z}/\ell^m\mathbb{Z}))$, one yields a desired compatible

Date: April 10, 2007. The research is partially supported by NSC 96-2115-M-001-001.
2000 MSC: Primary: 12F12; Secondly: 14G35.
Key words and phrases: Galois covers, Hilbert modular varieties.

system of étale Galois covers. Alternatively, one replaces the Hilbert modular variety $\mathbf{M}_F$ by the Shimura curve $\mathbf{M}_B$ associated to an indefinite quaternion algebra B over $\mathbb{Q}$ in which both p and ℓ split, and takes $X := \mathbf{M}_B \otimes \overline{\mathbb{F}}_p$.

Theorem 1.1 is a special case of the following stronger result, which is communicated to the author by Akio Tamagawa.

Theorem 1.2. *Let G is a pro-finite group that is topologically generated by g elements and that is almost pro-prime-to-p, i.e. G admits a finite quotient G_0 whose kernel is pro-prime-to-p. Then there exists a proper smooth connected curve X_0 of genus g over $\overline{\mathbb{F}}_p$ so that $\pi_1(X_0)$ admits a surjective map onto G. .*

2. Hecke invariant subvarieties

In this section we describe a theorem of Chai on Hecke invariant subvarieties in a Hilbert modular variety.

Let F be a totally real number field of degree g and O_F be the ring of integers in F. Let V be a 2-dimensional vector space over F and $\psi : V \times V \to \mathbb{Q}$ be a $\mathbb{Q}$-bilinear non-degenerate alternating form such that $\psi(ax, y) = \psi(x, ay)$ for all $x, y \in V$ and $a \in F$. We choose and fix a self-dual O_F-lattice $V_{\mathbb{Z}} \subset V$. Let p be a fixed rational prime, not necessarily unramified in F. We choose a projective system of primitive prime-to-p-th roots of unity $\zeta = (\zeta_m)_{(m,p)=1} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$. We also fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$. For any prime-to-$p$ integer $m \geq 1$ and any connected $\mathbb{Z}_{(p)}[\zeta_m]$-scheme S, we obtain an isomorphism $\zeta_m : \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mu_m(S)$.

Let $n \geq 3$ be a prime-to-p positive integer and ℓ is a prime with $(\ell, pn) = 1$. Let $m \geq 0$ be a non-negative integer. Denote by $\mathbf{M}_{F,n\ell^m}$ the moduli space over $\mathbb{Z}_{(p)}[\zeta_{n\ell^m}]$ that parametrizes equivalence classes of objects $(A, \lambda, \iota, \eta)_S$ over a connected locally Noetherian $\mathbb{Z}_{(p)}[\zeta_{n\ell^m}]$-scheme S, where

- (A, λ) is a principally polarized abelian scheme over S of relative dimension g,
- $\iota : O_F \to \mathrm{End}_S(A)$ is a ring monomorphism such that $\lambda \circ \iota(a) = \iota(a)^t \circ \lambda$ for all $a \in O_F$, and
- $\eta : V_{\mathbb{Z}}/n\ell^m V_{\mathbb{Z}} \xrightarrow{\sim} A[n\ell^m](S)$ is an O_F-linear isomorphism such that

$$e_\lambda(\eta(x), \eta(y)) = \zeta_{n\ell^m}(\psi(x, y)), \quad \forall\, x, y \in V_{\mathbb{Z}}/n\ell^m V_{\mathbb{Z}}, \tag{2.1}$$

  where e_λ is the Weil pairing induced by the polarization λ.

The object (A, λ, ι) above is called a (principally) polarized abelian O_F-variety, and η is called an O_F-linear symplectic level-$n\ell^m$ structure with respect to the trivialization $\zeta_{n\ell^m}$.

Let G be the automorphism group scheme over $\mathbb{Z}$ associated to the pair $(V_{\mathbb{Z}}, \psi)$; for any commutative ring R, the group of R-valued points is

$$G(R) := \{g \in \mathrm{GL}_{O_F}(V_{\mathbb{Z}} \otimes_{\mathbb{Z}} R)\,;\, \psi(g(x), g(y)) = \psi(x, y),\ \forall\, x, y \in V_{\mathbb{Z}} \otimes_{\mathbb{Z}} R\,\}.$$

Let $\Gamma(n\ell^m)$ be the kernel of the reduction map $G(\mathbb{Z}) \to G(\mathbb{Z}/n\ell^m\mathbb{Z})$. It is well-known that one has the complex uniformization

$$\mathbf{M}_{F,n\ell^m}(\mathbb{C}) \simeq \Gamma(n\ell^m)\backslash G(\mathbb{R})/SO(2, \mathbb{R})^g.$$

In particular, the geometric generic fiber $\mathbf{M}_{F,n\ell^m} \otimes \overline{\mathbb{Q}}$ is connected. It follows from the arithmetic compactification constructed in Rapoport [7] that the geometric special fiber $\mathbf{M}_{F,n\ell^m} \otimes \overline{\mathbb{F}}_p$ is also connected. Write $M_{n\ell^m} := \mathbf{M}_{F,n\ell^m} \otimes \overline{\mathbb{F}}_p$ for the reduction modulo p of the moduli scheme $\mathbf{M}_{F,n\ell^m}$. We have a natural morphism $\pi_{m,m'} : M_{n\ell^{m'}} \to M_{n\ell^m}$, for $m < m'$, which is induced from the map $(A, \lambda, \iota, \eta) \mapsto (A, \lambda, \iota, \ell^{m'-m}\eta)$. Let $\widetilde{M}_n := (M_{n\ell^m})_{m\geq 0}$ be the tower of this projective system.

Let $(\mathcal{X}, \lambda, \iota, \eta) \to M_n$ be the universal family. The cover $M_{n\ell^m}$ represents the étale sheaf

$$\mathcal{P}_m := \underline{Isom}_{M_n}((V_{\mathbb{Z}}/\ell^m V_{\mathbb{Z}}, \psi), (\mathcal{X}[\ell^m], e_\lambda)\,; \zeta_{\ell^m}) \tag{2.2}$$

of O_F-linear symplectic level-ℓ^m structures with respect to ζ_{ℓ^m}. This is a $G(\mathbb{Z}/\ell^m\mathbb{Z})$-torsor. Let $\bar{x}$ be a geometric point in M_n. Choose an O_F-linear isomorphism $y : V \otimes \mathbb{Z}_\ell \simeq T_\ell(\mathcal{X}_{\bar{x}})$ which is compatible with the polarizations with respect to ζ. This amounts to choose a geometric point in $\widetilde{M}_n$ over the point $\bar{x}$. The action of the geometric fundamental group $\pi_1(M_n, \bar{x})$ on the system of fibers $(\mathcal{X}_{\bar{x}}[\ell^m])_m$ gives rise to the monodromy representation

$$\rho_{M_n,\ell} : \pi_1(M_n, \bar{x}) \to \mathrm{Aut}_{O_F}(T_\ell(\mathcal{X}_{\bar{x}}), e_\lambda) \tag{2.3}$$

and to the monodromy representation (using the same notation), through the choice of y,

$$\rho_{M_n,\ell} : \pi_1(M_n, \bar{x}) \to G(\mathbb{Z}_\ell). \tag{2.4}$$

The connectedness of $\widetilde{M}_n$ affirms that the monodromy map $\rho_{M_n,\ell}$ is surjective.

For any non-negative integer $m \geq 0$, let $\mathcal{H}_{\ell,m}$ be the moduli space over $\overline{\mathbb{F}}_p$ that parametrizes equivalence classes of objects $(\underline{A}_i = (A_i, \lambda_i, \iota_i, \eta_i), i = 1, 2, 3; \varphi_1, \varphi_2)$ as the diagram

$$\underline{A}_1 \xleftarrow{\ \varphi_1\ } \underline{A}_3 \xrightarrow{\ \varphi_2\ } \underline{A}_2,$$

where

- each $\underline{A}_i$ is a g-dimensional polarized abelian O_F-variety with a symplectic level-n structure, and both $\underline{A}_1$ and $\underline{A}_2$ are in M_n;
- φ_1 and φ_2 are O_F-linear isogenies of degree ℓ^m that preserve the polarizations and level structures.

Let $\mathcal{H}_\ell := \cup_{m\geq 0}\mathcal{H}_{\ell,m}$. An ℓ-adic Hecke correspondence is an irreducible component $\mathcal{H}$ of $\mathcal{H}_\ell$ together with natural projections pr_1 and pr_2. A subset Z of M_n is called *ℓ-adic Hecke invariant* if $\mathrm{pr}_2(\mathrm{pr}_1^{-1}(\mathrm{Z})) \subset \mathrm{Z}$ for any ℓ-adic Hecke correspondence $(\mathcal{H}, \mathrm{pr}_1, \mathrm{pr}_2)$. If Z is an ℓ-adic Hecke invariant, locally closed subvariety of M_n, then the Hecke correspondences induce correspondences on the set $\Pi_0(Z)$ of geometrically irreducible components. We say $\Pi_0(Z)$ is *ℓ-adic Hecke transitive* if the ℓ-adic Hecke correspondences operate transitively on $\Pi_0(Z)$, that is, for any two maximal points η_1, η_2 of Z there is an ℓ-Hecke correspondence $(\mathcal{H}, \mathrm{pr}_1, \mathrm{pr}_2)$ so that $\eta_2 \in \mathrm{pr}_2(\mathrm{pr}_1^{-1}(\eta_1))$.

Theorem 2.1 (Chai)**.** *Let Z be an ℓ-adic Hecke invariant, smooth locally closed subvariety of M_n. Let $\bar{\eta}$ be a geometric generic point of an irreducible component Z^0 of Z. Suppose that the abelian variety $A_{\bar{\eta}}$ corresponding to the point $\bar{\eta}$ is not supersingular, and that the set $\Pi_0(Z)$ is ℓ-adic Hecke transitive. Then the monodromy representation*

$$\rho_{Z^0,\ell} : \pi_1(Z^0, \bar{\eta}) \to G(\mathbb{Z}_\ell) \tag{2.5}$$

is surjective and Z is irreducible.

The proof of this theorem is given by Chai [1] for Siegel modular varieties, which uses the semi-simplicity of the geometric monodromy group of a pure $\mathbb{Q}_\ell$-sheaf on a variety over a finite field due to Grothendieck and Deligne ([2, Corollary 1.3.9 and Theorem 3.4.1]). Chai's proof also works for Hilbert modular varieties as stated in Theorem 2.1; see the expository account in [11]. Let $Z_m := M_{n\ell^m} \times_{M_n} Z$. Theorem 2.1 also implies that Z_m is irreducible provided the conditions for Z are satisfied.

3. The construction

Lemma 3.1 (Krasner's Lemma)**.** *Let k be a local field of characteristic zero and $f(X)$ be a monic separable polynomial of degree n. If $g(X)$ is a monic polynomial of degree n whose coefficients are sufficiently close to those of $f(X)$. Then $g(X)$ is separable and there is an isomorphism of k-algebras $k[X]/(g(X)) \simeq k[X]/(f(X))$.*

Proof. See a proof of this version of Krasner's lemma in [6, p. 317]. ∎

Lemma 3.2. *Let S be a finite set of places of a number field k. Let L_v, for each $v \in S$, be a product of local fields over k_v of same degree $[L_v : k_v] = n$, where k_v is the completion of k at v. Then there is a number field F over k of degree n such that $F \otimes_k k_v \simeq L_v$ for all $v \in S$.*

Proof. Write L_v as $k_v[X]/(P_v(X))$ for some monic separable polynomial $P_v(X)$ of degree n. By an effective version of Hilbert's irreducibility theorem [3, Theorem 1.3], there is an irreducible monic polynomial $P(X) \in k[X]$ of degree n whose coefficients are sufficiently close to those of $P_v(X)$ for each $v \in S$. Set $F := k[X]/(P(X))$. By Krasner's lemma (Lemma 3.1), one has $F \otimes_k k_v \simeq k_v[X]/(P(X)) \simeq k_v[X]/(P_v(X))$ for all $v \in S$. This completes the proof. ∎

Corollary 3.3. *Given a datum (p, ℓ, R) as before, there is a totally real number field F of degree $d = \dim_{\mathbb{Q}_\ell} L$ so that (1) $O_F \otimes \mathbb{Z}_\ell \simeq R$ and (2) the prime p splits completely in F.*

Proof. Take $S = \{\infty, p, \ell\}$ and

$$L_\infty = \mathbb{R}^d, \quad L_p = \mathbb{Q}_p^d, \quad L_\ell = L,$$

and apply Lemma 3.2. ∎

.

Assume that $d > 1$. Let F be a totally real number field as in Corollary 3.3. Write the set of ring homomorphisms from O_F to $\mathbb{F}_p$ as $\{\sigma_1, \dots, \sigma_d\}$. Define modular varieties M_n and $M_{n\ell^m}$ over $\overline{\mathbb{F}}_p$ as in Section 2 (with a choice of a system of roots of unity ζ). Let $a : (\mathcal{X}, \lambda, \iota, \eta) \to M_n$ be the universal family. Let $H^1_{\mathrm{DR}}(\mathcal{X}/M_n)$ be the algebraic de Rham cohomology; it has a decomposition

$$H^1_{\mathrm{DR}}(\mathcal{X}/M_n) = \oplus_{i=1}^d H^1_{\mathrm{DR}}(\mathcal{X}/M_n)^i \tag{3.1}$$

with respect to the O_F-action, where $H^1_{\mathrm{DR}}(\mathcal{X}/M_n)^i$ is the σ_i-isotypic component. Each component $H^1_{\mathrm{DR}}(\mathcal{X}/M_n)^i$ is a locally free $\mathcal{O}_{M_n}$-module of rank 2. The Hodge filtration

$$0 \to \omega_{\mathcal{X}/M_n} \to H^1_{\mathrm{DR}}(\mathcal{X}/M_n) \to R^1 a_* \mathcal{O}_{\mathcal{X}} \to 0 \tag{3.2}$$

also has the same decomposition

$$0 \to \omega^i_{\mathcal{X}/M_n} \to H^1_{\mathrm{DR}}(\mathcal{X}/M_n)^i \to R^1 a_* \mathcal{O}^i_{\mathcal{X}} \to 0, \tag{3.3}$$

for all $1 \le i \le d$. Let $F_{\mathcal{X}/M_n} : \mathcal{X} \to \mathcal{X}^{(p)}$ be the relative Frobenius morphism, where $\mathcal{X}^{(p)}$ is base change of $\mathcal{X}$ by the absolute Frobenius morphism $F_{M_n} : M_n \to M_n$. The morphism $F_{\mathcal{X}/M_n}$, by functoriality, induces an $\mathcal{O}_{M_n}$-linear map $F_i : R^1 a_* \mathcal{O}^i_{\mathcal{X}^{(p)}} \to R^1 a_* \mathcal{O}^i_{\mathcal{X}}$. By duality, one has $h_i := F_i^\vee : \omega^i_{\mathcal{X}/M_n} \to \omega^i_{\mathcal{X}^{(p)}/M_n}$. Since $\omega^i_{\mathcal{X}^{(p)}/M_n} \simeq (\omega^i_{\mathcal{X}/M_n})^{\otimes p}$, the homomorphism h_i is an element in $H^0(M_n, \mathcal{L}^i)$, where $\mathcal{L}^i := (\omega^i_{\mathcal{X}/M_n})^{\otimes(p-1)}$.

Let X be the closed subscheme of M_n defined by $h_i = 0$ for $2 \le i \le d$. Let $Y_m := M_{n\ell^m} \times_{M_n} X$. It is clear that X is stable under all ℓ-adic Hecke correspondences. We verify the conditions in Theorem 2.1:

Lemma 3.4.
(1) *The subscheme X is a smooth projective curve over $\overline{\mathbb{F}}_p$.*
(2) *Any maximal point of X is not supersingular.*
(3) *The set $\Pi_0(X)$ of irreducible components is ℓ-adic Hecke transitive.*

PROOF. Since points in X are not ordinary, it follows from the semi-stable reduction theorem that X is proper. By the Serre-Tate theorem, the deformations in M_n are the same as a product of deformations in an elliptic modular curve. It is well-known that the zero locus of the Hasse invariant is reduced and ordinary elliptic curves are dense in the mod p of an elliptic modular curve. From this the statements (1) and (2) follows. The statement (3) follows from [4, Cor. 4.2.4] (also see a proof in [11, Theorem 5.2]). ∎

By Theorem 2.1, the curves X and Y_m are irreducible. One also has $\mathrm{Aut}(Y_m/X) = G(\mathbb{Z}/\ell^m\mathbb{Z}) = \mathrm{SL}_2(R/\ell^m R)$. The construction is complete. This finishes the proof of Theorem 1.1.

The following question to which we do not know the answer. *What is the genus of X as above?*

Proof of Theorem 1.2. (This proof is standrad and is known to some experts.) First we know that for any algebraically closed field k with positive transcendental degree over $\mathbb{F}_p$ and any $g > 0$, there is a connected smooth proper curve X over k of genus g so that $\pi_1(X)$ admits a quotient which is free pro-finite of g generators. Choose such a curve X with $\mathrm{trdeg}_{\mathbb{F}_p} k = 1$ and we get a surjective map $\pi_1(X) \to G$. Let $X' \to X$ be the étale Galois cover corresponding to the natural surjection $\pi_1(X) \to G_0$. Specialize at a good point for a model $X' \to X$ of Galois covers over a curve over $\overline{\mathbb{F}}_p$ and get an étale Galois cover $X_0' \to X_0$ over $\overline{\mathbb{F}}_p$ (see [9, Proposition 2.5 and Corollary 3.5] for a detailed argument of specialization). We claim that $\pi_1(X_0)$ admits a surjective map onto G.

By the Galois theory and Grothendieck's specialization theorem, we have the exact sequences

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(X') \arrow[r] \arrow[d, "s'"] & \pi_1(X) \arrow[r] \arrow[d, "s"] & G_0 \arrow[r] \arrow[d, "="] & 1 \\
1 \arrow[r] & \pi_1(X_0') \arrow[r] & \pi_1(X_0) \arrow[r] & G_0 \arrow[r] & 1,
\end{tikzcd}$$

where s and s' are specilization maps, which are surjective. Let G' be the kernel of the map $\pi_0 : G \to G_0$. Since G' is prime-to-p pro-finite, the natural map $\pi(X') \to G'$ factors through its maximal prime-to-p quotient $\pi(X')^{(p)}$. We get surjective maps

$$\pi_1(X') \to \pi_1(X'_0) \to \pi_1(X'_0)^{(p)} \simeq \pi(X')^{(p)} \to G'.$$

We want to show that the map $f : \pi_1(X) \to G$ factors through $\pi_1(X_0)$, or equivalently $\ker s \subset \ker f$. Let $x \in \ker s$. Since its image in G_0 is 1, there is a unique element $x' \in \pi_1(X')$ whose image in $\pi_1(X)$ is x. Now $s'(x') = 1$, as its image in $\pi_1(X_0)$ is 1. This shows that $f(x) = 1$, and hence that $\ker s \subset \ker f$. This completes the proof. ∎

Remark 3.5. Consider quaternion algebras B over a totally real number field F so that B splits at exactly one of real places of F and B splits at all primes of F over p. Let $\mathbf{M}_B$ be the Shimura curve associated to B and take $X := \mathbf{M}_B \otimes \overline{\mathbb{F}}_p$ to be the reduction modulo p (see [5] for a nice summary of Ihara's work on Shimura curves). This exhibits a solution to the question **(Q)** for not just a prescribed system arising from SL_2 over $F \otimes \mathbb{Q}_\ell$ but also that from its inner twist.

Acknowledgment

This note is completed during the author's stay at Max-Planck-Institut für Mathematik in Bonn in 2007. He wishes to thank the Institut for kind hospitality and excellent working environment. He is grateful to Akio Tamagawa for helpful comments (Theorem 1.2 and Remark 3.5) which justify the content of this note.

References

[1] C.-L. Chai, Monodromy of Hecke-invariant subvarieties. Special issue in memory of A. Borel. *Pure Appl. Math. Q.* **1** (2005), 291–303.

[2] P. Deligne, La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.* **52** (1980), 137–252.

[3] T. Ekedahl, An effective version of Hilbert's irreducibility theorem. *Séminaire de Théorie des Nombres*, Paris 1988–1989, 241–249. Progr. Math., **91**, Birkhäuser Boston, 1990.

[4] E.Z. Goren and F. Oort, Stratifications of Hilbert modular varieties in positive characteristic. *J. Algebraic Geom.* **9** (2000), 111–154.

[5] Y. Ihara, Shimura curves over finite fields and their rational points. *Applications of curves over finite fields* (Seattle, WA, 1997), 15–23, *Contemp. Math.*, **245**, 1999.

[6] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory.* Pure and Applied Mathematics, **139**. Academic Press, Boston, MA, 1994.

[7] M. Rapoport, Compactifications de l'espaces de modules de Hilbert-Blumenthal. *Compositio Math.* **36** (1978), 255–335.

[8] M. Saïdi, Revêtements modérés et groupe fondamental de graphe de groupes. *Compositio Math.* **107** (1997), 319–338.

[9] Stevenson, Katherine F., Galois groups of unramified covers of projective curves in characteristic p. *J. Algebra* **182** (1996), 770–804.

[10] A. Tamagawa, Fundamental groups and geometry of curves in positive characteristic. *Arithmetic fundamental groups and noncommutative algebra* (Berkeley, CA, 1999), 297–333, Proc. Sympos. Pure Math., **70**, 2002.

[11] C.-F. Yu, Irreducibility of the Hilbert-Blumenthal moduli spaces with parahoric level structure. Preprint 2007.

Institute of Mathematics, Academia Sinica, 128 Academia Rd. Sec. 2, Nankang, Taipei, Taiwan and NCTS (Taipei office)

E-mail address: `chiafu@math.sinica.edu.tw`