ISRAEL JOURNAL OF MATHEMATICS **TBD** (XXXX), 1–17
DOI: 10.1007/s00000000000000000000000

UNRAMIFIED HEISENBERG GROUP EXTENSIONS OF NUMBER FIELDS

BY

Frauke M. Bleher*

Department of Mathematics, University of Iowa
14 MacLean Hall, Iowa City, IA 52242-1419, USA
e-mail: frauke-bleher@uiowa.edu

AND

Ted Chinburg**

Department of Mathematics, University of Pennsylvania
Philadelphia, PA 19104-6395, USA
e-mail: ted@math.upenn.edu

AND

Jean Gillibert

Institut de Mathématiques de Toulouse, CNRS UMR 5219
118 route de Narbonne, 31062 Toulouse Cedex, France
e-mail: Jean.Gillibert@math.univ-toulouse.fr

ABSTRACT

We construct étale generalized Heisenberg group covers of hyperelliptic curves over number fields. We use these to produce infinite families of quadratic extensions of cyclotomic fields that admit everywhere unramified generalized Heisenberg Galois extensions.

* The first author was supported in part by NSF Grant No. DMS-1801328.
** The second author is the corresponding author. He was supported in part by NSF FRG Grant No. DMS-1360767, NSF SaTC grants No. CNS-1513671 and No. CNS-1701785.

Received April 4, 2020 and in revised form February 12, 2021

1. Introduction

Let G be a finite group and suppose K is a number field. In this paper we consider the problem of constructing infinitely many unramified Galois G-extensions M/L of number fields for which L has bounded degree over K. When one imposes no conditions on the ramification of M/L, a classical technique is to specialize a G-cover $\pi : C' \longrightarrow C$ of curves over K for which C has many points over such L. To construct M/L that are unramified, a first step is to ensure that π itself is unramified. One can then find a model of π over a ring of S-integers of K that is unramified, and control the ramification of M/L over places in S by imposing conditions on how one specializes π. This approach was used in [1] by Bilu and the third author (see also [7]) to construct abelian unramified extensions of quadratic extensions of a given number field, using abelian covers π of a hyperelliptic curve C.

In this paper we consider nilpotent groups G. The essential obstruction to the above technique is the construction of an unramified G-cover $\pi : C' \longrightarrow C$ over K. When G is abelian, one constructs such π by imposing conditions on the K-rational torsion points of the Jacobian of C. For more general nilpotent covers, there is a technique which combines abelian information with data on cup products and higher Massey products of characters of Galois groups; see [10, 11] and their references, for example. However, the calculation of cup products is more difficult when K is not algebraically closed. This is due to the fact that $H^2(C, \mu_n)$ contains a subgroup isomorphic to

$$\mathrm{Pic}^0(C)/n\mathrm{Pic}^0(C)$$

when μ_n is the étale sheaf of n-th roots of unity, and this subgroup is in general non-trivial.

The main innovation in this paper is to exploit the action of $\mathrm{Aut}_K(C)$ on cup products in order to construct unramified nilpotent covers $\pi : C' \longrightarrow C$. We will illustrate this by taking G to be a (generalized) Heisenberg group of the form $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$; see Section 2 for a definition of this group. It is non-abelian and nilpotent of order n^{2d+1} and it is contained in the subgroup of unipotent upper-triangular matrices in $\mathrm{GL}_{d+2}(\mathbb{Z}/n\mathbb{Z})$. For example, we will produce by the above methods some infinite families of everywhere unramified $\mathcal{H}_3(\mathbb{Z}/n\mathbb{Z})$-extensions M/L with L a quadratic extension of $\mathbb{Q}(\zeta_n)$ (cf. Theorem 1.1). This method differs from other approaches based on group theory, Hurwitz spaces

and the Inverse Galois problem which we will describe in Remark 3.4. Previous work by Völklein and others (see [12] and [13]) leads to alternate proofs of some of the results in this paper, sometimes with stronger hypotheses, e.g., that n is prime.

Let C be a smooth projective hyperelliptic curve over a number field K. Our first result, Theorem 3.1, shows that the existence of an étale $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$-cover of C is equivalent to the existence of two families (each one having d elements) of n-torsion line bundles on C, which are globally orthogonal under the Weil pairing. We state Theorem 3.1 in the setting of twisted Heisenberg group schemes, in which $\mathbb{Z}/n\mathbb{Z}$ is replaced by μ_n; this allows us to work over smaller fields in the absence of roots of unity. As an illustration of Theorem 3.1, we give at the end of Section 3 several explicit examples of Heisenberg Galois covers of hyperelliptic curves. In this case, the strategy of applying elements of $\mathrm{Aut}_K(C)$ to control cup products amounts to using the hyperelliptic involution of C to show that the relevant cup product over K is trivial provided its base change to $\overline{K}$ is trivial.

We will apply the specialization results of [1] to the examples of covers constructed in Section 3. Suppose one is given a connected étale cover $\pi : C' \longrightarrow C$ over a number field K in which some K-rational point P_0 splits completely. In [1], it was shown that one can find infinitely many (in a strong quantitative sense) points in $C(\overline{K})$ such that the extension of number fields that results on specializing π over these points has the same degree as π and is everywhere unramified. This leads to the following result.

THEOREM 1.1: *Let $n > 1$ be an odd integer, and let ζ_n be a primitive n-th root of unity. Then there exist infinitely many quadratic extensions $L/\mathbb{Q}(\zeta_n)$ which admit a Galois extension with group $\mathcal{H}_3(\mathbb{Z}/n\mathbb{Z})$, unramified at all finite places of L. Moreover, given a finite set S of places of $\mathbb{Q}(\zeta_n)$, which may contain finite and infinite places, there exist infinitely many such L for which primes lying above S in L are totally split in the corresponding Galois extension.*

Furthermore, there is a constant $c > 0$, which depends only on n and S, for which the following is true. For sufficiently large positive N, the number of (isomorphism classes of) such fields L whose relative discriminant $\Delta(L/\mathbb{Q}(\zeta_n))$ satisfies

$$|\mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\Delta(L/\mathbb{Q}(\zeta_n))|^{1/\varphi(n)} \leq N$$

is at least $cN^{\varphi(n)/(4n-2)}/\log N$, where φ is Euler's function.

Two potential generalizations of our results are (i) to replace hyperelliptic curves by more general ones, and (ii) to replace Heisenberg groups by more general nilpotent groups. These generalizations are connected because to treat nilpotent groups with higher nilpotency, one must consider higher Massey products. To control such products with automorphisms of the base curve will require using more than hyperelliptic involutions.

Acknowledgements. The first and second authors would like to thank the University of Toulouse for its support and hospitality during work on this paper. The authors would also like to thank the referee for many helpful suggestions.

2. Heisenberg groups

In this section, we fix two integers $n > 1$ and $d \geq 1$. The Heisenberg group of rank $2d+1$ with coefficients in $\mathbb{Z}/n\mathbb{Z}$, denoted by $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$, is the subgroup of $\mathrm{GL}_{d+2}(\mathbb{Z}/n\mathbb{Z})$ consisting of matrices of the form

$$\begin{pmatrix} 1 & \mathbf{a} & c \\ 0 & I_d & \mathbf{b} \\ 0 & 0 & 1 \end{pmatrix}$$

where I_d is the $d \times d$ identity matrix, $\mathbf{a}$ (resp. $\mathbf{b}$) is a row (resp. column) vector of length d with coefficients in $\mathbb{Z}/n\mathbb{Z}$, and c belongs to $\mathbb{Z}/n\mathbb{Z}$. The center of this group is the set of matrices satisfying $\mathbf{a} = 0$ and $\mathbf{b} = 0$, which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. It follows that we have an exact sequence of groups

$$0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{2d} \longrightarrow 0. \tag{2.1}$$

Thus $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$ is a central extension of $(\mathbb{Z}/n\mathbb{Z})^{2d}$ by $\mathbb{Z}/n\mathbb{Z}$.

The twisted Heisenberg group scheme of rank $2d+1$ over $\mathbb{Z}[\frac{1}{n}]$, denoted by $\mathcal{H}_{2d+1}(\mu_n)$, is defined in the same way as the Heisenberg group $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$, but the vectors $\mathbf{a}$ and $\mathbf{b}$ in the matrix have coefficients in μ_n, and c belongs to $\mu_n^{\otimes 2}$. We have as previously an exact sequence

$$0 \longrightarrow \mu_n^{\otimes 2} \longrightarrow \mathcal{H}_{2d+1}(\mu_n) \longrightarrow (\mu_n)^{2d} \longrightarrow 0 \tag{2.2}$$

which is in fact an exact sequence of presheaves.

We note that $\mathcal{H}_{2d+1}(\mu_n)$ is a finite étale $\mathbb{Z}[\frac{1}{n}]$-group scheme. We underline the fact that $\mu_n^{\otimes 2}$ is not representable by a finite flat group scheme over $\mathbb{Z}$, so $\mathcal{H}_{2d+1}(\mu_n)$ does not extend to a finite flat group scheme over $\mathbb{Z}$. Nevertheless,

if ζ_n denotes a primitive n-th root of unity, then we have a non-canonical isomorphism between $\mathcal{H}_{2d+1}(\mu_n)$ and $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$ over $\mathbb{Z}[\frac{1}{n}, \zeta_n]$. Hence $\mathcal{H}_{2d+1}(\mu_n)$ extends to a constant group scheme over $\mathbb{Z}[\zeta_n]$.

Unless otherwise specified, all torsors we consider are relative to the étale topology. Thus, if Γ is an étale group scheme over a scheme X, we denote by $H^1(X, \Gamma)$ the pointed set of isomorphism classes of Γ-torsors over X for the étale topology. When Γ is abelian, this set is an abelian group.

If $\phi : \Gamma \longrightarrow \Lambda$ is a morphism of X-group schemes, and if ξ is a Γ-torsor over X, then the image of ξ by the natural map $\phi_* : H^1(X, \Gamma) \longrightarrow H^1(X, \Lambda)$ is a Λ-torsor. We say, by abuse of notation, that this is the Λ-torsor associated to ξ, the morphism ϕ being omitted.

Let us recall a result of Sharifi [10] which allows one to produce torsors for $\mathcal{H}_{2d+1}(\mu_n)$ whose associated $(\mu_n)^{2d}$-torsor is given.

THEOREM 2.1: *Let X be a connected $\mathbb{Z}[\frac{1}{n}]$-scheme. Suppose we are given two d-tuples $\chi_1, \ldots, \chi_d$ and $\chi'_1, \ldots, \chi'_d$ in $H^1(X, \mu_n)$ for some integer $d \geq 1$. Then there exists a $\mathcal{H}_{2d+1}(\mu_n)$-torsor ξ over X whose associated $(\mu_n)^{2d}$-torsor is the $2d$-tuple $(\chi_1, \ldots, \chi_d, \chi'_1, \ldots, \chi'_d)$ if and only if*

$$\sum_{i=1}^{d} [\chi_i \cup \chi'_i] = 0$$

where the sum is computed in the group $H^2(X, \mu_n^{\otimes 2})$. Moreover, ξ is connected if and only if the subgroup of $H^1(X, \mu_n)$ generated by $\chi_1, \ldots, \chi_d, \chi'_1, \ldots, \chi'_d$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2d}$.

Proof. See [10, Proposition 2.3]. We note that Sharifi's result is stated in terms of (twisted) Galois representations over a field K of characteristic prime to n, instead of torsors over a $\mathbb{Z}[\frac{1}{n}]$-scheme X. Nevertheless, his results immediately extend to our setting by considering representations of the étale fundamental group of X. ∎

Remark 2.2: If p and q are relatively prime integers, it follows from the Chinese remainder theorem that

$$\mathcal{H}_{2d+1}(\mathbb{Z}/pq\mathbb{Z}) \simeq \mathcal{H}_{2d+1}(\mathbb{Z}/p\mathbb{Z}) \times \mathcal{H}_{2d+1}(\mathbb{Z}/q\mathbb{Z}),$$

and similarly for twisted Heisenberg group schemes. Thus, we could assume that n is the power of some prime number. However, we prefer for simplicity to work with arbitrary n.

3. Geometric Heisenberg group extensions

Let K be a field, and let $\overline{K}$ be an algebraic closure of K. In our terminology, a hyperelliptic curve over K is a smooth projective geometrically connected K-curve of genus $g \geq 1$, endowed with a degree 2 map $\pi : C \longrightarrow \mathbb{P}^1_K$. This includes elliptic curves over K. In this setting, the Weierstrass points of C are none other than the ramification points of π. We denote by τ the hyperelliptic involution of C. The group $G = \{e, \tau\}$ acts on C, and the quotient morphism is the map $\pi : C \longrightarrow \mathbb{P}^1_K$.

If ξ is a Γ-torsor over C, and if $P_0 \in C(K)$ is a K-rational point of C, we say that ξ splits over P_0 if $P_0^* \xi$ is the trivial Γ-torsor over K.

THEOREM 3.1: *Let $n > 1$ be an odd integer with $\mathrm{char}(K) \nmid n$, and such that $[K(\mu_n) : K]$ is prime to n. Let C be a hyperelliptic curve over K, together with a K-rational Weierstrass point $P_0 \in C(K)$. Let $L_1, \ldots, L_d$ and $L'_1, \ldots, L'_d$ in $\mathrm{Pic}^0(C)[n]$ be such that*

$$\prod_{i=1}^{d} e_n(L_i, L'_i) = 1$$

where e_n denotes the Weil pairing. Then:

1. *For $i = 1, \ldots, d$, there exists a unique étale μ_n-torsor χ_i (resp. χ'_i) over C which splits over P_0, and whose associated $\mathbb{G}_m$-torsor is L_i (resp. L'_i).*
2. *There exists an étale $\mathcal{H}_{2d+1}(\mu_n)$-torsor ξ which splits over the point P_0, and whose associated $(\mu_n)^{2d}$-torsor is the $2d$-tuple*

$$(\chi_1, \ldots, \chi_d, \chi'_1, \ldots, \chi'_d).$$

3. *The torsor ξ is geometrically connected if and only if the subgroup generated by the L_i and the L'_i is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2d}$.*

Remark 3.2: The Weil pairing is a non-degenerate bilinear pairing of finite K-group schemes

$$e_n : J_C[n] \times J_C[n] \longrightarrow \mu_n$$

where J_C denotes the Jacobian of C. In particular, if L and L' belong to

$$\mathrm{Pic}^0(C)[n] = J_C[n](K),$$

then $e_n(L, L')$ belongs to $\mu_n(K)$.

Remark 3.3: In Theorem 3.1 (2), the $\mathcal{H}_{2d+1}(\mu_n)$-torsor ξ is unique up to a twist by a $\mu_n^{\otimes 2}$-torsor over C, which splits over P_0. This can be checked by going through the proof of Lemma 3.7 below.

Remark 3.4: The proof we will give of Theorem 3.1 uses the hyperelliptic involution of C to control cup products. We thank the referee for outlining a different approach which uses group theory, Hurwitz spaces and work on the Inverse Galois problem under some additional hypotheses. For simplicity, assume $K(\mu_n) = K$, so that μ_n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and $\mathcal{H}_{2d+1}(\mu_n)$ is isomorphic to the constant group $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$. Theorem 3.1 follows if one can construct a regular cover of $\mathbb{P}^1_K$ with group

$$\Gamma = \mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$$

having C as the quotient by $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$ and having inertia groups that are involutions mapping to the hyperelliptic involution of C. Such a Γ-cover is a central $\mathbb{Z}/n\mathbb{Z}$-extension of a cover with group $G = (\mathbb{Z}/n\mathbb{Z})^{2d} \rtimes \mathbb{Z}/2\mathbb{Z}$. When n is prime, [13, Theorem 9.17.(1)] describes a method of constructing G-covers of $\mathbb{P}^1_K$ of the required kind when C is allowed to vary using Hurwitz spaces. One can then apply results from [12] to show that the constrained central embedding problem associated to constructing an appropriate Γ-cover has a solution under appropriate hypotheses.

To prove Theorem 3.1 we need the following results.

LEMMA 3.5: *For all integers $j \geq 0$ there is a canonical isomorphism*

$$H^j(\mathbb{P}^1_K, \mu_n) = H^j(C, \mu_n)^G.$$

Proof. This is clear from the spectral sequence

$$H^p(G, H^q(C, \mu_n)) \Rightarrow H^{p+q}(\mathbb{P}^1_K, \mu_n)$$

together with the fact that G has order 2 and all of the groups $H^q(C, \mu_n)$ are annihilated by multiplication by the odd integer n. ∎

LEMMA 3.6: *There are canonical isomorphisms*

$$H^1(\mathbb{P}^1_K, \mu_n) = K^*/(K^*)^n \quad \text{and} \quad H^1(\mathbb{P}^1_K, \mathbb{G}_m) = \mathrm{Pic}(\mathbb{P}^1_K) = \mathbb{Z} \tag{3.1}$$

and an isomorphism of Brauer groups

$$H^2(\mathbb{P}^1_K, \mathbb{G}_m) = \mathrm{Br}(\mathbb{P}^1_K) = \mathrm{Br}(K) \tag{3.2}$$

induced by pulling back Azumaya algebras from K to $\mathbb{P}^1_K$. There is an exact sequence

$$0 \longrightarrow \mathrm{Pic}(\mathbb{P}^1_K)/n \longrightarrow H^2(\mathbb{P}^1_K, \mu_n) \longrightarrow H^2(\mathbb{P}^1_K, \mathbb{G}_m)[n] \longrightarrow 0. \tag{3.3}$$

Using the above isomorphisms, the sequence (3.3) becomes

$$0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow H^2(\mathbb{P}^1_K, \mu_n) \longrightarrow \mathrm{Br}(K)[n] \longrightarrow 0. \tag{3.4}$$

Moreover, any class in $H^2(\mathbb{P}^1_K, \mu_n)$ that splits over some K-rational point of $\mathbb{P}^1_K$ belongs to the kernel of the homomorphism $H^2(\mathbb{P}^1_K, \mu_n) \longrightarrow \mathrm{Br}(K)[n]$.

Proof. One has $H^1(\mathbb{P}^1_K, \mathbb{G}_m) = \mathrm{Pic}(\mathbb{P}^1_K) = \mathbb{Z}$ via the degree map. The cohomology of the Kummer sequence

$$1 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{[n]} \mathbb{G}_m \longrightarrow 1$$

then gives (3.1) and (3.3). To analyze $H^2(\mathbb{P}^1_K, \mathbb{G}_m)$ we use the Hochschild–Serre spectral sequence

$$H^p(K, H^q(\mathbb{P}^1_{\overline{K}}, \mathbb{G}_m)) \Rightarrow H^{p+q}(\mathbb{P}^1_K, \mathbb{G}_m). \tag{3.5}$$

By Tsen's theorem, $H^2(\mathbb{P}^1_{\overline{K}}, \mathbb{G}_m) = 0$. The action of the profinite group $\mathrm{Gal}(\overline{K}/K)$ on $H^1(\mathbb{P}^1_{\overline{K}}, \mathbb{G}_m) = \mathrm{Pic}(\mathbb{P}^1_{\overline{K}}) = \mathbb{Z}$ is trivial, so

$$H^1(K, H^1(\mathbb{P}^1_{\overline{K}}, \mathbb{G}_m)) = 0.$$

We have

$$H^2(K, H^0(\mathbb{P}^1_{\overline{K}}, \mathbb{G}_m)) = H^2(K, \overline{K}^*) = \mathrm{Br}(K).$$

Finally, the restriction map

$$H^1(\mathbb{P}^1_K, \mathbb{G}_m) \longrightarrow H^1(\mathbb{P}^1_{\overline{K}}, \mathbb{G}_m)$$

is an isomorphism. Putting these facts into the spectral sequence (3.5) gives (3.2). The last statement follows from the fact that the pullback from K to $\mathbb{P}^1_K$ induces a section of the surjection $H^2(\mathbb{P}^1_K, \mu_n) \longrightarrow \mathrm{Br}(K)[n]$. ∎

The final lemma we will need to prove Theorem 3.1 has to do with twisting Heisenberg torsors in order to ensure that they split over a particular point.

LEMMA 3.7: *Let ξ be a $\mathcal{H}_{2d+1}(\mu_n)$-torsor over C, whose associated $(\mu_n)^{2d}$-torsor splits over P_0. Then there exists a $\mathcal{H}_{2d+1}(\mu_n)$-torsor ξ' over C with the same associated $(\mu_n)^{2d}$-torsor such that ξ' splits over P_0 and ξ' is isomorphic to ξ over $\overline{K}$.*

Proof. Consider the following commutative diagram of pointed sets with exact rows [4, Chap. III, Proposition 3.3.1]:

$$\begin{array}{ccccccc} 1 & \longrightarrow & H^1(C,\mu_n^{\otimes 2}) & \longrightarrow & H^1(C,\mathcal{H}_{2d+1}(\mu_n)) & \xrightarrow{a} & H^1(C,(\mu_n)^{2d}) \\ & & \downarrow{\scriptstyle P_0^*} & & \downarrow{\scriptstyle P_0^*} & & \downarrow{\scriptstyle P_0^*} \\ 1 & \longrightarrow & H^1(K,\mu_n^{\otimes 2}) & \longrightarrow & H^1(K,\mathcal{H}_{2d+1}(\mu_n)) & \xrightarrow{a_K} & H^1(K,(\mu_n)^{2d}) \end{array}$$

in which the vertical maps are the restrictions to P_0. By definition of an exact sequence of pointed sets, the kernel of a is exactly the image of the map $H^1(C,\mu_n^{\otimes 2}) \longrightarrow H^1(C,\mathcal{H}_{2d+1}(\mu_n))$, and similarly for a_K.

By assumption, $a(\xi)$ belongs to the kernel of P_0^*, and hence $P_0^*\xi$ belongs to the kernel of a_K by commutativity. It follows that $P_0^*\xi$ comes from a $\mu_n^{\otimes 2}$-torsor over K, which we denote by c_0. Let us denote by $f : C \longrightarrow \mathrm{Spec}(K)$ the structural morphism. Since the group $\mu_n^{\otimes 2}$ is central in $\mathcal{H}_{2d+1}(\mu_n)$, it follows from [4, Chap. III, Remarque 3.4.4] that the contracted product

$$\xi' := \xi \times_C^{\mu_n^{\otimes 2}} f^*c_0$$

is a $\mathcal{H}_{2d+1}(\mu_n)$-torsor over C, which splits over P_0 because

$$P_0^* f^* c_0 = c_0.$$

Finally, ξ and ξ' are isomorphic over $\overline{K}$, because c_0 is just a Galois cohomology class over K, hence splits over $\overline{K}$. ∎

Proof of Theorem 3.1. Since the curve C is geometrically connected, we have

$$\mathbb{G}_m(C) = \mathbb{G}_m(K) = K^*.$$

Hence the Kummer exact sequence on C gives

$$0 \longrightarrow K^*/(K^*)^n \longrightarrow H^1(C,\mu_n) \longrightarrow \mathrm{Pic}(C)[n] \longrightarrow 0.$$

Moreover, the map

$$P_0^* : H^1(C,\mu_n) \longrightarrow H^1(K,\mu_n) \simeq K^*/(K^*)^n$$

is a retraction of the natural map $K^*/(K^*)^n \longrightarrow H^1(C,\mu_n)$. One deduces that, given $L \in \mathrm{Pic}(C)[n]$, there exists a unique μ_n-torsor χ on C which splits over the point P_0, and whose associated $\mathbb{G}_m$-torsor is L. This proves part (1).

For part (2), let us first prove that $\tau(\chi_i) = -\chi_i$ for all i. We have a sequence of canonical isomorphisms

$$H^1(K, \mu_n) \simeq H^1(\mathbb{P}^1_K, \mu_n) \simeq H^1(C, \mu_n)^G$$

and the map $P_0^* : H^1(C, \mu_n)^G \longrightarrow H^1(K, \mu_n)$ is the inverse isomorphism. Now, the μ_n-torsor $\chi_i + \tau(\chi_i)$ is invariant under the action of G, and P_0 (which is a ramification point of $C \longrightarrow \mathbb{P}^1_K$) is invariant by τ, from which it follows that

$$P_0^*(\chi_i + \tau(\chi_i)) = 2P_0^*\chi_i = 0.$$

The map P_0^* being an isomorphism, this proves that $\chi_i + \tau(\chi_i) = 0$. It follows that we have, for $i = 1, \dots, d$,

$$\tau(\chi_i \cup \chi_i') = \tau(\chi_i) \cup \tau(\chi_i') = (-\chi_i) \cup (-\chi_i') = \chi_i \cup \chi_i'.$$

Thus $\chi_i \cup \chi_i' \in H^2(C, \mu_n^{\otimes 2})^G$.

The map

$$H^2(C, \mu_n^{\otimes 2}) \longrightarrow H^2(C \otimes_K K(\mu_n), \mu_n^{\otimes 2})$$

is injective, because $[K(\mu_n) : K]$ is prime to n. Hence, in order to prove that $\sum_{i=1}^d [\chi_i \cup \chi_i'] = 0$, we may (and we do) assume that K contains a primitive n-th root of unity. Then for any K-scheme X and for all j we have natural isomorphisms

$$H^j(X, \mu_n^{\otimes 2}) \simeq H^j(X, \mu_n) \otimes \mu_n.$$

By Lemma 3.6, we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (\mathrm{Pic}(\mathbb{P}^1_K)/n) \otimes \mu_n & \longrightarrow & H^2(\mathbb{P}^1_K, \mu_n^{\otimes 2}) & \longrightarrow & \mathrm{Br}(K)[n] \otimes \mu_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\mathrm{Pic}(C)/n) \otimes \mu_n & \longrightarrow & H^2(C, \mu_n^{\otimes 2}) & \longrightarrow & \mathrm{Br}(C)[n] \otimes \mu_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & (\mathrm{Pic}(C \otimes_K \overline{K})/n) \otimes \mu_n & \xrightarrow{\sim} & H^2(C \otimes_K \overline{K}, \mu_n^{\otimes 2}) & & & &
\end{array} \tag{3.6}$$

in which the rows are obtained by tensoring the Kummer exact sequences by μ_n, and the vertical maps are obtained by base change.

We have proved that $\chi_i \cup \chi_i'$ is G-invariant, so that it comes from a class in $H^2(\mathbb{P}^1_K, \mu_n^{\otimes 2})$ by Lemma 3.5. Moreover, because $\chi_i \cup \chi_i'$ splits over the point P_0, the corresponding class in $H^2(\mathbb{P}^1_K, \mu_n^{\otimes 2})$ splits over the image of P_0 in $\mathbb{P}^1_K$. By diagram (3.6) and Lemma 3.6, it belongs to the image of

$$(\mathrm{Pic}(\mathbb{P}^1_K)/n) \otimes \mu_n \longrightarrow H^2(\mathbb{P}^1_K, \mu_n^{\otimes 2}).$$

On the other hand, the map $C \longrightarrow \mathbb{P}^1_K$ has degree 2, hence the natural map

$$(\mathrm{Pic}(\mathbb{P}^1_K)/n) \longrightarrow (\mathrm{Pic}(C \otimes_K \overline{K})/n)$$

can be identified, via the degree map, with the multiplication-by-2 map $[2] : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, which is an isomorphism, since n is odd. It follows that the composition of the two vertical maps in the first column of (3.6) is the multiplication-by-2 map $\mu_n \longrightarrow \mu_n$. Hence this composition is an isomorphism. Composing with the isomorphism at the bottom of (3.6), it follows that $\chi_i \cup \chi'_i$, and more generally $\sum_{i=1}^d [\chi_i \cup \chi'_i]$, can be identified with its image in $H^2(C \otimes_K \overline{K}, \mu_n^{\otimes 2})$.

Finally, by [8, Chap. V, Remark 2.4 (f)], the following diagram commutes

$$\begin{array}{ccc} H^1(C \otimes_K \overline{K}, \mu_n) \times H^1(C \otimes_K \overline{K}, \mu_n) & \xrightarrow{\cup} & H^2(C \otimes_K \overline{K}, \mu_n^{\otimes 2}) \\ \| & \| & \| \\ \mathrm{Pic}^0(C \otimes_K \overline{K})[n] \times \mathrm{Pic}^0(C \otimes_K \overline{K})[n] & \xrightarrow{e_n} & \mu_n \end{array}$$

We deduce that the image of $\sum_{i=1}^d [\chi_i \cup \chi'_i]$ in $H^2(C \otimes_K \overline{K}, \mu_n^{\otimes 2}) = \mu_n$ can be identified with

$$\prod_{i=1}^d e_n(L_i, L'_i)$$

which is trivial by hypothesis. Now according to Theorem 2.1, there exists a $\mathcal{H}_{2d+1}(\mu_n)$-torsor $C' \longrightarrow C$ whose associated $(\mu_n)^{2d}$-torsor is the $2d$-tuple $(\chi_1, \ldots, \chi_d, \chi'_1, \ldots, \chi'_d)$. By Lemma 3.7, we can make a constant field twist of the central action of the twisted Heisenberg group on C' to ensure that $C' \longrightarrow C$ splits over P_0. This completes the proof of part (2).

For part (3), we use that by Kummer theory, we have an isomorphism

$$H^1(C \otimes_K \overline{K}, (\mu_n)^{2d}) \simeq \mathrm{Hom}((\mathbb{Z}/n\mathbb{Z})^{2d}, \mathrm{Pic}^0(C \otimes_K \overline{K}))$$

under which connected torsors correspond to injective morphisms. But the image of the $(\mu_n)^{2d}$-torsor $(\chi_1, \ldots, \chi_d, \chi'_1, \ldots, \chi'_d)$ is none other than the map defined by the $2d$-tuple $(L_1, \ldots, L_d, L'_1, \ldots, L'_d)$. Therefore, our $(\mu_n)^{2d}$-torsor is geometrically connected if and only if the subgroup generated by the L_i and the L'_i in $\mathrm{Pic}^0(C \otimes_K \overline{K})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2d}$. The map $\mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}^0(C \otimes_K \overline{K})$ being injective, it suffices to check this over K. The conclusion of part (3) follows from the last statement in Theorem 2.1. ∎

3.1. An example with $d = 1$ over $\mathbb{Q}$.

Corollary 3.8: *Let $\lambda \in \mathbb{Q}^\times$, $\lambda^2 \neq 1$, and let $n > 1$ be an odd integer. Let C be the hyperelliptic curve defined over $\mathbb{Q}$ by the affine equation*

$$y^2 = x^{2n} - (1+\lambda^2)x^n + \lambda^2,$$

and let K be a number field such that $[K(\mu_n) : K]$ is prime to n. Then there exists a geometrically connected $\mathcal{H}_3(\mu_n)$-torsor over $C \otimes_{\mathbb{Q}} K$, which splits over the point $P_0 = (1, 0)$.

We note that, if n is prime, or more generally if $\varphi(n)$ is prime to n, then the hypotheses of Corollary 3.8 are satisfied for $K = \mathbb{Q}$.

Proof. We note that P_0 is a rational Weierstrass point of C. It is proved in [2, Lemma 3.3] that $\mathrm{Pic}^0(C)$ contains two independent classes of order n, which we denote by L and L'. The Weil pairing $e_n(L, L')$ takes values in $\mu_n(\mathbb{Q}) = \{1\}$, therefore $e_n(L, L') = 1$. If we consider the classes L and L' in $\mathrm{Pic}^0(C \otimes_{\mathbb{Q}} K)$, then their Weil pairing over K has the same value, hence the assumptions of Theorem 3.1 are satisfied, and the result follows. ∎

3.2. An example with $d = 2$, $n = 3$ over $\mathbb{Q}$.

Corollary 3.9: *There exists a hyperelliptic curve C defined over $\mathbb{Q}$, together with a rational Weierstrass point P_0, and a geometrically connected $\mathcal{H}_5(\mu_3)$-torsor over C which splits over P_0.*

Proof. Following an idea of Craig, a construction is given in [3, Theorem 2.3] of a hyperelliptic curve C over $\mathbb{Q}$, together with a rational Weierstrass point P_0, and four independent classes in $\mathrm{Pic}(C)[3]$. The same argument as in Corollary 3.8 proves that the assumptions of Theorem 3.1 are satisfied, hence the result. ∎

3.3. A remark on the general case. Let F be a number field, and let C be a hyperelliptic curve of genus g over F, with an F-rational Weierstrass point P_0. Let K be the field of definition of the points of $J_C[n]$, the full n-torsion subgroup of the Jacobian of C. Then $K(\mu_n) = K$, because the Weil pairing is non-degenerate. It is easy to check that the hypotheses of Theorem 3.1 are satisfied for the curve C over K when putting $d = g$. Hence there exists a geometrically connected, étale $\mathcal{H}_{2g+1}(\mathbb{Z}/n\mathbb{Z})$-torsor over C which splits over P_0, and whose associated $(\mathbb{Z}/n\mathbb{Z})^{2g}$-torsor is the maximal (pointed) étale Galois cover of C whose Galois group is an n-torsion abelian group.

Given F and n, one may ask which number fields K can be obtained as the field of definition of the points of $J_C[n]$ for some hyperelliptic curve C of genus g. We note that, in any case, K/F is Galois and

$$\mathrm{Gal}(K/F) \hookrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$$

where GSp denotes the general symplectic group. Indeed, $J_C[n]$ is a Galois module with underlying abelian group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$, and the Weil pairing on $J_C[n]$ is non-degenerate and alternating. It follows that $\mathrm{Gal}(\overline{K}/K)$ acts on $J_C[n]$ via $\mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$, so $[K : F]$ divides $\#\,\mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$. Sharper bounds on $[K : F]$ can be obtained with more hypotheses on C, e.g. by assuming that J_C has complex multiplication.

In view of such constructions involving torsion points on hyperelliptic curves, the following question naturally arises (see also [2, Question 3.5]):

Question 3.10: Given positive integers n and r, does there exist a hyperelliptic curve C defined over $\mathbb{Q}$ such that $\mathrm{Pic}^0(C)$ contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$?

The curve defined in Corollary 3.8 gives a positive answer to this question when $r = 2$ and n is arbitrary. To our knowledge, this is currently the strongest known general result concerning this question. Solutions for specific small pairs (n, r) are given in [5].

In view of the previous discussion, one may of course replace $\mathbb{Q}$ by an arbitrary number field F.

4. Arithmetic specialization

Throughout this section, K denotes a number field, and S a finite set of places of K. We denote by $\mathcal{O}_{K,S}$ the ring of S-integers of K, obtained by inverting in the full ring of integers of K all finite places which belong to S.

Let us consider a finite étale (not necessarily commutative) $\mathcal{O}_{K,S}$-group scheme G. We denote by $H^1_{\text{ét}}(\mathcal{O}_{K,S}, G)$ the cohomology set which classifies étale G-torsors over $\mathcal{O}_{K,S}$. We denote by G_K the generic fiber of G, and by $H^1(K, G_K)$ the (possibly non-abelian) Galois cohomology set

$$H^1(\mathrm{Gal}(\bar{K}/K), G_K(\bar{K})).$$

Let us recall that the "restriction to the generic fiber" map

$$H^1_{\text{ét}}(\mathcal{O}_{K,S}, G) \longrightarrow H^1(K, G_K)$$

is injective. This allows us to identify $H^1_{\text{ét}}(\mathcal{O}_{K,S}, G)$ with a subset of $H^1(K, G_K)$.

We now define a set of cohomology classes which are locally trivial at all places in S. These classes will be called S-split.

Definition 4.1: If S is a finite set of places of K, we let

$$H^1_{S\text{-split}}(\mathcal{O}_{K,S}, G) := \ker\left(H^1_{\text{ét}}(\mathcal{O}_{K,S}, G) \longrightarrow \prod_{v\in S} H^1_{\text{ét}}(K_v, G_{K_v})\right).$$

In more algebraic terms, $H^1_{S\text{-split}}(\mathcal{O}_{K,S}, G)$ is the subset of $H^1(K, G_K)$ consisting of K-algebras which are unramified at finite places outside S, and in which all places in S (including the infinite ones) are totally split. In particular, such algebras are unramified at all finite places of K.

We are now ready to state our specialization theorem, which follows immediately from the results of Bilu and the third author [1].

THEOREM 4.2: *Let us consider the setting of Theorem 3.1, with the additional assumption that K is a number field. Let $\psi : \tilde{C} \longrightarrow C$ be a geometrically connected étale $\mathcal{H}_{2d+1}(\mu_n)$-torsor which splits over the point P_0, whose existence is ensured by Theorem 3.1. Then there exists a finite set S of places of K with the following properties:*

(1) *S contains all places above n;*
(2) *the torsor $\psi : \tilde{C} \longrightarrow C$ extends to a $\mathcal{H}_{2d+1}(\mu_n)$-torsor between smooth $\mathcal{O}_{K,S}$-curves.*

Moreover, given any such S, there exist infinitely many (isomorphism classes of) quadratic extensions L/K with the following properties. There is a point $P \in C(L)$ such that the specialization of ψ at P is a connected $\mathcal{H}_{2d+1}(\mu_n)$-torsor and belongs to the subset $H^1_{S\text{-split}}(\mathcal{O}_{L,S}, \mathcal{H}_{2d+1}(\mu_n))$.

Furthermore, there is a constant $c > 0$ depending only on K, ψ and S for which the following is true. Let $g(C)$ denote the genus of C. For sufficiently large positive N, the number of (isomorphism classes of) such fields L whose relative discriminant $\Delta(L/K)$ satisfies

$$|\mathrm{N}_{K/\mathbb{Q}}\Delta(L/K)|^{1/[K:\mathbb{Q}]} \leq N$$

is at least $cN^{[K:\mathbb{Q}]/(4g(C)+2)}/\log N$.

In the statement above, slightly abusing notation, we denote by the same letter S the set of places of L lying above places in S.

Here is another way to state the conclusion of Theorem 4.2. For infinitely many quadratic extensions L/K, we obtain by specializing ψ an extension of degree n^{2d+1} of L that is a $\mathcal{H}_{2d+1}(\mu_n)$-torsor, in which all finite places are unramified and places above S are totally split.

In the case where $K(\mu_n) = K$, $\mathcal{H}_{2d+1}(\mu_n)$ is isomorphic to the constant Heisenberg group scheme $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$, and we obtain by specializing ψ a Galois extension of L with group $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$, in which all finite places are unramified and places above S are totally split.

Remark 4.3: Given a set S satisfying (1) and (2) in Theorem 4.2, any larger set also satisfies these conditions. When enlarging S, the condition that the specialization of ψ at P belongs to $H^1_{S\text{-split}}(\mathcal{O}_{L,S}, \mathcal{H}_{2d+1}(\mu_n))$ is stronger, which has the effect of enlarging the constant c in the quantitative statement.

Proof of Theorem 4.2. The existence of a set S satisfying conditions (1) and (2) follows by elementary considerations on the reduction of covers of curves, known as the Chevalley–Weil theorem; see for example [9, Section 4.2]. A hyperelliptic curve with a rational Weierstrass point admits an affine model of the form $y^2 = f(x)$ where $f \in K[x]$ is a polynomial of degree $2g + 1$. Theorem 4.2 now follows from [1, Theorems 4.3 and 4.7]. ∎

4.1. Unramified twisted Heisenberg torsors over quadratic fields. By combining Corollary 3.8 and Theorem 4.2, we obtain the following result.

Corollary 4.4: *Let p be an odd prime. Then there exist infinitely many (imaginary and real) quadratic fields L which admit a connected $\mathcal{H}_3(\mu_p)$-torsor, unramified at all finite places of L. Moreover, given a finite set T of prime numbers containing p, there exist infinitely many such L for which primes lying above T in L are totally split in the extension corresponding to the $\mathcal{H}_3(\mu_p)$-torsor.*

We assume here that p is prime in order to ensure that $[\mathbb{Q}(\mu_p) : \mathbb{Q}]$ is prime to p, which is required in the statement of Corollary 3.8. When applying Theorem 4.2, we choose a sufficiently large set S containing T and satisfying the required conditions.

One can also deduce from Theorem 4.2 a quantitative version of the statement above.

4.2. Unramified Heisenberg Galois extensions over quadratic extensions of cyclotomic fields. By combining Corollary 3.8 and Theorem 4.2 over the cyclotomic field $\mathbb{Q}(\zeta_n)$, one obtains Theorem 1.1 stated in the introduction.

4.3. General remarks about the unramified Inverse Galois problem. It is a folklore conjecture that every finite group occurs as the Galois group of an unramified Galois extension of some quadratic number field. In the case of finite abelian groups, this would be an immediate consequence of the Cohen–Lenstra heuristics.

In fact, in the abelian case, the strongest general result concerning this folklore conjecture is obtained by arithmetic specialization from the hyperelliptic curve of Corollary 3.8. More precisely, one obtains from this curve infinitely many imaginary quadratic fields whose class group contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$, and the rest follows from class field theory.

The construction of unramified Galois extensions of small degree number fields has a long history. Shafarevich proved that the Inverse Galois problem over $\mathbb{Q}$ has a solution for solvable groups. Using Shafarevich-type methods, it was recently proved by Kim [6] that, if G is a solvable group of exponent g, there exists a number field K of degree g such that G can be realized as the Galois group of an everywhere unramified extension of K. Since $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$ is a metabelian group of exponent n, one deduces from Kim's result that there exist number fields K of degree n over which $\mathcal{H}_{2d+1}(\mathbb{Z}/n\mathbb{Z})$ can be realized as the Galois group of an everywhere unramified extension. However, the approach in [6] by itself does not apply to the folklore conjecture as soon as G has exponent larger than 2.

Our Theorem 1.1 is a result in the direction of the folklore conjecture, using a completely different, geometric approach. The advantage of this approach is that it can in principle lead to proofs of the folklore conjecture for various G of large exponent provided one can construct hyperelliptic curves with suitable properties. More explicitly, the proof of Theorem 1.1 suggests a connection between Question 3.10 and the folklore conjecture.

References

[1] Y. Bilu and J. Gillibert, *Chevalley–Weil theorem and subgroups of class groups*, Israel Journal of Mathematics **226** (2018), 927–956.

[2] J. Gillibert and A. Levin, *Pulling back torsion line bundles to ideal classes*, Mathematical Research Letters **19** (2012), 1171–1184.

[3] J. Gillibert and A. Levin, *A geometric approach to large class groups: a survey*, in *Class Groups of Number Fields and Related Topics*, Springer, Singapore, 2020, pp. 1–15.

[4] J. Giraud, *Cohomologie non abélienne*, Die Grundlehren der mathematischen Wissenschaften, Vol. 179, Springer, Berlin–New York, 1971.

[5] E. W. Howe, F. Leprévost and B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Mathematicum **12** (2000), 315–364.

[6] K.-S. Kim, *Construction of unramified extensions with a prescribed solvable Galois group*, Acta Arithmetica **190** (2019), 49–56.

[7] A. Levin, *Variations on a theme of Runge: effective determination of integral points on certain varieties*, Journal de Théorie des Nombres de Bordeaux **20** (2008), 385–417.

[8] J. S. Milne, *Étale Cohomology*, Princeton Mathematical Series, Vol. 33, Princeton University Press, Princeton, NJ, 1980.

[9] J.-P. Serre, *Lectures on the Mordell–Weil Theorem*, Aspects of Mathematics, Friedrich Vieweg & Sohn, Braunschweig, 1997.

[10] R. Sharifi, *Twisted Heisenberg representations and local conductors*, Ph.D. thesis, The University of Chicago, 1999.

[11] R. Sharifi, *Massey products and ideal class groups*, Journal für die reine und angewandte Mathematik **603** (2007), 1–33.

[12] H. Völklein, *Central extensions as Galois groups*, Journal of Algebra **146** (1992), 144–152.

[13] H. Völklein, *Groups as Galois Groups. An Introduction*, Cambridge Studies in Advanced Mathematics, Vol. 53, Cambridge University Press, Cambridge, 1996.