

Curves with infinite K -rational geometric fundamental group

Gerhard Frey, Ernst Kani and Helmut Völklein

1 Rational Geometric Fundamental Groups

Let K be a finitely generated field with separable closure K_s and absolute Galois group G_K . By a curve C/K we always understand a smooth geometrically irreducible projective curve. Let $F(C)$ be its function field and let $\Pi(C)$ be the Galois group of the maximal unramified extension of $F(C)$. We have the exact sequence

$$1 \rightarrow \Pi_g(C) \rightarrow \Pi(C) \rightarrow G_K \rightarrow 1 \quad (\star)$$

where $\Pi_g(C)$ is the geometric (profinite) fundamental group of $C \times \text{Spec}(K_s)$ (i.e. $\Pi_g(C)$ is equal to the Galois group of the maximal unramified extension of $F(C) \otimes K_s$).

This sequence induces a homomorphism ρ_C from G_K to $\text{Out}(\Pi_g(C))$ which is the group of automorphisms modulo inner automorphisms of $\Pi_g(C)$. It is well known that ρ_C is an important tool for studying C . For instance, it determines C up to K -isomorphisms if the genus of C is at least 2 and K is a number field or even a \mathfrak{p} -adic field (see [Mo]).

So it is of interest to find quotients $\bar{\Pi}(C)$ of $\Pi(C)$ such that the induced map of G_K is not the identity but the induced representation $\bar{\rho}_C$ becomes trivial. We give a geometric interpretation of such quotients. For this we assume that the sequence (\star) is split and choose a section s which induces a homomorphism σ from G_K to $\text{Aut}(\Pi_g(C))$. Let U be a normal subgroup of $\Pi(C)$ contained in $\Pi_g(C)$. The representation ρ_C becomes trivial modulo U if and only if the map $\sigma \bmod U$ has its image inside of $\text{Inn}(\Pi_g(C)/U)$.

Let Z be the center of $\Pi_g(C)/U$ and $\bar{\Pi} = (\Pi_g(C)/U)/Z$. Our condition on U implies that there is exactly one group theoretical section \bar{s} from G_K to $(\bar{\Pi}(C)/U)/Z$ inducing the trivial action on $\bar{\Pi}$ and so $\bar{\Pi}$ occurs as Galois group of an unramified regular extension of $F(C)$ in a natural way.

Thus, to find center free infinite factors of Π_g on which ρ_C becomes trivial

is equivalent with finding infinite regular Galois coverings of C . Choosing as base point a geometric point of C we can say that “ Π is a factor of the geometric fundamental group of C over K ”.

Remark 1.1 If \bar{s} can be extended to a (group theoretical) section into $\Pi(C)/U$ then again it induces the trivial action on $\Pi_g(C)/U$ and hence this group occurs as Galois group of a regular unramified extension of $F(C)$. This is always true if K is a finite field or if Π/U is abelian.

But there is a difficulty: The sections \bar{s} corresponding to different quotients of Π_g may not be compatible (i.e. the composite of the corresponding coverings are not regular) and so we do not have a “maximal unramified regular covering” of C over K .

So we specialize, assume that C has a K -rational point P and choose a splitting s_P of (\star) corresponding to P by identifying G_K with the decomposition group of an extension of the place corresponding to P in $F(C)$ to its separable closure . Now the finite quotients of $\Pi_g(C)$ on which $s_P(G_K)$ operates trivially correspond to unramified Galois coverings C' of C on which the decomposition group of P operates trivially. Hence P has K -rational extensions to C' and the choice of s_P corresponds to the choice of such an extension P' . (If we make another choice, then the corresponding section is replaced by a conjugate in $\Pi(C)$.) We can regard C' as etale covering of C with respect to the base points P resp. P' .

Taking the limit we get the **K -rational geometric fundamental group of C with base point P** :

$$\Pi_g(C, P) := \Pi_g(C) / \langle (s_P(\sigma) - 1)\Pi_g(C) \rangle_{\sigma \in G_K}.$$

Remark 1.2 The construction of unramified coverings with base points is also of interest for coding theory:

Assume that $g(C) \geq 1$. Since

$$g(C') - 1 = [C' : C](g_C - 1)$$

and $\#\{P' \in C'(K)\}$ divisible by $[C' : C]$ we get (if $C'(K) \neq \emptyset$) that

$$\frac{|C'(K)|}{g(C') - 1} \geq \frac{1}{(g_C - 1)}$$

and this means that C' lies in a “good family” of coverings and so it is desirable to have infinite towers in this restricted sense over curves C (of small genus).

If K is a finite field such towers can be constructed by using class field theory of curves over any finite field (cf. Serre[Se1]) or over fields of square order by using Shimura curves (cf. [Ih]). By Ihara's method one can even obtain curves of genus 2 which are optimal. The curve given by $y^2 = x^6 - 1$ is such an example.

All these known examples are defined over finite fields and are of very special type.

In this paper we shall use either quartic coverings of the projective line or quadratic coverings of elliptic curves with enough ramification points (instead of quadratic coverings of the projective line as in the class field tower constructions) to find for every genus $g \geq 3$ curves with infinite geometric fundamental group defined over $\mathbb{Q}(i)$ or over $\mathbb{F}_q(i)$ (where i is a fourth root of unity) and we find even parametric families of such curves over every ground field containing i (cf. Theorem 5.22).¹

More precisely we get the

Result: *Let K be a field of characteristic $\neq 2, 3$ which contains a fourth root of unity. Take $a = \frac{2b^2}{1+b^4}$ with $b \in K^*$, $b^4 \neq 1$.*

Let C be a cyclic covering of degree 4 of the projective line given by an equation

$$s^4 = (1 + b^4)t(t^2 - 1)(t - a)g(t)$$

with a polynomial $g(t)$ such that $g(0)g(1)g(-1) \neq 0$ and $g(a) = 1$. Then C has an infinite K -rational geometric fundamental group with base point P_a corresponding to the place $t = a$.

We apply this and get the

Consequence: *Let b and a be as above.*

Let E_b be the elliptic curve defined over K by the equation

$$E_b : \quad y^2 = (1+b^4)x(x^2-1)(x-a).$$

Then for every natural number $g \geq 3$ there exist quadratic coverings C of E_b defined over K of genus $g_C = g$ with infinite K -rational geometric fundamental group with base point lying over P_a , the point of E_b corresponding to $x = a$.

¹We remark that we do not have any example of a curve defined over \mathbb{Q} with infinite \mathbb{Q} -rational geometric fundamental group.

Example: Let K , b and a be as above. The curve

$$C_a : y^4 = (1 + b^4)x(x^2 - 1)(x - a)$$

has an infinite K -rational geometric fundamental group with base point $(a, 0)$.

We thus have examples of curves of genus g with an infinite K -rational geometric fundamental group for every $g \geq 3$. No such example can exist for curves of genus $g = 1$, as will be explained in the next section. This leaves only the case $g = 2$. Here (cf. Example 4.13) we shall find very special curves with an infinite tower of regular unramified Galois coverings but we cannot decide there whether there are rational points in the tower.

There are other interesting aspects related to curves of genus 2 in the context of the questions discussed in this paper which will be investigated in more detail in the paper [FKV].

2 Abelian coverings

In this section we shall give a short review of the special case of abelian unramified coverings.

The largest abelian factor of $\Pi_g(C)$ which appears as the Galois group of a regular unramified extension of $F(C)$ is $\Pi_g(C)^{ab} / \langle (s_P(\sigma) - 1)\Pi_g(C)^{ab} \rangle_{\sigma \in G_K}$ and so it is independent of the choice of P or of the choice of the splitting. (But the coverings will depend on the choices.) Moreover, one sees that every abelian group which can be realized as Galois group of a regular unramified covering of C can be realized in such a way that a given point $P \in C(K)$ splits completely (cf. [V] or [Se]). So we do not have to distinguish between extensions with or without K -rational base points as long as we only want to describe the occurring Galois groups.

Let us begin by looking at elliptic curves. Here we have the following finiteness result:

Theorem 2.1 *Let K be a finitely generated field. Then there is a number $N = N(K)$ such that for all elliptic curves E defined over K we have $|E(K)_{tor}| \leq N$.*

Proof. We use induction with respect to the transcendence degree of K over its prime field K_0 .

If K is a finite field the claim is obvious. If K is a number field the theorem of Merel gives a bound N depending on $[K : \mathbb{Q}]$ only (cf. [Me]).

Let K be transcendental of degree $d_K \geq 1$ over K_0 . We fix a subfield $K_1 \subset K$ such that K_1 is finitely generated over K_0 and such that K is a function field of one variable over K_1 of genus g_K .

Let E/K be an elliptic curve with a K -rational point P of order n . Let K_2 be the smallest extension field of K_1 in K over which E is defined and over which P is rational.

If K_2 is equal to K_1 we can use the induction hypothesis, otherwise K_2 is a function field over K_1 with a K_1 -rational embedding of the function field of the modular curve $X_1(n)$ into K_2 and hence into K .

Thus, g_K bounds the genus of $X_1(n)$ which is of size $O(n^2)$ (cf. Miyake[Mi], if $(n, \text{char}(K)) = 1$ and Igusa[Ig], for $n = \ell^r$, $\ell = \text{char}(K)$), and so n is bounded.

Corollary 2.2 *There is a universal bound $n = n(K)$ such that for all regular unramified Galois covers ϕ of elliptic curves E over K we have $\deg(\phi) \leq n$.*

Proof. If ϕ is an unramified Galois covering of E , then the covering curve E' is an elliptic curve too, ϕ is an isogeny and the Galois group G_K acts on the kernel of ϕ trivially, i.e. $\text{Ker}(\phi) \leq E'(K)$. Using the universal bound for torsion points obtained in the theorem the corollary follows.

Next we consider the case that the genus of C is larger than 1, and study as before the existence of regular unramified abelian Galois coverings of C .

Proposition 2.3 *If $\phi : C_1 \rightarrow C$ is a regular abelian unramified covering, then $\deg \phi$ is bounded by a number depending on K and on C .*

Proof. By Serre [Se] we know that there is an abelian variety A/K such that ϕ induces an isogeny

$$\phi_* : A \rightarrow J_C$$

with $\text{Ker}(\phi_*) \subset A(K)$ and $|\text{Ker}(\phi_*)| = \deg(\phi)$. If K is finite we have $|A(K)| = |J_C(K)|$, and so we are done. If K is a number field or a field of transcendence degree larger than 1 over its prime field we can use reduction theory to get the result.

Remark: Since at present we do not have an analogue of Merel's theorem for abelian varieties, we can only find a bound depending on the genus and on the conductor of C , and not only on K , even if K is a number field.

3 Coverings of \mathbb{P}^1 with given ramification type

3.1 The Construction Principle

In the last section we had seen that for a given curve C over a finitely generated field K , the degree of the abelian unramified regular extensions of C/K is bounded.

The situation changes if we look for non-abelian coverings. Indeed, in the next section we shall give examples of families of curves of arbitrary genus $g \geq 3$ defined over a finitely generated field K which have infinite towers of unramified regular Galois coverings. However, it should be remarked that the dimension of these families is small compared with the dimension of the moduli space of curves of genus g and so it can be conjectured that for “general curves”, the degree of a regular unramified Galois covering is bounded by a number $N(g, K)$.

The construction of these curves is based on the following principle. We begin with the projective line \mathbb{P}^1 and choose a finite G_K -invariant set S_0 of points of \mathbb{P}^1 . Then we look for Galois coverings C' of \mathbb{P}^1 with a *simple* Galois group G (in our examples G is a projective linear group). We require that this covering is unramified outside of S_0 and that the ramification in points $P_i \in S_0$ has an order e_{P_i} which is small and prime to $\text{char}(K)$. We take a Galois covering C_0 of \mathbb{P}^1 disjoint to C' which ramifies in all P_i with an order which is a multiple of e_{P_i} . By Abhyankar’s Lemma it follows that $C' \times_{\mathbb{P}^1} C_0 / C_0$ is unramified with Galois group G and, because of the simplicity of G , regular.

To find C' we follow [FV] and use Hurwitz spaces which are moduli spaces for the ramification cycle configuration inside of G ; this boils down to proving the existence of K -rational points on these spaces. This Diophantine problem leads to interesting relations between arithmetic geometry and group theory. Sometimes group theory or, to be more precise, the theory of rigidity implies the existence of rational points on the corresponding Hurwitz spaces. This is the case in our examples which are related to Thompson tuples, and so in this case the existence of such coverings is obtained by pure group theory (and Riemann’s existence theorem).

However, this method fails to produce K -rational points on these coverings and so arithmetic-geometric methods have to be invoked in order to prove the existence of such points (which is necessary for our considerations of

K -rational fundamental groups).

In the case of the Thompson tuples, such a method is readily available, for behind their very construction (cf. [V3]) lies a deep arithmetic reason, viz. *the existence of a family of abelian varieties with good reduction.*

3.2 Rigidity

For the convenience of the reader we shall now give a very short overview over rigid systems of conjugacy classes. We shall assume that $\text{char}(K) = 0$, but actually it is enough to avoid fields with characteristics dividing the order of the occurring Galois groups and we shall use this fact in our examples.

We want to describe the regular Galois coverings of the projective line. For this, we recall the situation over the complex numbers over which we can use as crucial tool the Riemann existence theorem.

We have the following invariants for a finite Galois extension $L/\mathbb{C}(x)$: its Galois group G , the finite set $\underline{P} = \{P_1, \dots, P_r\}$ of branch points (which lie in $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$) and for each branch point P_i the associated conjugacy class C_i of G consisting of the distinguished inertia group generators over P_i . Define the **ramification type** of $L/\mathbb{C}(x)$ to be the class of the triple $(G, \underline{P}, \mathbf{C})$, where $\mathbf{C} = (C_1, \dots, C_r)$. We say that two such triples are in the same class if the sets \underline{P} are the same and if there is an isomorphism between the groups that identifies the conjugacy classes associated with the same point of \underline{P} .

The extension $L/\mathbb{C}(x)$ is defined over a subfield K of \mathbb{C} if there is a Galois extension $L_K/K(x)$, regular over K , which becomes equivalent to L when tensored with \mathbb{C} .

\mathbf{C} is **weakly rigid** if any two generating systems $\sigma_1, \dots, \sigma_r$ of G with $\sigma_i \in C_i$ and $\sigma_1 \cdots \sigma_r = 1$ are conjugate under an automorphism of G and if there is one such generating system. By Riemann's existence theorem, \mathbf{C} is weakly rigid if and only if there is exactly one Galois extension of $\mathbb{C}(x)$ of type $(G, \underline{P}, \mathbf{C})$ (up to equivalence), see [V], Th. 2.17. This uniqueness can be exploited to define the covering of \mathbb{P}^1 over a smaller field. To do this, we sharpen the group theoretical conditions for the ramification type as follows.

\mathbf{C} is **quasi-rigid** if it is weakly rigid and every automorphism of G fixing each C_i is inner.

Now suppose \mathbf{C} is quasi-rigid and that $L/\mathbb{C}(x)$ is a corresponding extension. Let L' be the fixed field of the center $Z(G)$ of G . Then the extension $L'/\mathbb{C}(x)$ is defined over the field generated over \mathbb{Q} by all branch points and by all roots of unity of order $\text{ord}(\sigma)$, $\sigma \in C_1 \cup \dots \cup C_r$. The exact minimal field of definition of L' may be even smaller and can be determined using the branch cycle argument (see [V], 3.2 and 3.3.2). This construction principle for Galois extensions of rational function fields (“rigidity criterion”) has successfully been used to realize given groups as Galois groups.

4 Construction of infinite towers of unramified curve covers

4.1 Thompson tuples and Belyi triples

Let q be a power of the prime p , and $n \geq 3$. We denote by \mathbb{F}_q^* the multiplicative group of the field \mathbb{F}_q with q elements. For any $\sigma \in \text{GL}_n(q)$, let c_1, \dots, c_n be the eigenvalues of σ (counted with multiplicities) and $\chi_\sigma(T) = \prod_i (T - c_i)$ its characteristic polynomial (normalized to be monic). We call σ a **perspectivity** if it has an eigenspace of dimension $n - 1$.

Definition 4.1 Let $r = n + 1$ (respectively, $r = 3$). A *Thompson tuple* (respectively, a *Belyi triple*) in $\text{GL}_n(q)$ is an r -tuple $(\sigma_1, \dots, \sigma_r)$ such that $\sigma_1, \dots, \sigma_r$ generate an irreducible subgroup of $\text{GL}_n(q)$, their product satisfies $\sigma_1 \cdots \sigma_r = 1$ and σ_i is a perspectivity for all $i = 1, \dots, r$ (respectively, for $i = 3$).

In [V1] one finds

Theorem 4.2 *Suppose that $(\sigma_1, \dots, \sigma_r)$ and $(\sigma'_1, \dots, \sigma'_r)$ are Thompson tuples (respectively, Belyi triples) in $\text{GL}_n(q)$ with $\chi_{\sigma_i} = \chi_{\sigma'_i}$ for all i . Then there is an element $g \in \text{GL}_n(q)$ with $\sigma'_i = g^{-1}\sigma_i g$ for all i . Thus $\sigma_1, \dots, \sigma_r$ are weakly rigid generators of $G = \langle \sigma_1, \dots, \sigma_r \rangle$, and they are quasi-rigid generators if the normalizer of G in $\text{GL}_n(q)$ equals $\mathbb{F}_q^* G$.*

We can apply the theory of rigid ramification types presented in the last section to obtain (cf. [V], Theorems 2.17, 3.26 and 7.9):

Corollary 4.3 *Let $(\sigma_1, \dots, \sigma_r)$ be a Thompson tuple or a Belyi triple in $\mathrm{GL}_n(q)$. Let C_i be the conjugacy class of σ_i in $G = \langle \sigma_1, \dots, \sigma_r \rangle$, and let P_1, \dots, P_r be distinct points of $\mathbb{P}^1(\mathbb{C})$. Put $\underline{P} = \{P_1, \dots, P_r\}$, $C_{P_i} = C_i$, and $\mathbf{C} = (C_P)_{P \in \underline{P}}$. Then we have:*

- (a) *There is a unique Galois extension $L'/\mathbb{C}(x)$ of ramification type $[G, \underline{P}, \mathbf{C}]$.*
- (b) *Suppose that the normalizer of G equals \mathbb{F}_q^*G . If $L = \mathrm{Fix}(Z(G))$ denotes the fixed field of the center $Z(G)$ of G , then the extension $L/\mathbb{C}(x)$ is defined over any subfield $K \subset \mathbb{C}$ which contains all the (finite) $P_i \in \underline{P}$ and all roots of unity of order $\mathrm{ord}(\sigma_i)$. In particular, there is a regular Galois extension L_0 of $K(x)$ with Galois group $\bar{G} = G/Z(G)$ with ramification type $[\bar{G}, \underline{P}, \bar{\mathbf{C}}]$, where \bar{C}_P is the image of C_P in \bar{G} .*

Corollary 4.4 *Suppose in addition that M is a regular extension of $K(x)$ which is linearly disjoint to the above extension L_0 over K , and which has the property that for each $i = 1, \dots, r$ and each place m of M lying above the place corresponding to P_i of $\mathbb{C}(x)$, the ramification index of m is a multiple of $\mathrm{ord}(\sigma_i)$. Then the composite $L_0 \cdot M$ is an unramified Galois extension of the function field M and its Galois group is isomorphic to \bar{G} .*

We therefore see that to find such field extensions L , it is enough to find Thompson tuples or Belyi triples. These will now be investigated in more detail. The first result in this direction (taken from [V1]) shows that they can be characterized by their characteristic polynomials:

Theorem 4.5 *Let $f_1, \dots, f_r \in \mathbb{F}_q[T]$ be monic polynomials of degree n with $\prod_i f_i(0) = (-1)^{rn}$.*

(a) *There exists a Belyi triple $(\sigma_1, \sigma_2, \sigma_3)$ in $\mathrm{GL}_n(q)$ with $\chi_{\sigma_i} = f_i$ if and only if $f_3(T) = (T - c)^{n-1}(T - d)$ for elements $c, d \in \mathbb{F}_q^*$ satisfying $abc \neq 1$ for all $a, b \in \bar{\mathbb{F}}_q$ with $f_1(a) = f_2(b) = 0$.*

(b) *There exists a Thompson tuple $(\sigma_1, \dots, \sigma_r)$ in $\mathrm{GL}_n(q)$ with $\chi_{\sigma_i} = f_i$ if and only if $f_i(T) = (T - a_i)^{n-1}(T - b_i)$ for elements $a_1, \dots, a_r, b_1, \dots, b_r \in \mathbb{F}_q^*$ satisfying $a_1 \cdots a_r \neq 1$ and $b_j \prod_{i \neq j} a_i \neq 1$ for all $j = 1, \dots, r$.*

From Theorem 4.2 we see that the tuples $(\sigma_1, \dots, \sigma_r)$ are classified by their characteristic polynomials χ_{σ_i} , and so the group $G = \langle \sigma_1, \dots, \sigma_r \rangle$ depends only on the χ_{σ_i} (up to conjugation). In the case of Thompson tuples there is a complete classification of the related groups (cf. [V1] and [V4]). In the

following Theorem 4.6 we shall state only that part of this classification which will be relevant for us below.

In order to state the result, we require the following terminology. A Thompson tuple $(\sigma_1, \dots, \sigma_{n+1})$ is called **normalized** if $\chi_{\sigma_i} = (T - 1)^{n-1}(T - b_i)$ for $i = 1, \dots, n$.

Theorem 4.6 *Let n be odd and ≥ 3 . Suppose $(\sigma_1, \dots, \sigma_{n+1})$ is a normalized Thompson tuple in $\mathrm{GL}_n(q)$ generating the group G with $\chi_{\sigma_i}(T) = (T - 1)^{n-1}(T - b_i)$ for certain $b_i \in \mathbb{F}_q$ for $i = 1, \dots, n$. If $n = 3$ assume that some b_i has multiplicative order > 3 . Suppose that $\mathbb{F}_q = \mathbb{F}_p(a_{n+1}, b_1, \dots, b_{n+1})$, and assume that if $q = q_0^2$ is a square, then not all the a_i, b_i have norm 1 over \mathbb{F}_{q_0} . Then*

$$\mathrm{SL}_n(q) \leq G \leq \mathrm{GL}_n(q).$$

4.2 Curves with infinite towers of unramified regular Galois extensions

We now apply the above results to construct unramified Galois G -covers of curves with group $G = \mathrm{PSL}_n(p)$ for suitable values of n and p . In order to be able to specify precisely which values are suitable here, we first introduce the following notation.

Notation. Let $n \geq 3$ be an odd natural number, and let $d_1, \dots, d_{n+1} > 3$ be integers. Then we denote by $\mathbb{P}(n, d_1, \dots, d_{n+1})$ the set of all prime numbers p satisfying the following conditions:

- (i) $(n, p - 1) = 1$;
- (ii) there are elements $b_1, \dots, b_{n+1} \in \mathbb{F}_p^*$ with $b_1 \cdots b_{n+1} = 1$ such that each b_i has multiplicative order d_i in \mathbb{F}_p^* .

A trivial but useful fact is

Lemma 4.7 *If d_1, \dots, d_n are prime to n and $d_{n+1} = \mathrm{lcm}(d_1, \dots, d_n)$, then every prime p with $p \not\equiv 1 \pmod{l}$ for all primes $l \mid n$ and $p \equiv 1 \pmod{d_{n+1}}$ is in $\mathbb{P}(n, d_1, \dots, d_{n+1})$. Moreover, there is a constant c (depending only on n and d_1, \dots, d_{n+1}) such that for all primes $l \geq c$ there are infinitely many $p \in \mathbb{P}(n, d_1, \dots, d_{n+1})$ such that l does not divide the order of $\mathrm{GL}_n(p)$.*

From now on, suppose that the integers d_1, \dots, d_{n+1} satisfy the conditions of this lemma, and that K is a field of characteristic 0 containing a primitive d^{th} root of unity, where $d = \text{lcm}(d_1, \dots, d_{n+1}, 2) = \text{lcm}(d_{n+1}, 2)$. Moreover, let $p \in \mathbb{P}(n, d_1, \dots, d_{n+1})$ and choose $b_i \in \mathbb{F}_p^*$ such that condition (ii) holds. Then by Theorem 4.5 there is a normalized Thompson tuple $(\sigma_1, \dots, \sigma_{n+1})$ in $\text{GL}_n(p)$ corresponding to these b_i with $a_{n+1} = -1$. The order of σ_i equals d_i for $i \leq n$ and it equals $\text{lcm}(d_{n+1}, 2) = d$ for $i = n + 1$.

By Theorem 4.6 the group $G = \langle \sigma_1, \dots, \sigma_{n+1} \rangle$ contains $\text{SL}_n(p)$. Thus the group $\tilde{G} = G/Z(G)$ is isomorphic to the simple group $\text{PSL}_n(p)$ (because we assumed $(n, p - 1) = 1$).

It remains to choose the ramification points.

Since the automorphism group of \mathbb{P}^1 acts sharply triple transitive we can assume without loss of generality that $P_{n-1} = 0$, $P_n = 1$ and $P_{n+1} = \infty$. The other ramification points are then denoted by $t_1, \dots, t_{n-2} \in K$.

Using Corollary 4.3 we see that for every $p \in \mathbb{P}(n, d_1, \dots, d_{n+1})$, we get a regular Galois extension F'_p of $K(X)$ with Galois group $\text{PSL}_n(p)$ ramified only in $0, 1, \infty, t_1, \dots, t_{n-2}$ with ramification indices dividing d .

Since for different primes p the Galois groups of the F'_p 's are non-isomorphic simple groups, the composite field

$$F'_{\mathbb{P}(n, d_1, \dots, d_{n+1})} = \prod_{p \in \mathbb{P}(n, d_1, \dots, d_{n+1})} F'_p$$

has the same regularity and ramification properties.

Next, let M_d be any regular extension field of $K(X)$ such that every extension of the places $0, 1, \infty, t_1, \dots, t_{n-2}$ is ramified with an order divisible by d . (For instance, take M_d as a cyclic cover of $K(x)$ of degree d totally ramified at $0, 1, \infty, t_1, \dots, t_{n-2}$. In this case the genus of M_d is equal to $(n-1)(d-1)/2$.) Using Corollary 4.4, we get that $F'_{\mathbb{P}(n, d_1, \dots, d_{n+1})} \cdot M_d$ is a regular unramified extension of M_d with Galois group equal to

$$\prod_{p \in \mathbb{P}(n, d_1, \dots, d_{n+1})} \text{PSL}_n(p).$$

Thus, if we take $K = \mathbb{Q}(\zeta_d, t_1, \dots, t_{n-2})$, where the t_1, \dots, t_{n-2} are algebraically independent over \mathbb{Q} , then we obtain:

Theorem 4.8 *Let $n \geq 3$ be an odd number and let $d_1, \dots, d_n > 3$ be integers prime to n , $d_{n+1} := \text{lcm}(d_1, \dots, d_n)$ and $d = \text{lcm}(2, d_{n+1})$. Then*

$\mathbb{P}(n, d_1, \dots, d_{n+1})$ is an infinite set and there is an $(n - 2)$ -dimensional rational family \mathcal{C} of curves of genus $(n - 1)(d - 1)/2$ defined over $\mathbb{Q}(\zeta_d)$ such that for all $p \in \mathbb{P}(n, d_1, \dots, d_{n+1})$ there is an unramified regular Galois cover \mathcal{C}_p with Galois group $\mathrm{PSL}_n(p)$ and the composite of these covers is an infinite unramified regular Galois tower.

On the other hand, if we choose the t_i 's to be algebraic over \mathbb{Q} , we obtain:

Theorem 4.9 *Let K be a number field. Let n be odd and at least equal to 3 and let d be as in the previous theorem. Then there are infinitely many curves of genus $(d - 1)(n - 1)/2$ defined over K with infinite towers of unramified regular Galois covers defined over $K(\zeta_d)$.*

As was mentioned above, the Hurwitz space theory and the theory of Thompson tuples works also over fields of characteristic l as long as l is prime to the order of the Galois group. Using the second part of Lemma 4.7 we see that Theorem 4.8 holds if we replace \mathbb{Q} by \mathbb{F}_l for almost all primes l . Hence we have

Corollary 4.10 *Let n and d be as above, and let l be a sufficiently large prime such that there are infinitely many primes p with $p^i - 1$ prime to l for $i = 1, \dots, n$. Then there exist curves of genus $(d - 1)(n - 1)/2$ defined over $K = \mathbb{F}_l(\zeta_d)$ which have an infinite tower of unramified regular Galois covers defined over K .*

Now we discuss the simplest possibility and get the following example which will play an important role in Section 5.3.

Example 4.11 Let $n = 3$ and $d_1 = \dots = d_4 = d = 4$, and let K be a field of characteristic ≥ 5 which contains a fourth root of unity $\zeta_4 = i$. Furthermore, let $t \in K$ be such that $t \neq 0, 1$.

Then for every $p \equiv 5 \pmod{12}$ we get an extension of \mathbb{P}^1 defined over K whose Galois group is equal to $\mathrm{PSL}_3(p)$ and which is ramified of order 4 in $\{0, 1, \infty, t\}$.

Fix an integer $g_0 \geq 1$. If $g_0 = 1$, let \mathcal{C}_0 be an elliptic curve which covers \mathbb{P}^1 with ramification points $\{0, 1, \infty, t\}$, and if $g_0 > 1$, let \mathcal{C}_0 be a hyperelliptic curve of genus g_0 whose set of Weierstrass points contains $\{0, 1, \infty, t\}$. Let \mathcal{C} be a quadratic extension of \mathcal{C}_0 ramified in the extensions of $\{0, 1, \infty, t\}$.

Then \mathcal{C} has genus $g := g_0 + \delta/2$, where δ is the number of ramified primes in the cover $\mathcal{C}/\mathcal{C}_0$.

For example, if we choose \mathcal{C} as a cyclic cover of degree 4 over \mathbb{P}^1 which is ramified in the Weierstrass points of \mathcal{C}_0 with ramification order 4 and in s additional points of \mathbb{P}^1 with ramification order 2, then $g = 3g_0 + s$.

Hence we get

Corollary 4.12 *Let K be a field of characteristic $\neq 2, 3$ which contains a primitive fourth root of unity $i = \zeta_4$. Let $t \in K$, $t \neq 0, 1$ and let \mathcal{C}_0 be either an elliptic curve ($g_0 = 1$) or a hyperelliptic curve of genus g_0 defined over K with at least four K -rational points of order 2 respectively, Weierstrass points equal to $\{0, 1, \infty, t\}$.*

Then for all non-negative integers s there are quadratic covers of \mathcal{C}_0 defined over K of genus $3g_0 + s$ with an infinite tower of regular unramified Galois covers over K .

If we want to obtain examples as above for curves of genus 2, then we have to use Belyi triples, but in that case we find only isolated examples. Here is one of them:

Example 4.13 Let Φ_m be the cyclotomic polynomial of order m , and let $(\sigma_1, \sigma_2, \sigma_3)$ be a Belyi triple in $\mathrm{GL}_3(p)$ with characteristic polynomials $\chi_{\sigma_1} = (T+1)\Phi_6$, $\chi_{\sigma_2} = (T-1)\Phi_3$, and $\chi_{\sigma_3} = (T-1)^2(T+1)$. Then the images $\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3$ generate the simple group $\mathrm{PSL}_3(p)$ for $p \equiv -1 \pmod{3}$, and there is a corresponding extension $L_p/\mathbb{Q}(x)$ branched at $0, \infty, 1$. Take $x = t^6$ and let $M/\mathbb{Q}(t)$ be the genus 2 function field extension branched where t is a sixth root of 1, i.e. M corresponds to the curve with equation

$$y^2 = t^6 - 1.$$

Then $L_p \cdot M/M$ is unramified with group $\mathrm{PSL}_3(p)$ and defined over \mathbb{Q} . It follows that the curve $y^2 = t^6 - 1$ has an infinite tower of regular unramified Galois extensions over \mathbb{Q} and over \mathbb{F}_l for all primes $l \geq 5$.

We observe that although we obtain in this way the example of Ihara mentioned in the first section, we have actually realized different Galois groups by this method. At present, however, we cannot answer the question concerning the existence of rational points in the associated infinite tower.

Further examples (for $\mathrm{PSL}_3(p)$ again) are obtained by taking χ_{σ_3} as above, and $\chi_{\sigma_1} = (T-1)\Phi_3$, $\chi_{\sigma_2} = (T+1)\Phi_4$, or alternatively, $\chi_{\sigma_1} = (T+1)\Phi_3$, $\chi_{\sigma_2} = (T-1)\Phi_4$. We thank G. Malle for pointing out these examples.

4.3 Geometric Interpretation of Thompson tuples

In the last section, the examples of almost unramified covers of \mathbb{P}^1 were constructed by using group theory. This construction did not provide any method for determining the existence of rational points in the covers, nor did it explain the arithmetical “reason” behind the existence of such examples. However, both these aspects are greatly elucidated by using the results of [V3] to relate the Thompson tuples to torsion points of Jacobians of curves which are cyclic covers of the projective line.

The basic idea here is the following. If $\phi : C \rightarrow \mathbb{P}_K^1$ is a cyclic covering with group $Z = \text{Aut}(\phi)$ defined over a field K and $\lambda : Z \rightarrow \mathbb{F}_q^*$ is a faithful character, then the Galois group G_K acts \mathbb{F}_q -linearly on the λ -component $J_C[p]_\lambda$ of the group $J_C[p]$ of p -torsion points of the Jacobian variety J_C of C . Now it turns out that if the ramification points $t_1, \dots, t_{n+2} \in K$ of ϕ are in “sufficiently general position“, then the image of the Galois group G_K in $\text{GL}_n(J_C[p]_\lambda)$ is (essentially) generated by a Thompson tuple, and conversely, every Thompson tuple arises in this fashion.

In order to make this connection between cyclic coverings and Thompson tuples more precise, it is useful to introduce the following alternate description of Thompson tuples, using the *Braid group*.

For this, let $s = n + 2$, and let Q_1, \dots, Q_{s-1} be the standard generators of the *Artin braid group* \mathcal{B}_s on s strings. Mapping Q_i to the transposition $(i, i + 1)$ yields a homomorphism $\kappa : \mathcal{B}_s \rightarrow S_s$. The kernel of κ is called the *pure braid group*, and is denoted by $\mathcal{B}^{(s)}$. It is generated by the elements

$$Q_{ij} = Q_{j-1} \cdots Q_{i+1} Q_i^2 Q_{i+1}^{-1} \cdots Q_{j-1}^{-1}, \quad 1 \leq i < j \leq s.$$

The braid group \mathcal{B}_s acts on tuples (g_1, \dots, g_s) of elements of any group by the rule that Q_i maps (g_1, \dots, g_s) to

$$(g_1, \dots, g_{i-1}, g_{i+1}, g_{i+1}^{-1} g_i g_{i+1}, \dots, g_s)$$

Lemma 4.14 (a) *If $\underline{\zeta} = (\zeta_1, \dots, \zeta_{n+2})$ is an $(n+2)$ -tuple of elements $\zeta_i \in \mathbb{F}_q^*$ satisfying the conditions*

$$\prod_{j=1}^{n+2} \zeta_j = 1, \quad \zeta_i \neq 1, \text{ for all } i, \tag{1}$$

then there is a unique (up to conjugation) normalized Thompson tuple $\underline{\sigma} = \underline{\sigma}_\zeta = (\sigma_1, \dots, \sigma_{n+1})$ in $\text{GL}_n(q)$ such that

$$\begin{aligned}\chi_{\sigma_i}(T) &= (T-1)^{n-1}(T - \zeta_i^{-1}\zeta_{n+2}^{-1}), \quad 1 \leq i \leq n, \\ \chi_{\sigma_{n+1}}(T) &= (T - \zeta_{n+2})^{n-1}(T - \zeta_{n+1}^{-1}).\end{aligned}$$

Moreover, every normalized Thompson tuple $\underline{\sigma}$ in $\text{GL}_n(q)$ is of the form $\underline{\sigma} = \underline{\sigma}_\zeta$, for a unique $(n+2)$ -tuple $\underline{\zeta}$ satisfying (1).

(b) In the situation of (a) there is a homomorphism

$$\Phi_\zeta : \mathcal{B}^{(s)} \rightarrow \text{GL}_n(q)$$

such that for $i = 1, \dots, s-1$ the elements $\tau_i := \Phi_\zeta(Q_{is})$ are perspectivities with $\chi_{\tau_i} = (T-1)^{n-1}(T - \zeta_i^{-1}\zeta_s^{-1})$ and $\tau_1 \cdots \tau_{s-1} = \zeta_s^{-1} \cdot \text{id}$. Thus $(\tau_1, \dots, \tau_{s-2}, \zeta_s \tau_{s-1})$ is a Thompson tuple associated with ζ .

Proof. (a) Put $s = n+2$. Recall from Theorem 4.5 that a normalized Thompson tuple $(\sigma_1, \dots, \sigma_{n+1})$ is characterized by the characteristic polynomials of the elements σ_i and so by the s -tuples $(b_1, \dots, b_{n+1}, a) \in (\mathbb{F}_q)^{n+2}$ which satisfy the additional properties that $\prod_{i=1}^{n+1} b_i \cdot a^{n-1} = 1$ and that $a \neq 1$, $b_{n+1} \neq 1$ and $a \cdot b_i \neq 1$ for $1 \leq i \leq n$.

We associate to $(\sigma_1, \dots, \sigma_{n+1})$ the s -tuple $(\zeta_1, \dots, \zeta_{n+1}, \zeta_s)$ with $\zeta_i = (ab_i)^{-1}$ for $1 \leq i \leq n$, $\zeta_{n+1} = b_{n+1}^{-1}$ and $\zeta_s = a$. This tuple has the property that all ζ_i are different from 1 and that $\prod_{i=1}^s \zeta_i = 1$.

Conversely, if $\zeta_1, \dots, \zeta_{n+2} \in \mathbb{F}_q^*$ satisfying condition (1) are given, then $a := \zeta_{n+2}$, $b_{n+1} := \zeta_{n+1}$ and $b_i := \zeta_i^{-1}\zeta_{n+2}^{-1}$, for $1 \leq i \leq n$ satisfy the above conditions and hence give rise to a Thompson tuple $\underline{\sigma}_\zeta = (\sigma_1, \dots, \sigma_{n+1})$ with the indicated characteristic polynomials.

(b) For the definition of Φ_ζ see [V4] and [MSV]. (It is essentially the *Gassner representation* of $\mathcal{B}^{(s)}$ associated with ζ). The first assertion follows from [V4], Lemma 3 and relation (5). The relation $\tau_1 \cdots \tau_{s-1} = \zeta_s^{-1} \cdot \text{id}$ follows from the definition of Φ_ζ and the fact that the element

$$Q_{1s} \cdots Q_{s-1,s} = Q_{s-1} \cdots Q_2 Q_1^2 Q_2 \cdots Q_{s-1}$$

acts by sending (g_1, \dots, g_s) to $(g_1, \dots, g_s)^{g_s}$. The τ_i generate an irreducible group by [V1], Lemma 3.3.

We thus see that ζ -tuples give rise to Thompson tuples and conversely. On the other hand we can also attach to such tuples an (essentially unique) cyclic covering $\phi : C \rightarrow \mathbb{P}^1$ which is ramified at $s = n + 2$ prescribed points $t_1, \dots, t_s \in K$ as follows.

Lemma 4.15 *Suppose $\zeta_1, \dots, \zeta_s \in \mathbb{F}_q^*$ satisfy $\zeta_1 \cdot \dots \cdot \zeta_s = 1$ and $d_i := \text{ord}(\zeta_i) \neq 1$, $1 \leq i \leq s$. Let K be a field containing a primitive d -th root of unity where $d = \text{lcm}(d_1, \dots, d_s)$ and suppose that $t_1, \dots, t_s \in K$ are s distinct points. Then there is a cyclic covering $\phi = \phi_{t, \zeta} : C \rightarrow \mathbb{P}_K^1$ and a faithful character $\lambda : Z := \text{Aut}(\phi) \rightarrow \mathbb{F}_q^*$ such that ϕ is unramified outside of $\{t_1, \dots, t_s\}$ and is ramified at t_i in such a way that the distinguished inertia group generator z_i at t_i satisfies $\lambda(z_i) = \zeta_i$, for $1 \leq i \leq s$. Furthermore, all automorphisms of ϕ are defined over K .*

Proof. This is elementary and well-known, but in order to be able to discuss the examples below it is useful to make this precise. Thus, fix a primitive d -th root $\zeta \in \mathbb{F}_q$ (which exists by hypothesis). Then there exist unique numbers m_1, \dots, m_s with $0 < m_i < d$ such that $\zeta_i = \zeta^{m_i}$. Now consider the cyclic covering $\phi : C \rightarrow \mathbb{P}^1$ defined by the equation

$$y^d = (x - t_1)^{m_1} (x - t_2)^{m_2} \dots (x - t_s)^{m_s}.$$

Since $(m_1, \dots, m_s) = 1$, this is a covering of degree d and since $m_1 + \dots + m_s \equiv 0 \pmod{d}$, it follows that ϕ is unramified at infinity and hence also outside of $\{t_1, \dots, t_s\}$. Now let σ be the unique generator of $Z := \text{Aut}(\phi)$ such that $\sigma(y) = e^{2\pi i/d} y$. Then $z_i = \sigma^{m_i}$ is the distinguished inertia group generator at t_i , and so if we let $\lambda : Z \rightarrow \mathbb{F}_q^*$ be the unique homomorphism such that $\lambda(\sigma) = \zeta$, then $\lambda(z_i) = \zeta_i$, as desired.

Now let J_C denote the Jacobian of the curve C of Lemma 4.15, and let p be a prime not dividing d . Then the group $Z = \text{Aut}(\phi)$ acts on the group $J_C[p]$ of (\bar{K} -rational) p -torsion points of J_C , and so $J_C[p]$ is the direct sum of its λ -components $J_C[p]_{\lambda^k} = J_C[p] \otimes_{\mathbb{F}_p[Z]} V_{\lambda^k}$, where $V_{\lambda^k} \simeq \mathbb{F}_{q^k}$ denotes the representation space of the linear characters $\lambda^k : Z \rightarrow \mathbb{F}_{q^k}^*$ of Z . Since the automorphisms $z \in Z$ are defined over K , the Galois action commutes with the Z -action, and so G_K acts \mathbb{F}_{q^k} -linearly on each space $J_C[p]_{\lambda^k}$ (which has a natural \mathbb{F}_{q^k} -vector space structure). Since $J_C[p]_{\lambda}$ has dimension $n = s - 2$ over \mathbb{F}_q (see [V3], or equation(3) below), this yields a homomorphism $G_K \rightarrow \text{GL}_n(q)$.

Theorem 4.16 *Let $\zeta = (\zeta_1, \dots, \zeta_s)$ be a ζ -tuple in \mathbb{F}_q satisfying condition (1) with the property that $\mathbb{F}_q = \mathbb{F}_p(\zeta_1, \dots, \zeta_s)$, and let $\underline{\sigma}_\zeta = (\sigma_1, \dots, \sigma_{s-1})$ be the associated Thompson tuple in $\mathrm{GL}_n(q)$, where $n = s - 2$. In addition, let t_1, \dots, t_{s-1} be distinct points in k , and let $t_s = X$ be transcendental over k . Put $K = k(X)$, and choose accordingly the cyclic covering*

$$\phi = \phi_{t, \zeta} : C \rightarrow \mathbb{P}_K^1$$

and character $\lambda : Z \rightarrow \mathbb{F}_q^$ as in the previous Lemma. Let $S = J_C[p]_\lambda$ be the associated λ -component of the p -torsion points of J_C , and let $N = N_{\lambda, Z'}$ be the fixed field of the kernel of the homomorphism*

$$\rho_{\lambda, Z'} : G_K \rightarrow \mathrm{GL}_n(q)/Z'$$

induced by the action of G_K on $S \simeq \mathbb{F}_q^n$, where $Z' \leq Z(\mathrm{GL}_n(q))$ is any subgroup containing $\lambda(Z)$.

(a) The Galois group of the extension $\bar{k}N/\bar{k}(X)$ is the subgroup

$$G' = \langle \sigma'_1, \dots, \sigma'_{s-1} \rangle \leq \mathrm{GL}_n(q)/Z'$$

generated by the images σ'_i of the Thompson tuple in $\mathrm{GL}_n(q)/Z'$. Moreover, the ramification type of this extension is $[G', \{t_1, \dots, t_{s-1}\}, \mathbf{C}']$, where $\mathbf{C}' = (C'_1, \dots, C'_{s-1})$ and C'_i denotes the class of σ'_i in G' .

(b) If G' is self-normalizing in $\mathrm{GL}_n(q)/Z'$, then N is regular over k , and hence $\mathrm{Gal}(N/k(X)) \simeq \mathrm{Gal}(\bar{k}N/\bar{k}(X)) \simeq G'$.

Proof. The analogous result for the case that the branch points t_1, \dots, t_s are algebraically independent over k was proved in [V3], Theorem A. So we have to carry through a specialization argument which essentially boils down to replacing the pure braid group $\mathcal{B}^{(s)}$ by its normal subgroup generated by $Q_{1,s}, \dots, Q_{s-1,s}$.

As in the proof of Theorem A of [V3], let \mathcal{O}_s be the space of subsets of \mathbb{C} of cardinality s , and $\mathcal{H}(\mathbf{C})$ the Hurwitz space related to covers of type ζ ; and let \mathbf{p} be a point of $\mathcal{H}(\mathbf{C})$ over the point $\bar{\mathbf{p}} = \{t_1, \dots, t_s\}$ of \mathcal{O}_s such that the corresponding cover of \mathbb{P}^1 has ramification of type ζ_i over t_i . We can proceed as in that proof till to step 4.

There we specialize: \mathcal{O} has to be replaced by the curve $\tilde{\mathcal{L}}$ defined as follows: Let \mathcal{L} be the curve on \mathcal{O}_s consisting of all $\{t_1, \dots, t_{n+1}, t\}$, $t \in \mathbb{C} \setminus$

$\{t_1, \dots, t_{n+1}\}$, and $\tilde{\mathcal{L}}$ the (absolutely) irreducible component of the inverse image of \mathcal{L} in $\mathcal{H}_s(G)^{(\mathbf{A}_1)}$ that contains \mathbf{p}_1 ; here $\mathbf{A}_1 = V \cdot Z'$. The fundamental group $\pi_1(\mathcal{O}_s, \bar{\mathbf{p}})$ can be identified with the braid group \mathcal{B}_s in such a way that $Q_{1,s}, \dots, Q_{s-1,s}$ correspond to loops around t_1, \dots, t_{s-1} on \mathcal{L} that generate $\pi_1(\mathcal{L}, \bar{\mathbf{p}})$. Let H be the stabilizer of $\tilde{\mathcal{L}}$ in $\mathbf{A}_0/\mathbf{A}_1 \cong \mathrm{GL}_n(q)/Z'$. Let $\Phi'_\zeta : \mathcal{B}^{(s)} \rightarrow \mathrm{GL}_n(q)/Z'$ be the composition of Φ_ζ (see Lemma 4.14) with the canonical map $\mathrm{GL}_n(q) \rightarrow \mathrm{GL}_n(q)/Z'$. As in [V5], Lemma 2.2 we see that H is conjugate in $\mathrm{GL}_n(q)/Z'$ to the group G' generated by $\Phi'_\zeta(Q_{1,s}), \dots, \Phi'_\zeta(Q_{s-1,s})$. We may assume $H = G'$.

Then similarly as in Step 4, the Galois action of $G_{\bar{k}(X)}$ on the subspace $S \cong \mathbb{F}_q^n$ of the p -division points of the Jacobian of C induces modulo Z' the group $H = G'$. Furthermore, if we let $N' = \bar{k}N$ (which is the fixed field of the kernel of the map $G_{\bar{k}(X)} \rightarrow G'$), then the extension $N'/\bar{k}(X)$ is ramified where t equals some t_i , and $\Phi'_\zeta(Q_{i,s})$ is a corresponding distinguished inertia group generator. This (together with Lemma 4.14) proves part (a) of the theorem.

(b) Note that $G_{\bar{k}(X)}$ is normal in $G_{k(X)}$. Thus, if G' is self-normalizing in $\mathrm{GL}_n(q)/Z'$, then the image of $G_{k(X)}$ in $\mathrm{GL}_n(q)/Z'$ also equals G' , and so the corresponding extension $N/k(X)$ is regular over k .

Remark 4.17 Let $K(S_\lambda)$ denote the extension of K obtained by adjoining the coordinates of the p -torsion points in $S_\lambda \subset J_C[p]$ to K . Then clearly $K(S_\lambda) = N_{\lambda,1}$ is the fixed field of the kernel of the representation

$$\rho_\lambda : G_K \rightarrow \mathrm{Aut}(S_\lambda) \simeq \mathrm{GL}_n(q)$$

on S_λ , and hence is a Galois extension of K which contains the field(s) $N = N_{\lambda,Z'}$ of Theorem 4.16. Moreover, $K(S_\lambda)$ is cyclic over N with Galois group $\mathrm{Gal}(K(S_\lambda)/N) \leq Z'$. We shall see below in Theorem 5.14 that the extension $K(S_\lambda)/N_{\lambda,Z'}$ is always an *unramified* extension.

The consequence of Theorem 4.16 is that the almost unramified families of covers of \mathbb{P}^1 constructed in the previous section are obtained by adjoining Galois invariant subspaces of torsion points of families of abelian varieties to $K(X)$. This imposes strong conditions on these abelian varieties.

In the next section we shall discuss some consequences of these conditions in more detail.

5 A family of curves with infinite geometric fundamental group

5.1 The abelian variety J_C^{new}

In order to interpret the results of the previous section geometrically, it is useful to introduce the following “new part” J_C^{new} of the Jacobian J_C of a cyclic covering $\pi : C \rightarrow C'$ of curves, which is (partially) analogous to the new part of the Jacobian of the modular curve $X_0(N)$.

Definition 5.1 Let $\pi : C \rightarrow C'$ be a cyclic covering of curves defined over an arbitrary field K , and let $Z = \text{Aut}(\pi) \simeq \mathbb{Z}/N\mathbb{Z}$ denote its covering group. For each subgroup $H \leq Z$ let $\pi_H : C \rightarrow C_H = C/H$ denote the quotient map. Then we call the abelian subvariety

$$J_C^{old} := \sum_{\substack{H \leq Z \\ H \neq 1}} \pi_H^* J_{C/H}$$

the *old part* of J_C , and its orthogonal complement (with respect to the canonical polarization on J_C) the *new part* J_C^{new} .

For our purposes it is important to observe that J_C^{new} and J_C^{old} can be expressed in terms the following idempotent ε_{new} of the group ring $\mathbb{Q}[Z]$:

$$\varepsilon_{new} = \sum_{d|N} \mu(d) \varepsilon_d,$$

where, for a subgroup $H \leq Z$ of order d ,

$$\varepsilon_d = \varepsilon_H = \frac{1}{d} \sum_{h \in H} h \in \mathbb{Q}[Z].$$

Lemma 5.2 *If $\chi : Z \rightarrow \mathbb{C}^*$ is a fixed character of order $N = |Z|$, then*

$$\varepsilon_d = \sum_{\substack{k=0 \\ d|k}}^{N-1} \varepsilon_{\chi^k} \quad \text{and} \quad \varepsilon_{new} = \sum_{\substack{k=1 \\ (k,N)=1}}^{N-1} \varepsilon_{\chi^k}, \quad (2)$$

where $\varepsilon_{\chi^k} = \frac{1}{N} \sum_{g \in Z} \chi(g)^k g^{-1} \in \mathbb{C}[Z]$ denotes the primitive idempotent associated to the character χ^k . In particular, ε_{new} is a symmetric idempotent of $\mathbb{Q}[Z]$ and

$$\varepsilon_d \cdot \varepsilon_{new} = 0, \quad \text{for all } d|N, d \neq 1.$$

Proof. Since the χ^k form a dual basis of the group ring $\mathbb{C}[Z]$, it is enough to verify (2) after evaluating both sides by χ^k , for $k = 0, \dots, N-1$. Now for any class function ψ on Z we have $\psi(\varepsilon_H) = (1_H, \psi|_H)$, $\psi(\varepsilon_{\chi^k}) = (\chi^k, \psi)$. Since for a subgroup H of order d we have $\chi^k|_H = 1_H \iff \text{Ker}(\chi^k) \geq H \iff d|k$, it follows that $\chi^k(\varepsilon_d) = 1$ if $d|k$ and $\chi^k(\varepsilon_d) = 0$ otherwise. From this, the first formula of (2) is obvious and the second follows readily, using the fact that $s := \sum_{d|(k,N)} \mu(d) = 1$, if $(k, N) = 1$ and $s = 0$ otherwise.

Thus, by (2) we see that ε_{new} is a sum of pairwise orthogonal idempotents, and hence is also an idempotent. Furthermore, ε_{new} is symmetric since all ε_d are symmetric.

Finally, if $d \neq 1$, then (2) shows that ε_d and ε_{new} have no common components ε_{χ^k} , and hence are orthogonal.

Corollary 5.3 *Put $\tilde{\varepsilon}_{new} = N\varepsilon$ and $\tilde{\varepsilon}_{old} = N - \tilde{\varepsilon}$. Then $\tilde{\varepsilon}_{new}, \tilde{\varepsilon}_{old} \in \text{End}(J_C)$ and we have*

$$J_C^{old} = \tilde{\varepsilon}_{old}(J_C), \quad J_C^{new} = \tilde{\varepsilon}_{new}(J_C).$$

Furthermore, $J_C = J_C^{old} + J_C^{new}$, and $J_C^{old} \cap J_C^{new} \leq J_C[N]$; in particular, $J_C \sim J_C^{old} \times J_C^{new}$.

Proof. By definition, $N\varepsilon_{new} \in \mathbb{Z}[Z] \subset \text{End}(J_C)$, and so $\tilde{\varepsilon}_{new}, \tilde{\varepsilon}_{old} \in \text{End}(J_C)$; note that $\tilde{\varepsilon}_{old} = N(1 - \varepsilon_{new}) = \sum_{1 \neq d|N} \mu(d)N\varepsilon_d$. Put $\tilde{\varepsilon}_d = d\varepsilon_d \in \mathbb{Z}[Z]$. Then $\tilde{\varepsilon}_d(J_C) = \pi_{H_d}^*(J_C/H_d)$, so it follows from the definition that $\tilde{\varepsilon}_{old}(J_C) \subset \sum_{1 \neq d|N} \pi_{H_d}^*(J_C/H_d) = J_C^{old}$. On the other hand, by Lemma 5.2 we have $\tilde{\varepsilon}_{old}\tilde{\varepsilon}_d = N\tilde{\varepsilon}_d$, if $d \neq 1$, so $\pi_{H_d}^*(J_C/H_d) = \tilde{\varepsilon}_d(J_C) = \tilde{\varepsilon}_{old}(\tilde{\varepsilon}_d(J_C)) \subset \tilde{\varepsilon}_{old}(J_C)$ and hence $J_C^{old} = \tilde{\varepsilon}_{old}(J_C)$. By construction, $\tilde{\varepsilon}_{new} + \tilde{\varepsilon}_{old} = N$, $\tilde{\varepsilon}_{new} \cdot \tilde{\varepsilon}_{old} = 0$, so $J_C^{new} := \tilde{\varepsilon}_{new}(J_C)$ is the orthogonal complement of J_C^{old} , and hence the isogeny relation follows.

Corollary 5.4 *Suppose $p \neq \text{char}(K)$ is a prime with $p \equiv 1 \pmod{N}$. Then there exist primitive characters $\lambda : Z \rightarrow \mathbb{F}_p^*$ and $\tilde{\lambda} : Z \rightarrow \mathbb{Z}_p^*$ of order N and we have natural identifications (of Z -modules and G_K -modules)*

$$J_C^{new}[p] = \bigoplus_{\substack{1 \leq k < N \\ (k, N) = 1}} J_C[p]_{\lambda^k}, \quad \text{and} \quad T_p(J_C^{new}) = \bigoplus_{\substack{1 \leq k < N \\ (k, N) = 1}} T_p(J_C)_{\tilde{\lambda}^k},$$

where $T_p(A) = \varprojlim A[p^n]$ denotes the Tate-module of an abelian variety A . In particular, $\dim J_C^{new} = \frac{1}{2}\phi(N)(2g_{C'} - 2 + r)$, where $r = \#\{P \in C'(\bar{K}) : e_P(\pi) > 1\}$ denotes the number of ramified primes.

Proof. By the hypothesis on p , both \mathbb{F}_p and \mathbb{Z}_p contain a primitive N -th root of unity and so λ and $\tilde{\lambda}$ exist. Thus, if we replace χ by λ and $\tilde{\lambda}$ in (2), the analogous formulae of (2) hold in $\mathbb{F}_p[Z]$ and in $\mathbb{Z}_p[Z]$. From this the above decomposition follows because $J_C^{new}[p] = \varepsilon_{new}(J_C[p])$ and $J_C[p]_{\lambda^k} = \varepsilon_{\lambda^k}(J_C[p])$, and similarly, $T_p(J_C^{new}) = \varepsilon_{new}T_p(J_C)$ and $T_p(J_C)_{\tilde{\lambda}^k} = \varepsilon_{\tilde{\lambda}^k}T_p(J_C)$. (Note that this is also a decomposition of G_K -modules since the Z -action commutes with the G_K -action.)

To work out the dimension of J_C^{new} , we use the well-known fact (cf. Serre[Se2], p. 106) that the character h_1 of the representation of Z on $T_p(J_C) \otimes \mathbb{Q}_p$ is given by

$$h_1 = 2 \cdot 1_Z + (2g_{C'} - 2)\text{reg}_Z + a_Z$$

where $a_Z = \sum_{P' \in C'} a_{P'}$, and $a_{P'} = (\text{reg}_Z - 1_{D_P}^*)$ denotes the (tame) Artin character at P' . (Here D_P is the decomposition group of any $P \in \pi^{-1}(P')$, and $*$ denotes induction.) From this it follows easily (by Frobenius reciprocity) that if $k \not\equiv 0 \pmod{N}$, then the rank of $T_p(J_C)_{\tilde{\lambda}^k}$ ($= \dim_{\mathbb{F}_p}(J_C[p]_{\lambda^k})$) is

$$(h_1, \tilde{\lambda}^k) = (2g_{C'} - 2) + r_k, \text{ where } r_k := (a_Z, \tilde{\lambda}^k) = \#\{P' \in C' : e_{P'} \nmid k\}. \quad (3)$$

Since $\text{rank}(T_p(J_C^{new})) = 2 \dim(J_C^{new})$, the asserted dimension formula follows.

Using the abelian variety J_C^{new} , we can now give the following geometric interpretation of the main result (Theorem 4.16) of the previous section.

Theorem 5.5 *Let $K = k(t)$, where t is transcendental over k and k contains the N -th roots of unity. Suppose that t_1, \dots, t_{n+1} are $n+1$ distinct elements in k , and put $t_{n+2} = t$. In addition, suppose that m_1, \dots, m_{n+2} are integers with $1 \leq m_i < N$ such that $\gcd(m_1, \dots, m_{n+2}, N) = 1$, $m_1 + \dots + m_{n+2} \equiv 0 \pmod{N}$ and $m_i \neq N - m_{n+2}$, for $1 \leq i \leq n+1$. Let $\pi : C \rightarrow \mathbb{P}^1$ denote the cyclic covering of degree N defined by the equation*

$$y^N = c(x - t_1)^{m_1} \cdots (x - t_{n+2})^{m_{n+2}}, \quad (4)$$

where $c \in k^*$, and let $A = J_C^{new}$ denote the new part of the Jacobian J_C of C . Then $\dim A = \frac{1}{2}\phi(N)n$, and for any prime $p \equiv 1 \pmod{N}$ we have:

(a) *The group $A[p]$ of p -torsion points of A is the direct sum of G_K -invariant subspaces $S_i = J_C[p]_{\lambda^i}$, where $(i, N) = 1$, and $\lambda : Z = \text{Aut}(\pi) \rightarrow \mathbb{F}_p^*$ is a primitive character. Moreover, G_K acts irreducibly on each S_i , and hence semi-simply on $A[p]$.*

(b) Let L_i (respectively, \tilde{M}_i and M_i) denote the fixed field of the kernel of the action of G_K on S_i (respectively, on $S_i/\lambda^i(Z)$ and on $\mathbb{P}(S_i)$), so $L_i \supset \tilde{M}_i \supset M_i$. Then L_i/\tilde{M}_i is a cyclic extension of order dividing N , and \tilde{M}_i/K (respectively, M_i/K) is a Galois extension whose geometric part $\tilde{G} := \text{Gal}(\bar{k}\tilde{M}_i/\bar{k}K) \leq \text{GL}_n(p)/\lambda^i(Z)$ (respectively, $\bar{G} := \text{Gal}(\bar{k}M_i/\bar{k}K) \leq \text{PGL}_n(p)$) is generated by the image of the Thompson tuple attached to the covering. In addition, \tilde{M}_i (and hence also M_i) is ramified only at t_1, \dots, t_{n+1} with ramification order dividing N .

(c) The field $K(A[p])$ (which is generated over K by the coordinates of all p -torsion points of A) is an abelian extension of the compositum \tilde{M} of all the \tilde{M}_i 's of degree dividing $N^{\phi(N)}$. Moreover, \tilde{M}/K is ramified only at t_1, \dots, t_{n+1} with ramification order dividing N .

(d) If $(n, p-1) = 1$, (and $N \nmid 6$ if $n = 3$), then M_i is regular over k and

$$\text{Gal}(M_i/K) = \text{PGL}_n(p) = \text{PSL}_n(p).$$

Proof. (a) The first assertion follows directly from the decomposition of Corollary 5.4. Next, choose a ‘‘canonical generator’’ σ of Z as in the proof of Lemma 4.15. Then for any i with $(i, N) = 1$, the hypotheses on the m_j 's guarantee that the $(n+2)$ -tuple $\zeta_1 = \lambda^i(\sigma^{m_1}), \dots, \zeta_{n+2} = \lambda^i(\sigma^{m_{n+2}})$ satisfies condition (1) of Lemma 4.14 and so by Theorem 4.16(a) (with $Z' = Z(\text{GL}_n(p))$) it follows that the image of the Galois group $G_{\bar{k}K}$ on $\mathbb{P}(S_i)$ is generated by a Thompson tuple and hence $G_K \geq G_{\bar{k}K}$ acts irreducibly on S_i . (b) Since $\text{Gal}(L_i/\tilde{M}_i) = \text{Gal}(L_i/K) \cap \lambda^i(Z) \leq \lambda^i(Z)$ (viewed as subgroups of $\text{Aut}_{\mathbb{F}_p}(S_i) \simeq \text{GL}_n(p)$), the first assertion is clear. The other assertions follow directly from Theorem 4.16(a) by taking $Z' = \lambda^i(Z)$ (respectively, $Z' = Z(\text{GL}_n(p))$).

(c) Since $A[p]$ is the direct sum of the S_i 's (cf. part (a)), we have $K(A[p]) = \prod L_i$, and so both assertions follow from part (b).

(d) The hypothesis implies that n is odd and that $\text{PSL}_n(p) = \text{PGL}_n(p)$. Thus, from Theorem 4.6 it follows that the image \bar{G} of the Thompson tuple in $\text{PGL}_n(p)$ generates the whole group. In particular, \bar{G} is self-normalizing, and so M_i is regular over k by Theorem 4.16(b).

Remark 5.6 We shall see below in Theorem 5.14 that the extension L_i/M_i is always unramified; in particular, $K(A[p])$ is unramified over \tilde{M} .

By applying a variant of the Serre-Tate criterion of potentially good reduction (see below), we obtain

Theorem 5.7 *If C/K is as in Theorem 5.5, then the new part $A = J_C^{\text{new}}$ of its Jacobian J_C has potentially good reduction over K . In other words, there is a finite extension K_0 of K such that $A_{K_0} = A \otimes K_0$ extends to an abelian scheme \mathcal{A} over the projective curve T_0 with function field K_0 , i.e. for each geometric point $P \in T_0(\bar{K})$ the fibre of \mathcal{A} over P is an abelian variety.*

Proof. By Theorem 5.5 (c), we see that for all primes $p \equiv 1 \pmod{N}$, the ramification degrees of the extension $K(A[p])/K$ divide $N^{\phi(N)+1}$, and so the assertion follows from the following criterion:

Proposition 5.8 (Serre-Tate Criterion) *Let K be a field with a discrete valuation v , and let A be an abelian variety over K . Then the following conditions are equivalent:*

- (i) *A has potentially good reduction at v ;*
- (ii) *the ramification degree of v in $K(A[m])$ is bounded for all m prime to $\text{char}(\kappa(v))$;*
- (iii) *there is a constant c such that the ramification degree $e_v(K(A[p])/K) \leq c$, for infinitely many primes p .*

Proof. This is well-known, but for convenience of the reader we present the proof.

(i) \Rightarrow (ii): This follows from the criterion of Néron-Ogg-Shafarevich for good reduction; cf. Serre-Tate[ST], Theorem 2.

(ii) \Rightarrow (iii): Trivial.

(iii) \Rightarrow (i): By replacing K by a suitable finite extension K' , we may assume without loss of generality that A has semi-stable reduction at v . (For example, we could take $K' = K(A[p])$, for any prime $p \geq 3$, $p \neq \text{char}(\kappa(v))$; cf. Grothendieck[Gro], Prop. 4.7). In addition, we may assume that K is henselian with separably closed residue field. Then the implication (iii) \Rightarrow (i) follows once we have verified:

Claim: If A does not have good reduction at v , then $p|e_v(K(A[p])/K)$, for every prime $p \nmid \#\Phi(A_K)$ ($p \neq \text{char}(\kappa(v))$), where $\Phi(A_K)$ denotes the (finite) group of components of the Néron model of A/K with respect to v .

To see this, we first note that for p as above, $\#(A[p](K)) = \#(A^0[p](\kappa(v))) = p^{t+2a}$, where t denotes the toric rank and a the abelian rank of the connected component A^0 of the identity of the reduction of the Néron model. (Note

that $t + a = d := \dim A$, and that $t > 0$ since A has bad reduction.) On the other hand, for $K' = K(A[p])$ we clearly have $\#(A[p](K')) = p^{2d}$, and so $p^t | \#\Phi(A_{K'})$. Thus, $p | \#(\Phi(A_{K'})/\Phi(A_K))$. On the other hand, the quotient group $\Phi(A_{K'})[p]/\Phi(A_K)[p]$ has exponent $e_v(K'/K)$; this follows from [Gro], Th. 11.5, together with formula (10.3.5). Thus $p | e_v(K'/K)$, as asserted.

Remark. In the above implication (iii) \Rightarrow (i) we needed several deep results from Grothendieck's article [Gro]. However, all these can be avoided if in condition (iii) we can assume in addition that $K(A[p])/K$ is *tamely ramified* for the primes p in question. (This is always the case if $|\mathrm{GL}_{2d}(p)|$ is prime to the residue characteristic $\mathrm{char}(K)$, but for the above application we need to assume only that $(\mathrm{char}(K), N) = 1$ since we already know that the ramification degree divides a power of N .)

In that case the implication (iii) \Rightarrow (i) can be proved as follows:

Again, it is enough to prove this in the case that K is henselian with separably closed residue field. If L denotes the compositum of the $K(A[p])$'s for the primes in question, then the hypothesis (and tame ramification) implies that L is a finite (cyclic) extension of K . By construction, $L(A[p]) = L$ for infinitely many p 's, so by the Néron-Ogg-Shafarevich criterion for good reduction (cf. [ST], Theorem 1), A has good reduction over L and hence potentially good reduction over K .

Let us now come back to Theorem 5.7. By imposing further restrictions on the m_i 's, we can conclude that all of J_C has potentially good reduction:

Corollary 5.9 *Suppose that C/K is as above and satisfies in addition the condition that $m_i \not\equiv -m_{n+2} \pmod{d}$, for every $d|N$ with $e_{n+2} \nmid d \neq 1$, where $e_{n+2} = \frac{N}{(m_{n+2}, N)}$. Then J_C has potentially good reduction over K .*

Proof. Induct on the number of the divisors of N . If N is prime, then $J_C = J_C^{\mathrm{new}}$ and so the assertion follows from the theorem. If N is composite, then by the theorem it is enough to show that J_C^{old} has potentially good reduction or, equivalently, that every $J_d := J_{C/H_d}$ has potentially good reduction (for $d|N$, $d \neq 1$). This is clear if $e := e_{n+2} | d$, for then $C_d := C_{H_d}$ is unramified at t_{n+2} and hence the covering is already defined over K . Thus, assume $e \nmid d$. Then the ramification of $C_d \rightarrow \mathbb{P}^1$ satisfies the same hypotheses as $C \rightarrow \mathbb{P}^1$, and so by the induction hypothesis we have that J_{C_d} has good reduction.

5.2 Rational points on $K(\mathbb{P}(S_i))$

One of the advantages of the above geometric description of the extensions generated by Thompson tuples is that it is possible to determine whether or not the extension field has a rational point. This is based on the following (well-known) fact.

Proposition 5.10 *Let A be an abelian variety over K which has potentially good reduction with respect to a discrete valuation v on K . Suppose that v is unramified in $K' = K(A[m])$, where $m \geq 3$ is an integer which is relatively prime to the characteristic of the residue field $k = \kappa(v)$ of v . Then:*

- (i) *the reduction A_v of A at v is an abelian variety over k ;*
- (ii) *if v' denotes any extension of v to K' , then its residue field is $\kappa(v') = k(A_v[m])$.*

Proof. The first assertion follows from [ST], Theorem 2, Corollary 2(b). To prove the second, let $k' = \kappa(v')$. Then the reduction map $r_{v'} : A(K') \rightarrow A_{v'}(k')$ induces an isomorphism $A[m](K') \simeq A_{v'}[m](k')$, so all m -torsion points of A_v are rational over k' . Thus $k(A_v[m]) \subset k'$. To prove that equality holds, let $\sigma \in \text{Gal}(k'/k(A_v[m]))$. Then σ lifts uniquely to an automorphism $\tilde{\sigma} \in D_{v'}(K'/K)$, where $D_{v'}(K'/K) \leq \text{Gal}(K'/K)$ denotes the decomposition group of v' . Since the action of $\tilde{\sigma}$ on $A[m]$ is (via $r_{v'}$) the same as that of σ on $A_{v'}[m] = A_v[m]$, this means that $\tilde{\sigma}$ acts trivially on $A[m]$. But then $\tilde{\sigma}$ and hence σ are both trivial, so $k' = k(A_v[m])$.

Corollary 5.11 *In the above situation, suppose that $S \subset A[m]$ is a G_K -invariant subspace. Let \bar{S} denote the image of S in $A_{v'}[m]$. Then $\kappa(v'_{K(S)}) = k(\bar{S})$ and $\kappa(v'_{K(\mathbb{P}(S))}) = k(\mathbb{P}(\bar{S}))$. In particular, if $m = p$ is a prime, then v splits completely in $K(\mathbb{P}(S))$ if and only if every \bar{k} -isogeny of A_v with kernel in \bar{S} is k -rational.*

Proof. By the same argument as in the proof of the proposition, we see that $\text{Gal}(k'/k(\bar{S})) \simeq D_{v'}(K'/K) \cap \text{Gal}(K'/K(S)) = D_{v'}(K'/K(S))$, and so the first assertion follows. To prove the second, we note that the group $\text{Gal}(K(S)/K(\mathbb{P}(S)))$ consists of those $\sigma \in \text{Gal}(K(S)/K)$ which act diagonally on S . Since $\text{Gal}(k(\bar{S})/k(\mathbb{P}(\bar{S})))$ is defined similarly, we see that $\text{Gal}(k(\bar{S})/k(\mathbb{P}(\bar{S}))) \simeq D_{v'_{K(S)}}(K(S)/K(\mathbb{P}(S)))$, and so the second assertion follows.

To prove the last assertion, we observe that by the above result v splits completely in $K(\mathbb{P}(S)) \iff k(\mathbb{P}(\bar{S})) = k \iff$ every $\sigma \in \text{Gal}(k(\bar{S})/k)$ acts diagonally on $\bar{S} \iff \sigma(\mathbb{F}_p \bar{s}) = \mathbb{F}_p \bar{s}$, for all $\bar{s} \in \bar{S}$ and $\sigma \in \text{Gal}(k(\bar{S})/k) \iff$ every isogeny $\varphi : A_v \rightarrow A'$ with kernel $\text{Ker}(\varphi) = \mathbb{F}_p \bar{s}$ (where $\bar{s} \in \bar{S} - \{0\}$) is k -rational \iff every \bar{k} -isogeny of A_v with kernel in \bar{S} is k -rational.

The main difficulty in applying the above criterion to our situation is the fact that we need to guarantee that v is unramified in $K(A[p])$ for some p . Although we already know by Theorem 5.5 the ramification behaviour of the extension $K(\mathbb{P}(S_i))/K$, there remains the problem of understanding that of $K(S_i)/K(\mathbb{P}(S_i))$. This will be analyzed next by using the following criterion.

Proposition 5.12 *Let A/K be an abelian variety and let v be a discrete valuation of K . Moreover, let $I = I_v$ denote the inertia group of an extension v' of v to $K' = K(A[p])$, where $p \neq \text{char}(\kappa(v))$ is a prime. If $S \subset A[p]$ is a non-zero G_K -invariant subspace and $H = \text{Gal}(K'/K(\mathbb{P}(S)))$, then $v'_{|K(S)}$ is unramified over $K(\mathbb{P}(S))$ if and only if $S^{I \cap H} \neq \{0\}$. In particular, if $S^I \neq \{0\}$, then $v'_{|K(S)}$ is unramified over $K(\mathbb{P}(S))$.*

Proof. Let $H_0 = \text{Gal}(K'/K(S)) \leq H$. Then $v'_{|K(S)}$ is unramified over $K(\mathbb{P}(S)) \iff I \cap H \leq H_0 \iff I \cap H$ acts trivially on $S \iff S^{I \cap H} = S$. Thus, if $v'_{|K(S)}$ is unramified, then clearly $S^{I \cap H} = S \neq \{0\}$. Conversely, if $S_0 := S^{I \cap H} \neq \{0\}$ and $g \in I \cap H$, then g acts diagonally on S and trivially on S_0 , so g acts trivially on all of S . Thus $I \cap H \leq H_0$, and so $v'_{|K(S)}$ is unramified.

Corollary 5.13 *Suppose in addition that $S = A[p]_\lambda$ where $\lambda : Z \rightarrow \mathbb{F}_p^*$ is a character on a finite subgroup $Z \leq \text{Aut}(A)$. If either $A[p]_\lambda^I \neq \{0\}$ or if $T_p(A)_\lambda^{\tilde{I}} \neq \{0\}$, where $\tilde{\lambda} : Z \rightarrow \mathbb{Z}_p^*$ is a lift of λ and $\tilde{I} \leq G_K$ denotes the absolute inertia group of an extension of v (and of v') to K^{sep} , then $v'_{|K(S)}$ is unramified over $K(\mathbb{P}(S))$.*

In particular, if the reduction A_v of the Néron model of A/K at v is not unipotent (i.e. the connected component of A_v is not an extension of additive groups), then v' is unramified over $K(\mathbb{P}(A[p]))$.

Proof. If the second hypothesis holds, then also $V := T_p(A)_\lambda^{\tilde{I}} \otimes \mathbb{F}_p \neq \{0\}$. But then $\{0\} \neq V \subset (T_p(A)_\lambda \otimes \mathbb{F}_p)^{\tilde{I}} = A[p]_\lambda^I$, which means that the second

hypothesis implies the first. Now if the first hypothesis holds, then $S^{I \cap H} \supset S^I \neq \{0\}$, and so the conclusion follows directly from the proposition.

In particular, taking for $\tilde{\lambda}$ the trivial character (on $Z = \{1\}$), then by [Gro], Prop. 2.2.5 (and (2.1.11)) we have $\text{rank}(T_p(A)^{\tilde{\lambda}}) = n - \lambda(A)$, where $n = \dim(A)$ and $\lambda(A)$ denotes the unipotent rank of A_v . Thus, $T_p(A)^{\tilde{\lambda}} = \{0\} \iff A_v$ is unipotent, and so the assertion follows from the previous criterion.

The above criterion can be used in our situation in the following way.

Theorem 5.14 *In the situation and notation of Theorem 5.5, let v_i denote the place of K/k corresponding to the specialization $t \rightarrow t_i$, for $1 \leq i \leq n+1$. Then:*

(a) *If v is any place of K/k with $v \notin R := \{v_1, \dots, v_{n+1}\}$, then C and hence J_C and $A = J_C^{\text{new}}$ have good reduction at v .*

(b) *For each i with $1 \leq i \leq n+1$, let \bar{C}_i denote the normalization of the curve*

$$y^N = c(x - t_1)^{m_1} \cdots (x - t_{n+1})^{m_{n+1}} \cdot (x - t_i)^{m_{n+2}},$$

and let $\bar{\pi}_i : \bar{C}_i \rightarrow \mathbb{P}_k^1$ denote the associated cyclic covering of degree N . Then \bar{C}_i is the normalization of the reduction of C at v_i , and the new part $J_{\bar{C}_i}^{\text{new}}$ of its Jacobian has dimension $\frac{1}{2}\phi(N)(n-1)$.

(c) *Let J_{v_i} and A_{v_i} denote the reductions of the Néron models of J_C and $A = J_C^{\text{new}}$ at v_i , and let $J_{v_i}^0$ and $A_{v_i}^0$ denote their respective connected components of the identity. Then there are natural surjections of algebraic groups $f_i : J_{v_i}^0 \rightarrow J_{\bar{C}_i}^0$ and $f_i^{\text{new}} : A_{v_i}^0 \rightarrow J_{\bar{C}_i}^{\text{new}}$.*

(d) *Let $\tilde{I} = \tilde{I}_{v_i} \leq G_K$ denote the inertia group of an extension of v_i to K^{sep} . Then for any prime $p \equiv 1 \pmod{N}$ (with $p \neq \text{char}(K)$) and any primitive character $\tilde{\lambda} : Z \rightarrow \mathbb{Z}_p^*$, we have that $\text{rank}(T_p(J_C)^{\tilde{\lambda}}) \geq n - 1$.*

(e) *For p as above, let $\lambda : Z \rightarrow \mathbb{F}_p^*$ be a primitive character. Then for any j with $(j, N) = 1$, the extension $L_j = K(S_j)$ is everywhere unramified over $M_j = K(\mathbb{P}(S_j))$, and hence $K' = K(A[p])$ is ramified over K only at the places of R with ramification index dividing N and is unramified over $M = \prod M_j$.*

Proof. Recall that C is by definition the normalization of the projective plane curve $C' \subset \mathbb{P}_K^2$ defined by equation (4). Let \mathcal{C}' denote the closure of C in $\mathbb{P}_{\mathbb{P}^1}^2 = \mathbb{P}^2 \times \mathbb{P}^1$, and let $\nu : \mathcal{C} \rightarrow \mathcal{C}'$ denote its normalization (in $\kappa(\mathcal{C}') = \kappa(C)$).

Then, if v is a place of K/k with $v \neq v_\infty$, the place at infinity, then the fibre C'_v of \mathcal{C}' is the projective plane curve over $\kappa(v)$ defined by the equation

$$y^N = c(x - t_1)^{m_1} \cdots (x - t_{n+1})^{m_{n+1}} \cdot (x - \bar{t})^{m_{n+2}},$$

where $\bar{t} \in \kappa(v) \supset K$ denotes the image of t in the residue field of v . Since this curve is reduced and geometrically irreducible, it follows that the same is true for the fibres C_v of \mathcal{C} , and so the normalization $\tilde{\nu}_v : \tilde{C}_v \rightarrow C'_v$ of C'_v factors over the finite map $\nu_v : C_v \rightarrow C'_v$. Note that by considering a different affine model, the above argument extends to show that the last assertions are also true for $v = v_\infty$.

(a) If $v \neq v_\infty$, then the hypothesis on v means that $\bar{t} \neq t_1, t_2, \dots, t_{n+1}$. Thus, by Riemann-Hurwitz, the genus of \tilde{C}_v is the same as that of C , and so C has good reduction at v . Then J_C also has good reduction (cf. [BLR], 9.4/4) and hence so does any quotient A of J_C (cf. [BLR], 7.5/3). Since the argument for $v = v_\infty$ is similar, this proves assertion (a).

(b) Now suppose that $v = v_i$, so $\bar{t} = t_i$ (and $\kappa(v) = k$). Then C'_v is the projective plane curve defined by the given equation and so by what was said above, $\bar{C}_i = \tilde{C}_v$, which proves the first assertion. The second assertion follows directly from Corollary 5.4, for $\bar{\pi}_i : \bar{C}_i \rightarrow \mathbb{P}_k^1$ is a cyclic covering of degree N which is ramified at precisely $r = n + 1$ places.

(c) Let $\delta : \tilde{\mathcal{C}} \rightarrow \mathcal{C}$ denote a desingularization of \mathcal{C} (which exists since the base \mathbb{P}_K^1 is clearly excellent). Then, since \mathcal{C} is normal, \bar{C}_i is the normalization of a component of the fibre \tilde{C}_v of $\tilde{\mathcal{C}}$ at $v = v_i$. Thus, we have a natural surjection $\text{Pic}_{\tilde{C}_v/k}^0 \rightarrow \text{Pic}_{\bar{C}_i/k}^0$ (cf. [BLR], 9.2/13). On the other hand, by [BLR], Th. 9.5/4, $\text{Pic}_{\tilde{C}_v/k}^0$ is canonically isomorphic to the connected component J_i^0 of the identity of the reduction $J_i = J_{v_i}$ of the Néron model of J_C at $v = v_i$, and so we have a canonical surjection $f_i : J_i^0 \rightarrow J_{\bar{C}_i}$.

Next we observe that the covering automorphisms $\sigma \in \text{Aut}(\pi)$ map isomorphically onto those of $\bar{\pi}_i : \bar{C}_i \rightarrow \mathbb{P}_k^1$, and so these extend to automorphisms of J_i^0 and of $J_{\bar{C}_i}$ in such a way that f_i becomes equivariant. From this it follows that if $\bar{\varepsilon}_i : J_{\bar{C}_i} \rightarrow J_{\bar{C}_i}^{\text{new}}$ denotes the projection map onto the new part of $J_{\bar{C}_i}$ (cf. Corollary 5.3), then the composition $\bar{\varepsilon}_i \circ f_i$ factors over the map $\tilde{\varepsilon}_{\text{new},i} : J_i^0 \rightarrow A_{v_i}^0$ which is induced by the universal property of Néron models; i.e. there is a homomorphism $f_i^{\text{new}} : A_{v_i}^0 \rightarrow J_{\bar{C}_i}^{\text{new}}$ such that $\bar{\varepsilon}_i \circ f_i = f_i^{\text{new}} \circ \tilde{\varepsilon}_{\text{new},i}$. Thus, since f_i and $\bar{\varepsilon}_i$ are surjective, so is f_i^{new} , which proves the assertion.

(d) By Grothendieck [Gro], Prop. 2.2.5 (and (2.2.3.3)), we have a natural identification $T_p(A_i^0) \simeq T_p(A)^{\tilde{I}}$ (after passing to the henselization of v_i). Since

the action of Z commutes with the Galois action, this induces an isomorphism $T_p(A_i^0)_{\bar{\lambda}} \simeq T_p(A)_{\bar{\lambda}}^{\tilde{f}}$. Now by (c), the map f_i^{new} is surjective, hence so is the induced map on the Tate modules, and therefore $T_p(A_i^0)_{\bar{\lambda}} \rightarrow T_p(J_{\bar{C}_i})_{\bar{\lambda}}$ is surjective as well. Thus, $\dim T_p(A)_{\bar{\lambda}} \geq \dim T_p(J_{\bar{C}_i})_{\bar{\lambda}} = n - 1$, the latter by formula (3) of Corollary 5.4.

(e) Let v be a place of K/k . If $v \neq v_i$, then A has good reduction at v , so $K(A[p])$ is unramified over K at v , hence a fortiori so is $K(S_j)$ over $K(\mathbb{P}(S_j))$. On the other hand, if $v = v_i$, then in view of (d) we can apply the criterion of Corollary 5.13 to see that $v'_{|K(S_j)}$ is unramified over $K(\mathbb{P}(S_j))$ for every extension v' of v . Thus, $L_j = K(S_j)$ is everywhere unramified over $M_j = K(\mathbb{P}(S_j))$ and hence $K(A[p]) = \prod L_j$ is unramified over $M = \prod M_j$ as well. On the other hand, it follows from Theorem 5.5 that each M_j and hence M is unramified outside R and ramified at each $v_i \in R$ of order dividing N , so the same is true for K' .

By using the above proposition, we can now make the assertion of Theorem 5.7 much more precise.

Theorem 5.15 *Let K_0 be a finite Galois extension of $K = k(t)$ such that the ramification index $e_i = e_{v_i}(K_0/K)$ at v_i is divisible by N , for $1 \leq i \leq n + 1$. Then $A = J_C^{new}$ has good reduction everywhere over K_0 , and hence $K_0(A[m])$ is unramified over K_0 for every integer m relatively prime to $\text{char}(K)$.*

Proof. If $p \equiv 1 \pmod{N}$ is any prime ($p \neq \text{char}(K)$), then by Abhyankar's Lemma it follows from Theorem 5.14(e) that $K_0(A[p]) = K(A[p]) \cdot K_0$ is unramified over K_0 . By the criterion of Néron-Ogg-Shafarevich, this means that $A_{K_0} = A \otimes K_0$ has good reduction everywhere, and hence $K_0(A[m])$ is unramified over K_0 for all m which are prime to $\text{char}(K)$.

Thus, by above theorem we can now apply Corollary 5.11 to obtain following criterion for the existence of rational points:

Corollary 5.16 *Suppose in addition that $v = v_{i_0}$ is totally ramified in K_0 , and let $A_{\tilde{v}}$ denote the reduction of $A \otimes K_0$ at \tilde{v} , where \tilde{v} denotes the (unique) extension of v to K_0 . If $p \neq \text{char}(K)$ is any prime and $S \subset A[p]$ is a G_K -invariant subspace such that*

($\star\star$) every isogeny of the reduction $A_{\tilde{v}}$ with kernel contained in \bar{S} (= the image of S in $A_{\tilde{v}}$) is rational over K ,

then every extension of \tilde{v} to $M_S := K_0(\mathbb{P}(S))$ is a K -rational point of M_S .

5.3 Example

We now return to Example 4.11, but change the notation slightly to conform with that of this section. Thus, let k be a field containing a primitive fourth root of unity i (so in particular $\text{char}(k) \neq 2$). As before, take $n = 3$ and (in the notation of Theorem 5.5) $N = 4$, $m_1 = \dots = m_3 = 1$, $m_4 = 3$ and $m_5 = 2$. Moreover, let the ramification points be $t_1 = 0, t_2 = 1, t_3 = -1, t_4 = a, t_5 = t$ where $a \in k \setminus \{0, \pm 1\}$ and t is transcendental over k , and put $K = k(t)$. Then a corresponding cyclic cover $\pi : C \rightarrow \mathbb{P}_K^1$ is given by the equation

$$Y^4 = cX(X-1)(X+1)(X-a)^3(X-t)^2 \text{ with } c \in k^*. \quad (5)$$

Clearly, C has genus 4 and $\deg(\pi) = 4$. Moreover, π has a subcover of degree 2 whose quotient curve is an elliptic curve E given by the equation

$$Z^2 = cX(X-1)(X+1)(X-a) \text{ with } Z = Y^2/((X-a)(X-t)). \quad (6)$$

Note that E is a constant curve, i.e. E is already defined over k . Moreover, E maps injectively into the Jacobian J_C of C and can be identified with the old part J_C^{old} of J_C (cf. section 5.1). Its complement in J_C is therefore the new part $A = J_C^{\text{new}}$; thus $J_C \sim E \times A$ and so $\dim A = 3$.

Next we choose a cyclic extension K_0 of K of degree 4 which is totally ramified at each of the points of $R = \{0, 1, -1, a\}$. For example, we can take $K_0 = k(t, s)$ where

$$s^4 = t(t^2 - 1)(t - a)g(t), \quad (7)$$

and $g(t) \neq 0$ is any nonzero polynomial of which does not vanish at R . Thus, if T_0 denotes the smooth curve over k defined by this equation (whose function field is K_0), then by Theorem 5.15 we obtain

Proposition 5.17 *The abelian variety $A_{K_0} = A \otimes K_0$ extends to an abelian scheme \mathcal{A} over the curve T_0 .*

Now we want to verify that the tower of unramified covers $K_0(\mathbb{P}(S_p))$ of K_0 attached to the subspaces $S_p \subset A[p]$ for $p \equiv 1 \pmod{4}$ has rational points which all lie over the same base-point \tilde{v} of K_0 .

For this we shall use the criterion $(\star\star)$ of Corollary 5.16 applied to the place $v = v_4$ corresponding to the specialization of t to $t_4 = a$. However, in order to do this, we need to determine the structure of the reduction $A_0 := A_{\tilde{v}}$ of A_{K_0} at the unique extension \tilde{v} of v to K_0 . (Recall that by the above proposition we know that A_0 is an abelian variety over k .) As a first step towards this end, we shall prove:

Proposition 5.18 *Let $J_{\tilde{v}}$ denote the reduction of the Jacobian $J = J_C \otimes K_0$ at \tilde{v} . Then*

$$J_{\tilde{v}} \simeq J_0 \times E_d,$$

where J_0 is the Jacobian of the curve C_0 which is the normalization of the curve defined by the equation

$$\bar{Y}^4 = c\bar{X}(\bar{X} - 1)(\bar{X} + 1)(\bar{X} - a)$$

and E_d denotes the elliptic curve given by the equation

$$Y^2 = X(X^2 - d), \tag{8}$$

where $d = c/g(a)$ and g is as in (7).

Proof. First note that since $J_C \sim E \times A$, and E is a constant curve, it follows from Proposition 5.17 that J has good reduction over T_0 and in particular at \tilde{v} . Thus, if \mathcal{C} denotes the minimal model of C at \tilde{v} , then \mathcal{C} has semi-stable reduction (use [BLR], 9.5/4, 9.2/5 and 9.2/12). Thus, if C_1, \dots, C_r denote the irreducible components of the reduction $C_{\tilde{v}}$ of \mathcal{C} , then each C_i is smooth (by [BLR], 9.2/12) and we have (by [BLR], 9.5/4 and 9.2/8)

$$J_{\tilde{v}} = J_{C_1} \times \dots \times J_{C_r}.$$

Thus, the assertion follows once we have shown that C_0 and E_d occur as components of $C_{\tilde{v}}$, for then all other components must have genus 0 (since $g(C) = 4, g(C_0) = 3$ and $g(E_d) = 1$). For this it is enough to show:

Claim: There are normal models \mathcal{C}' and \mathcal{C}'' of C over $\mathfrak{D}_{\tilde{v}}$ whose reductions $C'_{\tilde{v}}$ and $C''_{\tilde{v}}$ each have an irreducible component $C'_{\tilde{v},1}$ and $C''_{\tilde{v},1}$ with function field $\kappa(C'_{\tilde{v},1}) \simeq \kappa(C_0)$ and $\kappa(C''_{\tilde{v},1}) \simeq \kappa(E_d)$.

Indeed, if such a model \mathcal{C}' exists, then its desingularization and hence the minimal model \mathcal{C} have the same property (because $g(C_0) > 0$). But since all components of \mathcal{C} are smooth, there is a component C_1 of \mathcal{C} with $C_1 \simeq C_0$, and similarly, if such a model \mathcal{C}'' exists, then \mathcal{C} has a component $C_2 \simeq E_d$.

Proof of claim: a) The construction of \mathcal{C}' : Let $\tilde{\mathcal{C}}$ denote the normal model constructed in the proof of Theorem 5.14. Its fibre $\tilde{\mathcal{C}}_v$ at v is integral and has C_0 as its normalization (because $Y^4 = cX(X^2 - 1)(X - a)^5$ also has normalization C_0). Thus, if we let \mathcal{C}' denote (the normalization of) $\tilde{\mathcal{C}} \otimes \mathfrak{D}_{\tilde{v}}$, then its fibre $C'_{\tilde{v}}$ has normalization C_0 , as desired.

b) The construction of \mathcal{C}'' : Let $F_0 = \kappa(C \otimes K_0)$ denote the function field of $C \otimes K_0$; thus $F_0 = K_0(X, Y) = k(t, s, X, Y)$, where X and Y are related by equation (5) and t and s by equation (7). Put $x = (X - a)/s^4$ and $y = Y/s^5$. Then $F_0 = K_0(x, y)$ and equation (5) becomes

$$y^4 = x^3(x - B)^2 g_1(x),$$

where $B = (t - a)/s^4 = (t(t^2 - 1)g(t))^{-1} \in K = k(t)$ and $g_1(x) = cX(X^2 - 1) = c(s^4x + a)((s^4x + a)^2 - 1)$.

Let \mathfrak{A} denote the integral closure of $\mathfrak{B} = \mathfrak{D}_{\tilde{v}}[x]$ in F_0 , and let $\mathcal{C}'' = \text{Spec}(\mathfrak{A})$. Fix an irreducible component of the reduction of \mathcal{C}'' , and let V denote the associated (normalized) valuation of F_0 . We then have:

$$V(\sum a_i x^i) = e \min(\tilde{v}(a_i)), \quad \text{if } a_i \in K_0,$$

for some integer $e \geq 1$. Since by construction $\tilde{v}(s) = 1$, $\tilde{v}(t - a) = 4$ and $\tilde{v}(g(t)) = 0$, we see that $V(x - B) = V(g_1(x)) = 0$, and so also $V(y) = 0$. Thus, if \bar{x} and \bar{y} denote the images of x and y in the residue field $\kappa(V) = \mathfrak{D}_{\tilde{v}}/\mathfrak{M}_{\tilde{v}}$ of V , then the above relation specializes to

$$\bar{y}^4 = a_0 \bar{x}^3 (\bar{x} - b_0)^2,$$

where $a_0 = \overline{g_1(x)} = ca(a^2 - 1)$ and $b_0 = \bar{B} = (a(a^2 - 1)g(a))^{-1}$. Since this equation is irreducible over $k(\bar{x}) = \kappa(V|_{K_0(x)})$, we see that $[k(\bar{x}, \bar{y}) : k(\bar{x})] = 4$. Thus, since $[\kappa(V) : \kappa(V|_{K_0(x)})] \leq [F_0 : K_0(x)] = 4$, it follows that $\kappa(V) = k(\bar{x}, \bar{y})$. (It also follows that $e = 1$ and that V is the unique valuation above $V|_{K_0(x)}$, i.e. that the fibre of \mathcal{C}'' at \tilde{v} is integral, but we don't need this.)

It remains to show that $k(\bar{x}, \bar{y}) = \kappa(E_d)$. For this, put $u = \bar{y}^2/(\bar{x}(\bar{x} - b_0))$ and $v = a_0 \bar{y}/u$. Then by the above relation we have $u^2 = a_0 \bar{x}$, so $k(\bar{x}, \bar{y}) = k(u, v)$. Moreover, $v^2 = a_0 \bar{y}^2/\bar{x} = u(u^2 - a_0 b_0)$, so $\kappa(V) = \kappa(E_d)$, with $d = a_0 b_0 = c/g(a)$, as desired.

Remark 5.19 It follows from the above proof that reduction $C_{\tilde{v}}$ of the minimal model \mathcal{C} has the form $C_{\tilde{v}} = C_1 \cup \dots \cup C_r$, where $C_1 \simeq C_0$, $C_r \simeq E_d$, and $C_i \simeq \mathbb{P}^1$, for $2 \leq i \leq r - 1$, and each C_i meets C_{i-1} transversally in a unique point for $2 \leq i \leq r$.

Next we want to determine the abelian variety J_0 up to k -isogeny. To simplify matters, we shall assume in the following that $1 - a^2$ is a square in k or, equivalently, that $a = \frac{2b}{1+b^2}$ for some $b \in k$, where $b \neq 0, \pm 1$. (In fact, $b = (1 + \sqrt{(1 - a^2)})/a$.) In addition, we shall choose $c = (1 + b^2)$.

Lemma 5.20 *Let C_0 be the curve defined over k by the equation*

$$Y^4 = cX(X-1)(X+1)(X-a), \quad \text{where } a = \frac{2b}{1+b^2} \text{ and } c = 1+b^2,$$

for some $b \in k \setminus \{0, \pm 1\}$. Then its Jacobian J_0 is up to an isogeny of 2-power degree isomorphic to $E \times E_1 \times E_{b^2}$, where E is given by equation (6) and E_1 and E_{b^2} by equation (8) by putting $d = 1$ and $d = b^2$, respectively. In particular, if $b = b_1^2$ is a square in k , then J_0 is k -isogenous to $E \times E_1 \times E_1$.

Proof. Let $F = \kappa(C_0) = k(X, Y)$ denote the function field of C_0 . Then $F' := k(X, Y^2) = \kappa(E)$ is the function field of E . We shall show that there are two subfields $F_1 \simeq \kappa(E_1)$ and $F_2 \simeq \kappa(E_{b^2})$ of F which, for suitable $U, V \in F$, fit into the following field diagram of quadratic extensions:

$$\begin{array}{ccccc}
 & & F & & \\
 & / & | & \backslash & \\
 F_1 & & F_2 & & F' \\
 & \backslash & | & / & \backslash \\
 & & k(V) & & k(X) \\
 & & & \backslash & / \\
 & & & & k(U)
 \end{array}$$

From this the assertion follows because the fact that $F/k(V)$ is a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ -extension implies that $J_0 = J_F \sim J_{F'} \times J_{F_1} \times J_{F_2} = E \times E_1 \times E_{b^2}$ where the indicated isogeny has 2-power degree; cf. [KR].

To find these subfields, put $U = cX(X-a)/(X^2-1)$, so $[k(X) : k(U)] = 2$. Then

$$(U-1)(X^2-1) = cX(X-a) - (X^2-1) = (1-bX)^2$$

because $c-1 = b^2$ and $ca = 2b$ by hypothesis. Thus, if we put $Z_1 = Y(1-bX)/(X^2-1)$, then

$$Z_1^4 = U(U-1)^2,$$

and so, if we put $F_1 := k(U, Z_1)$, then $[F_1 : k(U)] = 4$ and $F_1(X) = F$. In particular, since $[F : k(X)] = 4$, we see that $F_1 \cap k(X) = k(U)$ and that $[F : F_1] = 2$.

Next, let $V = Z_1^2/(U - 1)$. Then by the above equation $V^2 = U$, so $Z_1^2 = V(U - 1) = V(V^2 - 1)$. From this we see that $k(V) = k(U, Z_1^2)$, so $[F_1 : k(V)] = 2$, and hence $F_1 = k(V, Z_1) \simeq \kappa(E_1)$. In addition, it follows that $k(V, X) = F'$ because F' is the unique proper intermediate field of $F/k(V)$. In addition, let us observe that

$$(U - b^2)(X^2 - 1) = cX(X - a) - b^2(X^2 - 1) = (X - b)^2,$$

because $(c - b^2) = 1$ and $ca = 2b$ by hypothesis. Therefore, if we put $X_1 = (X - b)/(1 - bX)$ and $Z_2 = Z_1 X_1$, then $X_1^2 = (U - b^2)/(U - 1)$ and $Z_2^2 = V(U - 1) \cdot (U - b^2)/(U - 1) = V(V^2 - b^2)$. From this we obtain for $F_2 := k(V, Z_2)$ that $[F_2 : k(V)] = 2$ and that $F_2 \simeq \kappa(E_{b^2})$. We therefore see that $F_1, F_2, F', k(V)$ and $k(U)$ fit into the above field diagram as indicated, and that $F_1 \simeq \kappa(E_1)$ and $F_2 \simeq \kappa(E_{b^2})$.

We can now determine the structure of the reduction $A_0 = A_{\bar{v}}$ of the abelian variety $A = J_C^{new}$ at \bar{v} .

Proposition 5.21 *Assume again that $a = \frac{2b}{1+b^2}$ and $c = 1 + b^2$ for some $b \in k^*$, and let $d = c/g(a)$. Then:*

(a) *There is a k -isogeny $\varphi : A_0 \rightarrow A'_0 := E_1 \times E_{b^2} \times E_d$ of 2-power degree, and hence A_0 is k' -isogenous to $E_1 \times E_1 \times E_1$, where $k' = k(\sqrt{b}, \sqrt[4]{d})$. Moreover, if $\sigma_0 \in \text{Aut}(A_0)$ denotes the automorphism induced by a generator $\sigma \in \text{Aut}(\pi)$ of the covering group, then we have $\varphi \circ \sigma_0 = \sigma'_0 \circ \varphi$ for some $\sigma'_0 \in \text{Aut}(A'_0)$.*

(b) *Let $\bar{S}_p \leq A_0[p]$ be an eigenspace of σ_0 , where $p \equiv 1 \pmod{4}$ is a prime. Then every cyclic \bar{k} -isogeny of A'_0 with kernel contained in $\varphi(\bar{S}_p)$ is an endomorphism of A'_0 . In particular, if $k' = k$, then every \bar{k} -isogeny of A_0 with kernel contained in \bar{S}_p is defined over k .*

Proof. (a) Since $A = J_C^{new}$ and $E = J_C^{old}$, we have an isogeny $\varphi_1 : E \times A \rightarrow J = J_C$ of 2-power degree (cf. Corollary 5.3) whose reduction $\bar{\varphi}_1 : E \times A_0 \rightarrow J_{\bar{v}}$ is a k -isogeny of the same degree. Moreover, by Proposition 5.18 we have an isomorphism $\varphi_2 : J_{\bar{v}} \xrightarrow{\sim} J_0 \times E_d$, and by Lemma 5.20 we have a k -isogeny $\varphi_3 : J_0 \rightarrow E \times E_1 \times E_{b^2}$ of 2-power degree. We thus see that $\tilde{\varphi} = (\varphi_3 \times id_{E_d}) \circ \varphi_2 \circ \bar{\varphi}_1 : E \times A_0 \rightarrow E \times E_1 \times E_{b^2} \times E_d = E \times A'_0$ is an isogeny of 2-power degree, and so the first assertion follows (by taking $\varphi = \tilde{\varphi}|_{\{0\} \times A_0}$) once we have shown that $\tilde{\varphi}(\{0\} \times A_0) = \{0\} \times A'_0$.

To prove this, it is enough to find automorphisms $\sigma_0 \in \text{Aut}(A_0)$ and $\sigma'_0 \in \text{Aut}(A'_0)$ with $\sigma_0^2 = [-1]_{A_0}$ and $(\sigma'_0)^2 = [-1]_{A'_0}$ such that

$$\tilde{\varphi} \circ (\tilde{\sigma}_0) = (\tilde{\sigma}'_0) \circ \tilde{\varphi},$$

where $\tilde{\sigma}_0 = [-1]_E \times \sigma_0$ and $\tilde{\sigma}'_0 = [-1]_E \times \sigma'_0$.

Indeed, since $1 + \sigma_0$ is an isogeny of A_0 (because $(1 + \sigma_0)(1 - \sigma_0) = 1 - [-1]_{A_0} = [2]_{A_0}$), we see that $(1 + ([-1]_E \times \sigma_0))(E \times A_0) = \{0\} \times A_0$, and similarly $(1 + \tilde{\sigma}'_0)(E \times A'_0) = \{0\} \times A'_0$, and hence $\tilde{\varphi}(\{0\} \times A_0) = \tilde{\varphi}((1 + \tilde{\sigma}_0)(E \times A_0)) = (1 + \tilde{\sigma}'_0)\tilde{\varphi}(E \times A_0) = (1 + \tilde{\sigma}'_0)(E \times A'_0) = \{0\} \times A'_0$, as desired.

To construct σ_0 and σ'_0 with these properties, let σ_J denote the automorphism (of order 4) on the Jacobian J induced by $\sigma \in \text{Aut}(\pi)$. Then σ_J maps the subvarieties E and A of J_C into themselves, and $(\sigma_J)|_E = [-1]_E$. Thus, if $\sigma_A = (\sigma_J)|_A$, then we have $\varphi_1 \circ ([-1] \times \sigma_A) = \sigma_J \circ \varphi_1$. Thus, if $\bar{\sigma}$ (resp. σ_0) denotes the automorphism induced by σ_J (resp. σ_A) on the reduction $J_{\bar{v}}$ (resp. on A_0), then we also have $\bar{\varphi}_1 \circ ([-1]_E \times \sigma_0) = \bar{\sigma} \circ \bar{\varphi}_1$.

Next we note that the proof of Proposition 5.18 shows that σ induces automorphisms σ_d and σ_{C_0} on E_d and on C_0 respectively, from which we see that $\varphi_2 \circ \bar{\sigma} = (\sigma_{J_0} \times \sigma_d) \circ \varphi_2$. Similarly, the proof of Lemma 5.20 shows that $\varphi_3 \circ \sigma_{J_0} = ([-1]_E \times \sigma_1 \times \sigma_{b^2}) \circ \varphi_3$, for certain automorphisms $\sigma_i \in \text{Aut}(E_i)$ where $i = 1, b^2$. We thus see that if we put $\sigma'_0 = \sigma_1 \times \sigma_{b^2} \times \sigma_d \in \text{Aut}(A'_0)$, then the above commutation relation holds.

It remains to show that $\sigma_0^2 = [-1]_{A_0}$ and that $(\sigma'_0)^2 = [-1]_{A'_0}$. The latter is clear, for by construction $\sigma'_0 = \sigma_1 \times \sigma_{b^2} \times \sigma_d$, where (for $i = 1, b^2, d$) the automorphism $\sigma_i \in \text{Aut}(E_i)$ has order 4 and so $\sigma_i^2 = [-1]_{E_i}$ because $\text{char}(k) \neq 2, 3$. To prove the former, recall that $A = \tilde{\varepsilon}_{\text{new}} J$, where $\tilde{\varepsilon}_{\text{new}} = 1 - \sigma_J^2$, so σ_J^2 acts on A like $[-1]_A$. Thus, $\sigma_A^2 = [-1]_A$ and hence by functoriality we have $\sigma_0^2 = [-1]_{A_0}$, as desired.

(b) Write $E_2 = E_{b^2}$ and $E_3 = E_d$, so $A'_0 = E_1 \times E_2 \times E_3$. Let $\bar{S}'_p = \varphi(\bar{S}_p) \leq A'_0[p]$, which is an eigenspace under the action of $\sigma'_0 = \sigma_1 \times \sigma_2 \times \sigma_3$.

Since $\sqrt[4]{-1} \in k$ and $j(E_i) = 1728$, we have for $i = 1, 2, 3$ that $\text{End}(E_i) \supset \mathbb{Z}[\sqrt[4]{-1}]$, and equality holds unless E_i is supersingular (i.e. unless $\text{char}(k) \equiv 3 \pmod{4}$). Thus, since $p \equiv 1 \pmod{4}$, there is an $\alpha_i \in \text{End}(E_i)$ of degree p such that $\text{Ker}(\alpha_i) = \bar{S}'_p \cap e_i(E_i)$, where $e_i : E_i \rightarrow A'_0$ is the embedding of E_i as the i -th factor of A'_0 . Thus, $\bar{S}'_p = \text{Ker}(\alpha_1) \times \text{Ker}(\alpha_2) \times \text{Ker}(\alpha_3)$.

Now since E_2 and E_3 are twists of E_1 , there are k' -isomorphisms $f_{1i} : E_1 \rightarrow E_i$, for $i = 2, 3$, which we can choose such that $f_{1i} \circ \alpha_1 = \alpha_i \circ f_{1i}$. Thus, if $\tilde{P}_1 \in E_1(\bar{k})$ is a generator of $\text{Ker}(\alpha_1)$, and $\tilde{P}_i = f_{1i}(P_1)$ then $\{P_1, P_2, P_3\}$ is a basis of \bar{S}'_p , where $P_i := e_i(\tilde{P}_i)$.

Now let h be a cyclic \bar{k} -isogeny of A'_0 with $\text{Ker}(h) \leq \bar{S}'_p$. Then $\text{Ker}(h)$ is generated by $P = aP_1 + bP_2 + cP_3$, for some $a, b, c \in \mathbb{F}_p$. W.l.o.g. we may assume that $a \neq 0$ (otherwise we interchange the roles of E_1, E_2 and E_3), and hence that $a = 1$. Then the k' -endomorphism $h' : A'_0 \rightarrow A'_0$, defined by the

matrix $\begin{pmatrix} (1-b)\alpha_1 & \alpha_1 f_{12}^{-1} & 0 \\ -bf_{12} & id_{E_2} & 0 \\ -cf_{13} & 0 & id_{E_3} \end{pmatrix}$ has kernel $\text{Ker}(h') = \langle P_1 + bP_2 + cP_3 \rangle =$

$\text{Ker}(h)$, which proves the first assertion.

From this the second assertion is immediate. Indeed, if $k' = k$, then by what was just shown, every \bar{k} -subgroup of \bar{S}'_p is k -rational, and hence the same is true for \bar{S}_p .

We can now summarize the results obtained above in the following theorem.

Theorem 5.22 *Suppose k contains a primitive fourth root of unity, and let $a = \frac{2b^2}{1+b^4}$, for some $b \in k^*$ with $b^4 \neq 1$. Let $K = k(t, s)$ be the function field of any curve of the form*

$$s^4 = t(t^2 - 1)(t - a)g(t),$$

where $g(t) \in k[t]$ is any polynomial which does not vanish at $\{0, 1, -1, a\}$, and which has been normalized in such a way that $(1 + b^4)/g(a)$ is a fourth power in k . Moreover, let \mathfrak{p} be the unique place of K/k inducing the specialization $t \mapsto a$. Then the k -rational geometric fundamental group of K with base point \mathfrak{p} is infinite; more precisely, for every prime $p \equiv 5 \pmod{12}$ (with $p \neq \text{char}(k)$), there is an unramified extension K_p/K with $\text{Gal}(K_p/K) \simeq \text{PSL}_3(p)$ in which \mathfrak{p} splits completely.

Proof. It is clearly enough to prove the last statement. For this, let C be the curve defined over $k(t)$ by the equation $Y^2 = (1 + b^4)X(X^2 - 1)(X - a)^3(X - t)^2$, and let J denote its Jacobian and $A = J^{\text{new}}$ its new part (cf. section 5.1). Since the hypotheses on $a, c = 1 + b^2$ and g ensure that $k' := k(\sqrt{b^2}, \sqrt[4]{c/g(a)}) = k$, it follows from Proposition 5.21a) that the reduction A_0 of $A \otimes K$ at \mathfrak{p} is k -isogenous to $E_1 \times E_1 \times E_1$.

Now let $p \equiv 5 \pmod{12}$ be any prime (and $\neq \text{char}(k)$), and let $S_p \leq A[p]$ denote an eigenspace of the automorphism σ_A (cf. proof of Proposition 5.21). By Theorem 5.5(b),(d) (and Abhyankar's Lemma) we know that $K_p := K(\mathbb{P}(S_p))$ is unramified over K and that $\text{Gal}(K_p/K) = \text{PSL}_3(p)$. Let \bar{S}_p denote the image of S_p in $A_0[p]$ under the reduction map at \mathfrak{p} ; clearly, \bar{S}_p is identical to

the set \bar{S}_p as defined in Proposition 5.21(b). Thus, by that proposition, condition $(\star\star)$ of Corollary 5.16 holds, and so it follows that \mathfrak{p} splits completely in K_p .

Remark 5.23 The simplest examples of fields K satisfying the hypothesis of Theorem 5.22 are clearly the fields $K = k(s, t)$, where

$$s^4 = (1 + b^4)t(t^2 - 1) \left(t - \frac{2b^2}{1+b^4} \right)$$

and $b \in k^*$ is any element with $b^4 \neq 1$; recall that fields of this type were studied in Lemma 5.20. Clearly, all these fields have genus 3. More generally, by choosing $g(t)$ suitably, we can obtain examples of fields of any genus $g \geq 3$ which satisfy the hypotheses of Theorem 5.22.

References

- [BLR] S. BOSCH, W. LÜTKEBOHMERT AND M. RAYNAUD, *Néron Models*. Springer-Verlag, Berlin, 1990.
- [FKV] G. FREY, E. KANI AND H. VÖLKLEIN, Curves of genus 2 with elliptic differentials and associated Hurwitz spaces. In preparation.
- [FV] M. FRIED AND H. VÖLKLEIN, The inverse Galois problem and rational points on moduli spaces. *Math. Annalen* **290** (1991), 771-800.
- [GS] A. GARCIA AND H. STICHTENOTH, On the asymptotic behaviour of some towers of function fields over finite fields. To appear in *J. Number Theory*.
- [Gro] A. GROTHENDIECK, *Modeles de Néron et monodromie*. SGA 7_I, Exp. IX. Springer Lecture Notes **288** (1972), 313-523.
- [Ig] J.-I. IGUSA, On the algebraic theory of elliptic modular functions. *J. Math. Soc. Japan* **20** (1968), 96-106.
- [Ih] Y. IHARA, On unramified extensions of function fields over finite fields. *Adv. Stud. in Pure Math.* **2** (1983), 83-97.
- [KR] E. KANI AND M. ROSEN, Idempotent relations and factors of Jacobians. *Math. Ann.* **284** (1989), 307-327.

- [MSV] K. MAGAARD, K. STRAMBACH AND H. VÖLKLEIN, Finite quotients of the pure symplectic braid group, to appear in Israel J. Math.
- [Me] L. MEREL, Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae* **124** (1996), 434–449.
- [Mi] MIYAKE, *Modular Forms*. Springer Verlag, Berlin, 1989.
- [Mo] S. MOCHIZUKI, The Local pro- p Grothendieck Conjecture for Hyperbolic Curves. RIMS Kyoto University, Preprint 1045 (1996).
- [Se] J.-P. SERRE, *Groupes algébriques et corps de classes*. Hermann, Paris, 1959.
- [Se1] J.-P. SERRE, Sur le nombre des points d’une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris* **296** (1983), série I, 397–402.
- [Se2] J.-P. SERRE, *Local Fields*. Springer Verlag, New York, 1979.
- [ST] J.-P. SERRE AND J. TATE, Good reduction of abelian varieties. *Ann. of Math.* **88** (1968), 492–517.
- [V] H. VÖLKLEIN, *Groups as Galois Groups – an Introduction*, *Cambr. Studies in Adv. Math.* **53**, Cambridge Univ. Press 1996.
- [V1] H. VÖLKLEIN, Rigid generators of classical groups, *Math. Annalen* **311** (1998), 421–438.
- [V2] H. VÖLKLEIN, Moduli spaces for covers of the Riemann sphere, *Israel J. Math.* **85** (1994), 407–430.
- [V3] H. VÖLKLEIN, Cyclic covers of P^1 , and Galois action on their division points, *Contemp. Math.* **186** (1995), 91–107.
- [V4] H. VÖLKLEIN, Braid group action through $GL_n(q)$ and $U_n(q)$, and Galois realizations, *Israel J. Math.* **82** (1993), 405–427.
- [V5] H. VÖLKLEIN, Braid group action, embedding problems and the groups $PGL(n, q)$, $PU(n, q^2)$, *Forum Math.* **6** (1994), 513–535.