ACTA ARITHMETICA
159.2 (2013)

Explicit Selmer groups for cyclic covers of $\mathbb{P}^1$

by

Michael Stoll (Bayreuth) and Ronald van Luijk (Leiden)

1. Introduction. Let k be a field and k^{s} a separable closure of k with Galois group $G_k = \mathrm{Gal}(k^{\mathrm{s}}/k)$. Let C be a smooth projective curve over k with Jacobian J. Let $\phi\colon J \to J$ be a separable isogeny and $J[\phi]$ the kernel of $\phi\colon J(k^{\mathrm{s}}) \to J(k^{\mathrm{s}})$. Taking Galois invariants of the short exact sequence

$$0 \to J[\phi] \to J(k^{\mathrm{s}}) \xrightarrow{\phi} J(k^{\mathrm{s}}) \to 0$$

gives rise to a long exact sequence, which induces another short exact sequence

$$0 \to J(k)/\phi J(k) \xrightarrow{\delta_\phi} \mathrm{H}^1(G_k, J[\phi]) \to \mathrm{H}^1(G_k, J(k^{\mathrm{s}}))[\phi] \to 0,$$

where $\mathrm{H}^1(G_k, J(k^{\mathrm{s}}))[\phi]$ stands for the kernel of the map

$$\phi_*\colon \mathrm{H}^1(G_k, J(k^{\mathrm{s}})) \to \mathrm{H}^1(G_k, J(k^{\mathrm{s}}))$$

induced by ϕ on cohomology. If $J(k)$ is finitely generated, which is the case if k is finitely generated as a field over its prime subfield, and if ϕ is not an automorphism, then often, including in the cases we will treat, the size of the group $J(k)/\phi J(k)$ yields a bound on the rank of the Mordell–Weil group $J(k)$. As many methods of retrieving arithmetic information about C, such as the Mordell–Weil sieve and Chabauty's method, involve the rank of $J(k)$, it is of interest to be able to bound the size of $J(k)/\phi J(k)$, or equivalently, of its image in $\mathrm{H}^1(G_k, J[\phi])$. Unfortunately, this group $\mathrm{H}^1(G_k, J[\phi])$ is in general very large and hard to handle.

Now assume that k is a global field. For each place v of k, we write k_v for the completion of k at v. Then the local analogues of the map $J(k)/\phi J(k) \to \mathrm{H}^1(G_k, J[\phi])$ for each place v can be put together to give the following commutative diagram:

2010 *Mathematics Subject Classification*: Primary 11G30; Secondary 11G10, 14G25, 14H30, 14H40.
Key words and phrases: Selmer group, fake Selmer group, descent.

DOI: 10.4064/aa159-2-4

$$\begin{array}{ccccc} J(k)/\phi J(k) & \xrightarrow{\delta_\phi} & \mathrm{H}^1(G_k, J[\phi]) & \longrightarrow & \mathrm{H}^1(G_k, J(k^{\mathrm{s}}))[\phi] \\ \downarrow & & \downarrow & \overset{\tau}{\searrow} & \downarrow \\ \prod_v J(k_v)/\phi J(k_v) & \longrightarrow & \prod_v \mathrm{H}^1(\mathrm{Gal}(k_v^{\mathrm{s}}/k_v), J[\phi]) & \longrightarrow & \prod_v \mathrm{H}^1(G_k, J(k_v^{\mathrm{s}}))[\phi] \end{array}$$

Here $\prod_v$ denotes the product over all places of k. By definition, the Selmer group $\mathrm{Sel}^\phi(J,k)$ is the kernel of τ: it consists of all elements of $\mathrm{H}^1(G_k, J[\phi])$ that map into the image of the local map

$$J(k_v)/\phi J(k_v) \to \mathrm{H}^1(\mathrm{Gal}(k_v^{\mathrm{s}}/k_v), J[\phi])$$

for every v. Clearly $\mathrm{Sel}^\phi(J,k)$ contains the image of δ_ϕ, and it can be shown that $\mathrm{Sel}^\phi(J,k)$ is an effectively computable finite group, which already gives a bound on $J(k)/\phi J(k)$. However, the description of $\mathrm{Sel}^\phi(J,k)$ as a subgroup of $\mathrm{H}^1(G_k, J[\phi])$ is not amenable to explicit computations.

In [PS], Poonen and Schaefer consider curves C with an affine model given by $y^p = f(x)$, where p is a prime number and f is p-power free and splits into linear factors over k^{s}. They assume that the characteristic of k is not equal to p and that k contains a primitive pth root ζ of unity. They take the isogeny to be $\phi = 1 - \zeta$, where ζ acts on C as $(x, y) \mapsto (x, \zeta y)$. From now on we restrict ourselves to this situation as well. Note that this includes hyperelliptic curves as the special case $p = 2$; then the isogeny ϕ is multiplication by 2. Upon applying an automorphism of the x-line, we may assume that the map to the x-line does not ramify at ∞, so that the degree of f is divisible by p ([1]). Let f_0 be a *radical* of f, i.e., a separable polynomial in $k[x]$ with the same roots in k^{s} as f, and set $L = k[T]/f_0(T)$. We assume that every point in $J(k)$ can be represented by a k-rational divisor on C. Poonen and Schaefer define a homomorphism $(x - T)\colon J(k) \to L^*/L^{*p}k^*$ and show that it factors as

$$J(k) \to J(k)/\phi J(k) \xrightarrow{\delta_\phi} \mathrm{Sel}^\phi(J,k) \to L^*/L^{*p}k^*. \tag{1.1}$$

We will recall the definition of this map in Section 4. For $p = 2$ and a polynomial f of degree 4 with a rational root, the curve C is elliptic; the last map in the factorization is injective in this case and the map $(x - T)$ gives the usual 2-descent map on C. For $p = 2$ and $\deg f = 6$, Cassels [Ca1] had already defined the map $(x - T)$ (using different notation), but it was Poonen and Schaefer who related it to the cohomological map δ_ϕ through the given factorization.

In general, and in fact already in Cassels' case, the last map in the factorization need not be injective; its kernel is trivial or isomorphic to μ_p.

([1]) For this to be true, k has to be sufficiently large. Later k will be a global field, and there will be no problem.

Following [PS], the image of $\mathrm{Sel}^\phi(J,k)$ in $L^*/L^{*p}k^*$ is called the *fake Selmer group* $\mathrm{Sel}^\phi_{\mathrm{fake}}(J,k)$; it is a quotient of the true Selmer group $\mathrm{Sel}^\phi(J,k)$. This means that, although the group $L^*/L^{*p}k^*$ is easier to work with explicitly than $\mathrm{Sel}^\phi(J,k)$, information may get lost by studying the image of $J(k)/\phi J(k)$ in the former group instead of the latter.

The aim of this paper is to replace the group $L^*/L^{*p}k^*$ by one that is equally easy to work with and that admits an injection from $\mathrm{Sel}^\phi(J,k)$ into it, and thus also from $J(k)/\phi J(k)$. The description of such a group involves a 'weighted norm map' N defined as follows. Let $f = c\prod_j f_j^{m_j}$ be the unique factorization of f over k with f_j monic and $c \in k^*$. For $\beta \in L^*$ we then set

$$N(\beta) = \prod_j \mathrm{Norm}_{L_j/k}(\beta_j)^{m_j},$$

where β_j is the image of β in the field $L_j = k[x]/f_j(x)$.

It turns out that the image of the last map $\mathrm{Sel}^\phi(J,k) \to L^*/L^{*p}k^*$ of the factorization (1.1) is contained in the kernel of the map $N\colon L^*/L^{*p}k^* \to k^*/k^{*p}$ induced by the weighted norm map. The new group consists of all elements of this kernel, together with some choice of pth root of their norm. More precisely, we will prove the following theorem.

THEOREM 1.1. *Let k be a global field containing a primitive pth root of unity, and let C, J, L and N be as in the discussion above. Assume that for each place v of k, the curve C has a k_v-rational divisor class of degree* 1. *Set $\Gamma = \{(\delta, n) \in L^* \times k^* \mid N(\delta) = n^p\}$ and let $\chi\colon L^* \to \Gamma$ be given by $\theta \mapsto (\theta^p, N(\theta))$. Let $\iota : k^* \to \Gamma$ be defined by $x \mapsto (x, x^{(1/p)\deg f})$. Then there is a homomorphism $(x - T, y)\colon J(k) \to \Gamma/\chi(L^*)\iota(k^*)$ that factors as*

$$J(k) \to J(k)/\phi J(k) \xrightarrow{\delta_\phi} \mathrm{Sel}^\phi(J,k) \hookrightarrow \Gamma/\chi(L^*)\iota(k^*)$$

and whose composition with the map $\Gamma/\chi(L^*)\iota(k^*) \to L^*/L^{*p}k^*$ induced by the projection $\Gamma \to L^*$ equals the map $(x - T)$.

The map $(x - T, y)$ will be defined in Section 4. The isomorphic image of $\mathrm{Sel}^\phi(J,k)$ in $\Gamma/\chi(L^*)\iota(k^*)$ is the *explicit Selmer group* $\mathrm{Sel}^\phi_{\mathrm{explicit}}(J,k)$.

If all one wants is to get the size of the Selmer group (and thus an upper bound on the Mordell–Weil rank), then the results of [PS] are sufficient, since they tell us exactly the difference between the $\mathbb{F}_p$-dimensions of $\mathrm{Sel}^\phi(J,k)$ and $\mathrm{Sel}^\phi_{\mathrm{fake}}(J,k)$. On the other hand, apart from the intellectual satisfaction resulting from a nice explicit description of the Selmer group itself, the additional information given by identifying $\mathrm{Sel}^\phi(J,k)$ with the explicit Selmer group gives us a handle on the covering spaces corresponding to its elements: in [FTvL] equations for the covering spaces are given in the genus two case that depend on the image of the Selmer group element in the fake Selmer group together with a square root of its norm, which

is precisely the information contained in the corresponding element of the explicit Selmer group. Explicit models of these covering spaces are useful for the search of potentially large Mordell–Weil generators and can also serve as a starting point for second descents. In particular, one can hope that our explicit Selmer group can be used to extend Cassels' method for computing the Cassels–Tate pairing on the 2-Selmer group of an elliptic curve [Ca2], which uses the quadratic Hilbert symbol on elements of the explicit version of the Selmer group, to Jacobians of curves of genus two.

Since our results here extend and improve what Poonen and Schaefer have done, much of this paper is based on [PS], including the weighted norm map N. The main new element brought in is the group Γ of Theorem 1.1, which was first introduced in [FTvL]. The recent preprint [BPS] contains in its appendix a general recipe for turning 'fake' Selmer groups into 'explicit' ones, which was developed as a generalization of the method given in [ScSt] for p-descent on elliptic curves with p odd and of the approach described here. Our result could in principle also be obtained as a special case of this general recipe. However, the more direct approach used here leads to a much simpler proof.

In the next section we will introduce some notation, all following [PS]. In Section 3 we identify some cohomology groups with more explicit groups such as those mentioned in Theorem 1.1. In Section 4 we define the maps $(x - T)$ and $(x - T, y)$, so that in the last section we can 'unfake' the fake Selmer group and replace it with the explicit Selmer group by proving Theorem 1.1.

2. Notation. Our setting will be the same as in [PS]. Let p be a prime. Let k be a field of characteristic not equal to p and let k^{s} be a separable closure of k with Galois group $G_k = \mathrm{Gal}(k^{\mathrm{s}}/k)$. Assume that k contains a primitive pth root of unity. For any G_k-module A and any integer $i \geq 0$ we abbreviate the cohomology group $\mathrm{H}^i(G_k, A)$ by $\mathrm{H}^i(A)$. Let $\pi\colon C \to \mathbb{P}^1$ be a cyclic cover of $\mathbb{P}^1$ over k of degree p such that all branch points are in $\mathbb{P}^1(k^{\mathrm{s}}) \setminus \{\infty\}$. By Kummer theory, the curve C has a (possibly singular) model in $\mathbb{A}^2(x, y)$ given by $y^p = f(x)$, where $f \in k[x]$ factors over k^{s} as

$$f(x) = c \prod_{\omega \in \Omega} (x - \omega)^{a_\omega}$$

with $c \in k^*$, with $1 \leq a_\omega < p$ for all ω in the set $\Omega \subset k^{\mathrm{s}}$ of roots of f, and where p divides the degree $\deg f = \sum_\omega a_\omega$ of f. Set $d = \#\Omega$. By the Riemann–Hurwitz formula the genus of C equals $g(C) = (d - 2)(p - 1)/2$.

For any k-variety V, we write $V^{\mathrm{s}} = V \times_k k^{\mathrm{s}}$, while $\kappa(V)$ and $\kappa(V^{\mathrm{s}})$ denote the function fields of V and V^{s}. Let $\mathrm{Div}\, C^{\mathrm{s}}$ be the group of all divisors on C^{s}. If $f \in \kappa(C^{\mathrm{s}})^*$, we denote the divisor of f by $\mathrm{div}(f) \in \mathrm{Div}\, C^{\mathrm{s}}$. We let

$\operatorname{Princ} C^{\mathrm{s}} = \{\operatorname{div}(f) : f \in \kappa(C^{\mathrm{s}})^*\}$ be the subgroup of principal divisors. Set $\operatorname{Pic} C^{\mathrm{s}} = \operatorname{Div} C^{\mathrm{s}}/\operatorname{Princ} C^{\mathrm{s}}$. Also set

$$\begin{aligned}\operatorname{Div} C &= \mathrm{H}^0(\operatorname{Div} C^{\mathrm{s}}),\\ \operatorname{Princ} C &= \mathrm{H}^0(\operatorname{Princ} C^{\mathrm{s}}),\\ \operatorname{Pic} C &= \operatorname{Div} C/\operatorname{Princ} C.\end{aligned}$$

As in [PS], we consider the divisor $\mathfrak{m} = \pi^*\infty \in \operatorname{Div} C$, the sum of all p points above $\infty \in \mathbb{P}^1$. For any function h in the function field $\kappa(C^{\mathrm{s}})$ of C^{s} we say that h *is* $1 \bmod \mathfrak{m}$ if $h(P) = 1$ for all points P in the support of $\mathfrak{m}$ (for a more general definition, see [PS, Section 2]). Let $\operatorname{Div}_{\mathfrak{m}} C^{\mathrm{s}} \subset \operatorname{Div} C^{\mathrm{s}}$ be the group of all divisors with support disjoint from $\mathfrak{m}$, and let $\operatorname{Princ}_{\mathfrak{m}} C^{\mathrm{s}} \subset \operatorname{Princ} C^{\mathrm{s}}$ be the subgroup of all principal divisors of functions that are $1 \bmod \mathfrak{m}$. Set $\operatorname{Pic}_{\mathfrak{m}} C^{\mathrm{s}} = \operatorname{Div}_{\mathfrak{m}} C^{\mathrm{s}}/\operatorname{Princ}_{\mathfrak{m}} C^{\mathrm{s}}$ and

$$\begin{aligned}\operatorname{Div}_{\mathfrak{m}} C &= \mathrm{H}^0(\operatorname{Div}_{\mathfrak{m}} C^{\mathrm{s}}),\\ \operatorname{Princ}_{\mathfrak{m}} C &= \mathrm{H}^0(\operatorname{Princ}_{\mathfrak{m}} C^{\mathrm{s}}),\\ \operatorname{Pic}_{\mathfrak{m}} C &= \operatorname{Div}_{\mathfrak{m}} C/\operatorname{Princ}_{\mathfrak{m}} C.\end{aligned}$$

Let $\operatorname{Div}^0 C^{\mathrm{s}} \subset \operatorname{Div} C^{\mathrm{s}}$ be the subgroup of divisors of degree 0 and let $\operatorname{Div}^0 C$, $\operatorname{Pic}^0_{\mathfrak{m}} C^{\mathrm{s}}$, etc. be the degree-zero parts of the corresponding groups. Let $\operatorname{Div}^{(p)} C^{\mathrm{s}} \subset \operatorname{Div} C^{\mathrm{s}}$ be the subgroup of divisors of degree divisible by p and let $\operatorname{Div}^{(p)} C$, $\operatorname{Pic}^{(p)}_{\mathfrak{m}} C^{\mathrm{s}}$, etc. be the degree-divisible-by-p parts of the corresponding groups. Let J and $J_{\mathfrak{m}}$ denote the Jacobian of C and the generalized Jacobian of the pair $(C, \mathfrak{m})$, respectively, so that $J(k^{\mathrm{s}}) = \operatorname{Pic}^0 C^{\mathrm{s}}$ and $J_{\mathfrak{m}}(k^{\mathrm{s}}) = \operatorname{Pic}^0_{\mathfrak{m}} C^{\mathrm{s}}$. We write $J[p]$ and $J_{\mathfrak{m}}[p]$ for the kernel of multiplication-by-p, written as $[p]$, on $J(k^{\mathrm{s}})$ and $J_{\mathfrak{m}}(k^{\mathrm{s}})$, respectively. We denote the trivial group in diagrams by 1.

3. Making cohomology groups explicit. Pick any $c_0 \in k^*$ and define a radical $f_0 = c_0 \prod_{\omega\in\Omega}(x - \omega) \in k[x]$ of f. Set $L = k[X]/f_0(X)$ and $L^{\mathrm{s}} = L \otimes_k k^{\mathrm{s}}$. We will denote the image of X in L and L^{s} by T. By the Chinese Remainder Theorem, the k^{s}-linear maps $\rho_\omega \colon L^{\mathrm{s}} \to k^{\mathrm{s}}$, $T \mapsto \omega$, combine to an isomorphism

$$\rho = (\rho_\omega)_{\omega\in\Omega} \colon L^{\mathrm{s}} \to \prod_{\omega\in\Omega} k^{\mathrm{s}},$$

which restricts to the diagonal embedding on $k^{\mathrm{s}} \subset L^{\mathrm{s}}$. From now on, whenever ω is used as index, it ranges over all elements of Ω. Note that the induced Galois action on $\prod_\omega k^{\mathrm{s}}$ is given by acting on the indices as well, so by $\sigma((a_\omega)_\omega) = (\sigma(a_{\sigma^{-1}\omega}))_\omega$. We often identify L^{s} with $\prod_\omega k^{\mathrm{s}}$ through ρ, thereby identifying T with the element $(\omega)_\omega$. For any commutative ring R, we let $\mu_p(R)$ denote the kernel of the homomorphism $R^* \to R^*$, $x \mapsto x^p$. We abbreviate $\mu_p(k) = \mu_p(k^{\mathrm{s}})$ by μ_p and note that ρ induces an isomor-

phism $\mu_p(L^{\mathrm{s}}) \to \prod_\omega \mu_p$. Let the 'weighted norm map' $N\colon L^{\mathrm{s}} \cong \prod_\omega k^{\mathrm{s}} \to k^{\mathrm{s}}$ be given by $(\beta_\omega)_\omega \mapsto \prod_\omega \beta_\omega^{a_\omega}$. Since p divides $\sum_\omega a_\omega$, the kernel of N contains μ_p. The map N is Galois-equivariant, as for conjugate roots $\omega, \omega' \in \Omega$ we have $a_\omega = a_{\omega'}$, so it induces a map $N\colon L \to k$. This map is the same as the norm map N that was defined in the introduction. Let M denote the kernel of the induced map $N\colon \mu_p(L^{\mathrm{s}}) \to \mu_p$. Then we obtain the following commutative diagram, in which the horizontal and vertical sequences are exact:

$$\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \mu_p & = & \mu_p & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & M & \longrightarrow & \mu_p(L^{\mathrm{s}}) & \xrightarrow{N} & \mu_p & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & M/\mu_p & \longrightarrow & \mu_p(L^{\mathrm{s}})/\mu_p & \xrightarrow{N} & \mu_p & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array} \tag{3.1}$$

Note that the map $N\colon \mu_p(L^{\mathrm{s}}) \to \mu_p$ is surjective because we can take 1 in each component of $\mu_p(L^{\mathrm{s}}) \cong \prod_\omega k^{\mathrm{s}}$ except for one component, say corresponding to ω, where we choose an a_ωth root of ζ, which exists because the greatest common divisor (a_ω, p) equals 1.

We will give a concrete description of the Galois cohomology groups $\mathrm{H}^1(M)$ and $\mathrm{H}^1(\mu_p(L^{\mathrm{s}}))$ and their images in $\mathrm{H}^1(M/\mu_p)$ and $\mathrm{H}^1(\mu_p(L^{\mathrm{s}})/\mu_p)$. Let $\partial\colon L^* \times k^* \to k^*$ be the homomorphism that sends (δ, n) to $N(\delta)n^{-p}$ and let ∂^{s} denote the corresponding map from $L^{\mathrm{s}*} \times k^{\mathrm{s}*}$ to $k^{\mathrm{s}*}$. Set

$$\begin{aligned}
\Gamma^{\mathrm{s}} &= \ker \partial^{\mathrm{s}} = \{(\delta, n) \in L^{\mathrm{s}*} \times k^{\mathrm{s}*} \mid N(\delta) = n^p\}, \\
\Gamma &= \mathrm{H}^0(\Gamma^{\mathrm{s}}) = \ker \partial = \{(\delta, n) \in L^* \times k^* \mid N(\delta) = n^p\}.
\end{aligned}$$

We will write ι for the injection $k^{\mathrm{s}*} \to \Gamma^{\mathrm{s}}$ given by $x \mapsto (x, x^{(1/p)\deg f})$; it restricts to an injection $\iota : k^* \to \Gamma$. Let the map $\chi\colon L^{\mathrm{s}*} \to \Gamma^{\mathrm{s}}$ be given by $\theta \mapsto (\theta^p, N(\theta))$. It is surjective, has kernel M, and restricts to a map $\chi\colon L^* \to \Gamma$. The long exact sequence associated to the short exact sequence

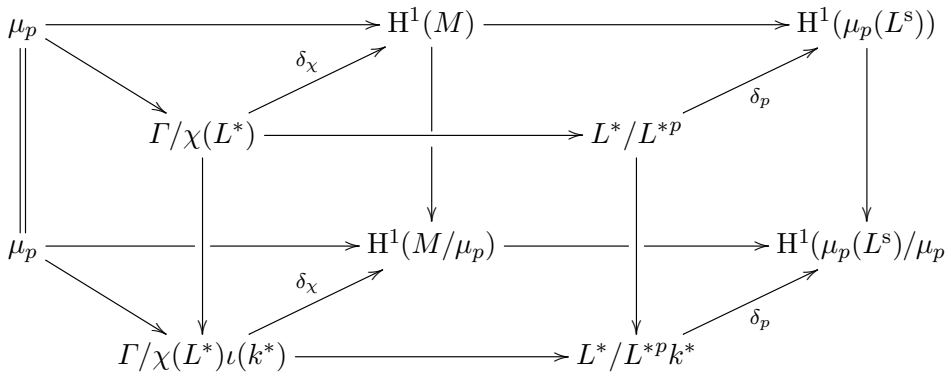
$$1 \to M \to L^{\mathrm{s}*} \xrightarrow{\chi} \Gamma^{\mathrm{s}} \to 1 \tag{3.2}$$

contains the connecting map $\delta_\chi\colon \Gamma \to \mathrm{H}^1(M)$, which sends (δ, n) to the class of the cocycle $G_k \ni \sigma \mapsto \sigma(\theta)/\theta \in M$ for a fixed choice of $\theta \in L^{\mathrm{s}*}$ with $\chi(\theta) = (\delta, n)$. Similarly, the short exact sequence

$$1 \to \mu_p(L^{\mathrm{s}}) \to L^{\mathrm{s}*} \xrightarrow{x \mapsto x^p} L^{\mathrm{s}*} \to 1 \tag{3.3}$$

provides a connecting map $\delta_p\colon L^* \to \mathrm{H}^1(\mu_p(L^{\mathrm{s}}))$. Parts of the following proposition were proved for $p = 2$ in [FTvL, Proposition 2.6].

PROPOSITION 3.1. *The map δ_χ induces an isomorphism $\delta_\chi\colon \Gamma/\chi(L^*) \to \mathrm{H}^1(M)$ and an isomorphism from $\Gamma/\chi(L^*)\iota(k^*)$ to the image of $\mathrm{H}^1(M)$ in $\mathrm{H}^1(M/\mu_p)$. The map δ_p induces an isomorphism $\delta_p\colon L^*/L^{*p} \to \mathrm{H}^1(\mu_p(L^{\mathrm{s}}))$ and an isomorphism from $L^*/L^{*p}k^*$ to the image of $\mathrm{H}^1(\mu_p(L^{\mathrm{s}}))$ in $\mathrm{H}^1(\mu_p(L^{\mathrm{s}})/\mu_p)$. These maps fit in the commutative diagram*



where the back face consists of part of the long exact sequences associated to the horizontal sequences in (3.1)*, the vertical maps in the front face are the obvious quotient-by-k^* maps, the horizontal maps in the front face are induced by the projection map $\Gamma \to L^*$, $(\delta, n) \mapsto \delta$, and the remaining maps from μ_p send $\zeta \in \mu_p$ to the class of $(1, \zeta)$.*

Proof. The commutativity of the front and back faces are obvious. The projection map $\Gamma^{\mathrm{s}} \to L^{\mathrm{s}*}$, $(\delta, n) \mapsto \delta$, induces a map between the short exact sequences (3.2) and (3.3). Part of the associated long exact sequences gives the following diagram:

$$\begin{array}{ccccccc} L^* & \xrightarrow{\chi} & \Gamma & \xrightarrow{\delta_\chi} & \mathrm{H}^1(M) & \longrightarrow & \mathrm{H}^1(L^{\mathrm{s}*}) \\ \| & & \downarrow & & \downarrow & & \| \\ L^* & \xrightarrow{x\mapsto x^p} & L^* & \xrightarrow{\delta_p} & \mathrm{H}^1(\mu_p(L^{\mathrm{s}})) & \longrightarrow & \mathrm{H}^1(L^{\mathrm{s}*}) \end{array}$$

By a generalization of Hilbert's Theorem 90 the group $\mathrm{H}^1(L^{\mathrm{s}*})$ is trivial (see [Se, Exercise X.1.2]). The commutativity of the quadrilateral in the top face follows, as well as the fact that the maps δ_χ and δ_p in it are isomorphisms. Similarly, also using that $\mathrm{H}^1(k^{\mathrm{s}*})$ vanishes by Hilbert's Theorem 90, the natural maps from the short exact sequence

$$1 \to \mu_p \to k^{\mathrm{s}*} \xrightarrow{x\mapsto x^p} k^{\mathrm{s}*} \to 1 \tag{3.4}$$

to (3.2) and (3.3) yield long exact sequences that induce the following diagrams:

$$\begin{array}{ccc} k^*/k^{*p} & \xrightarrow{\cong} & \mathrm{H}^1(\mu_p) \\ \downarrow & & \downarrow \\ \Gamma/\chi(L^*) & \xrightarrow[\delta_\chi]{\cong} & \mathrm{H}^1(M) \end{array} \qquad \begin{array}{ccc} k^*/k^{*p} & \xrightarrow{\cong} & \mathrm{H}^1(\mu_p) \\ \downarrow & & \downarrow \\ L^*/L^{*p} & \xrightarrow[\delta_p]{\cong} & \mathrm{H}^1(\mu_p(L^{\mathrm{s}})) \end{array}$$

The associated maps on cokernels of the vertical homomorphisms induce the claimed isomorphisms from $L^*/L^{*p}k^*$ to the image of $\mathrm{H}^1(\mu_p(L^{\mathrm{s}}))$ in $\mathrm{H}^1(\mu_p(L^{\mathrm{s}})/\mu_p)$ and from $\Gamma/\chi(L^*)\iota(k^*)$ to the image of $\mathrm{H}^1(M)$ in $\mathrm{H}^1(M/\mu_p)$. This also implies the commutativity of the left and right faces of the cube in the diagram. Commutativity of the quadrilateral in the bottom face follows immediately from the commutativity of the other faces of the cube and the fact that the quotient map $\Gamma/\chi(L^*) \to \Gamma/\chi(L^*)\iota(k^*)$ is surjective. Finally, choose a $\theta \in \mu_p(L^{\mathrm{s}})$ with $N(\theta) = \zeta$. Then the image of ζ in $\mathrm{H}^1(M)$ is represented by the cocycle $\sigma \mapsto \sigma(\theta)/\theta$, which coincides with $\delta_\chi((1,\zeta))$. It follows that also the triangular prism in the diagram commutes. ∎

4. A new map. Let h be a nonzero rational function on C. Then we can extend evaluation of h on points not in the support of $\mathrm{div}(h)$ multiplicatively to divisors whose support is disjoint from that of $\mathrm{div}(h)$ by setting

$$h(D) = \prod_P h(P)^{n_P} \quad \text{if } D = \sum_P n_P P.$$

If K is a field extension of k that is a field of definition of h, then this defines a group homomorphism from the group of K-defined divisors with support disjoint from that of $\mathrm{div}(h)$ into the multiplicative group of K.

In the following, we will frequently work with objects defined over L. There are (at least) two ways of interpreting what these objects mean. We can either just think of them as L-defined objects (functions, points, etc.), allowing étale algebras over k instead of only field extensions. Or else we remind ourselves that the elements of L correspond to Galois-equivariant maps from Ω into k^{s}; then a function defined over L can be considered as a Galois-equivariant map from Ω into $\kappa(C^{\mathrm{s}})$, etc. Sometimes, we use L^{s} in place of L; then the corresponding maps from Ω need not be Galois-equivariant. In this sense, $\mu_p(L^{\mathrm{s}})$ denotes the set of maps $\Omega \to \mu_p$, and M denotes the subset of maps η such that $N(\eta) = \prod_\omega \eta(\omega)^{a_\omega} = 1$.

For example, we let $W = (T, 0) \in C(L)$ be a 'generic ramification point' on C. In the second interpretation, W corresponds to the map $\omega \mapsto (\omega, 0)$ that gives all the ramification points on C indexed by the roots of f. In this section, we will consider the function $x - T$, which is an L-defined rational function on C. In our second interpretation, we associate to each $\omega \in \Omega$ the

rational function $x - \omega \in \kappa(C^{\mathrm{s}})$. We have

$$\operatorname{div}(x - T) = pW - \mathfrak{m} \quad \text{and} \quad \operatorname{div}(y) = \operatorname{Tr} W - \frac{1}{p}(\deg f)\mathfrak{m},$$

where $\operatorname{Tr} W = \sum_\omega a_\omega(\omega, 0)$ denotes the 'trace' of W, the additive analogue of the weighted norm N. In other words, in our first interpretation W is a prime divisor in $\operatorname{Div} C_L$, while in the second interpretation it corresponds to a Galois-equivariant map $\Omega \to \operatorname{Div} C^{\mathrm{s}}$ sending ω to the prime divisor $(\omega, 0)$, the images of which have weighted sum $\operatorname{Tr} W \in \operatorname{Div} C$.

A divisor on C^{s} is called *good* if its support is disjoint from $\mathfrak{m} = \pi^*\infty$ and from the ramification points of π, i.e., disjoint from the support of $\operatorname{div}(y)$. This also means that the support is disjoint from the support of $\operatorname{div}(x - T)$. Let $\operatorname{Div}_\perp C^{\mathrm{s}}$ denote the group of good divisors on C^{s}, and set $\operatorname{Div}_\perp C = \mathrm{H}^0(\operatorname{Div}_\perp C^{\mathrm{s}})$. Every divisor class in $\operatorname{Pic} C^{\mathrm{s}}$ and $\operatorname{Pic}_{\mathfrak{m}} C^{\mathrm{s}}$ is represented by a good divisor. Let $\operatorname{Div}^0_\perp C^{\mathrm{s}}$, $\operatorname{Div}^0_\perp C$, $\operatorname{Div}^{(p)}_\perp C^{\mathrm{s}}$, and $\operatorname{Div}^{(p)}_\perp C$ denote the obvious groups. By the introductory remarks of this section, the function $x - T$ defines homomorphisms

$$(x - T)\colon \operatorname{Div}_\perp C \to L^* \quad \text{and} \quad (x - T)\colon \operatorname{Div}_\perp C^{\mathrm{s}} \to L^{\mathrm{s}*}.$$

We further define the map

$$\alpha\colon J_{\mathfrak{m}}[p] \to L^{\mathrm{s}*}, \qquad \mathcal{D} \mapsto \frac{(x - T)(D)}{h(W)},$$

where D is a good divisor representing the class $\mathcal{D}$, and where $h \in \kappa(C^{\mathrm{s}})$ is the unique function that is $1 \bmod \mathfrak{m}$ and satisfies $\operatorname{div}(h) = pD$. As before, $h(W)$ can be interpreted as the map $\omega \mapsto h((\omega, 0)) \in k^{\mathrm{s}*}$. Note that α is well-defined as for any representative D' of $\mathcal{D}$ there is a function $g \in \kappa(C^{\mathrm{s}})$ that is $1 \bmod \mathfrak{m}$ with $\operatorname{div}(g) = D' - D$, so that $\operatorname{div}(g^p h) = pD'$; by Weil reciprocity we have

$$\begin{aligned}\frac{(x - T)(D')}{(g^p h)(W)} &= \frac{(x - T)(\operatorname{div}(g) + D)}{g^p(W)h(W)} = \frac{g(\operatorname{div}(x - T))}{g(pW)} \cdot \frac{(x - T)(D)}{h(W)} \\ &= \frac{g(pW - \mathfrak{m})}{g(pW)} \cdot \frac{(x - T)(D)}{h(W)} \\ &= \frac{g(pW)g(\mathfrak{m})^{-1}}{g(pW)} \cdot \frac{(x - T)(D)}{h(W)} = \frac{(x - T)(D)}{h(W)},\end{aligned}$$

since $g(\mathfrak{m}) = 1$. We will see that α induces an isomorphism between M and the kernel of an endomorphism of $J_{\mathfrak{m}}$ that we now define.

The group μ_p acts on C and C^{s} by letting $\zeta \in \mu_p$ act as $(x, y) \mapsto (x, \zeta y)$. Linear extension gives a Galois-equivariant action on $\operatorname{Div} C^{\mathrm{s}}$ by the group ring $\mathbb{Z}[\mu_p]$. The element $t = \sum_{\zeta \in \mu_p} \zeta \in \mathbb{Z}[\mu_p]$ sends a point $Q \in C^{\mathrm{s}}(k^{\mathrm{s}})$ to the divisor $t(Q) = \pi^*(\pi Q)$, which is linearly equivalent to $\mathfrak{m}$. We conclude that t sends a divisor $D \in \operatorname{Div} C^{\mathrm{s}}$ to a divisor linearly equivalent to $(\deg D)\mathfrak{m}$, and

the subgroups $\mathrm{Div}^0 C^{\mathrm{s}}$ and $\mathrm{Div}^0_{\mathfrak{m}} C^{\mathrm{s}}$ to $\mathrm{Princ}\, C^{\mathrm{s}}$ and $\mathrm{Princ}_{\mathfrak{m}} C^{\mathrm{s}}$, respectively. This implies that the induced action of $\mathbb{Z}[\mu_p]$ on J, on $J_{\mathfrak{m}}$, on $\mathrm{Pic}^0 C$, and on $\mathrm{Pic}^0_{\mathfrak{m}} C$ factors through the quotient $\mathbb{Z}[\mu_p]/t$, which is isomorphic to the cyclotomic subring of k generated by μ_p.

Fix, once and for all, a primitive pth root of unity $\zeta \in \mu_p$, so that this cyclotomic ring is equal to $\mathbb{Z}[\zeta]$. Set

$$\phi = 1 - \zeta \quad \text{and} \quad \psi = -\sum_{i=1}^{p-1} i\zeta^i$$

and notice that $\phi\psi = p$. Note that this is slightly different from [PS], where ϕ and ψ are defined as elements of the group ring $\mathbb{Z}[\mu_p]$. Let $J_{\mathfrak{m}}[\phi]$ and $J[\phi]$ denote the kernels of the action of ϕ on $J_{\mathfrak{m}}(k^{\mathrm{s}})$ and $J(k^{\mathrm{s}})$, respectively.

PROPOSITION 4.1. *There is an isomorphism $\epsilon\colon J_{\mathfrak{m}}[\phi] \to M$ such that the homomorphism α is the composition of $\psi\colon J_{\mathfrak{m}}[p] \to J_{\mathfrak{m}}[\phi]$ and ϵ. Furthermore, ϵ induces an isomorphism $J[\phi] \to M/\mu_p$.*

Proof. This is extracted from [PS]. Let $\mathcal{J}_{\mathfrak{m}}[p]$ denote the p-torsion of the group $\mathrm{Pic}_{\mathfrak{m}} C^{\mathrm{s}}/\langle \mathfrak{m}' \rangle$, where $\mathfrak{m}'$ denotes the class of $\pi^* P$ for any $P \in \mathbb{A}^1(k) \subset \mathbb{P}^1(k)$. By [PS, Section 7] there is a pairing

$$e_p\colon \mathcal{J}_{\mathfrak{m}}[p] \times \mathcal{J}_{\mathfrak{m}}[p] \to \mu_p,$$

defined for a pair $(\mathcal{D}_1, \mathcal{D}_2)$ of classes, represented respectively by divisors D_1 and D_2 with disjoint support, to be

$$e_p(\mathcal{D}_1, \mathcal{D}_2) = (-1)^{d_1 d_2} \frac{h_2(D_1)}{h_1(D_2)},$$

where for $i = 1, 2$ we have $d_i = \deg D_i$, while $h_i \in \kappa(C^{\mathrm{s}})$ is the unique function such that $x^{-d_i} h_i$ is $1 \bmod \mathfrak{m}$ and $\mathrm{div}(h_i) = pD_i - d_i\mathfrak{m}$. Note that the group $J_{\mathfrak{m}}[p] \cong \mathrm{Pic}^0_{\mathfrak{m}}(C^{\mathrm{s}})[p]$ is a subgroup of $\mathcal{J}_{\mathfrak{m}}[p]$. By [PS, Section 6 and Prop. 7.1] there is an isomorphism $\epsilon\colon J_{\mathfrak{m}}[\phi] \to M$ such that $\epsilon(\psi\mathcal{D}) = e_p(\mathcal{D}, W)$ for all $\mathcal{D} \in J_{\mathfrak{m}}[p]$. Let the class $\mathcal{D} \in J_{\mathfrak{m}}[p]$ be represented by a good divisor D, automatically of degree $d_1 = 0$, and let $h \equiv 1 \bmod \mathfrak{m}$ be a function satisfying $\mathrm{div}(h) = pD$. Note that $x^{-1}(x - T)$ is $1 \bmod \mathfrak{m}$, so that we can take $x - T$ as the function corresponding to W in the definition of e_p. Therefore, we have

$$\epsilon(\psi\mathcal{D}) = e_p(\mathcal{D}, W) = (-1)^0 \frac{(x - T)(D)}{h(W)} = \alpha(\mathcal{D}),$$

which shows that α factors as claimed. For the fact that ϵ induces an isomorphism $J[\phi] \to M/\mu_p$, see [PS, Section 6]. ∎

As in [PS], we denote the isomorphisms $J_{\mathfrak{m}}[\phi] \to M$ and $J[\phi] \to M/\mu_p$ from Proposition 4.1 both by ϵ.

Next, we define the homomorphism

$$(\gamma y)\colon \operatorname{Div}_{\perp}^{(p)} C^{\mathrm{s}} \to k^{\mathrm{s}*}, \qquad \sum_P n_P(P) \mapsto c^{-\frac{1}{p}\sum n_P} \prod_P y(P)^{n_P},$$

where c is the leading coefficient of f as before. This map descends to a map $(\gamma y)\colon \operatorname{Div}_{\perp}^{(p)} C \to k^*$. The name (γy) comes from the fact that if we choose any pth root $\gamma \in k^{\mathrm{s}}$ of c^{-1}, then the map (γy) is the restriction to $\operatorname{Div}_{\perp}^{(p)} C^{\mathrm{s}}$ of evaluation of γy on $\operatorname{Div}_{\perp} C^{\mathrm{s}}$. On $\operatorname{Div}_{\perp}^{0} C^{\mathrm{s}}$ it is also induced by evaluation of y. Therefore, when appropriate, we may refer to the map (γy) as just y. We remark that

$$N(x-T) = \prod_{\omega} (x-\omega)^{a_\omega} = c^{-1} f(x) = c^{-1} y^p = (\gamma y)^p. \tag{4.1}$$

Our main result gives a cohomological interpretation of the combined map

$$(x-T, \gamma y)\colon \operatorname{Div}_{\perp}^{(p)} C^{\mathrm{s}} \to L^{\mathrm{s}*} \times k^{\mathrm{s}*}.$$

To this end, let ϵ_* denote the maps on cohomology induced by both maps ϵ. The short exact sequences

$$1 \to J_{\mathfrak{m}}[\phi] \to J_{\mathfrak{m}}(k^{\mathrm{s}}) \xrightarrow{\phi} J_{\mathfrak{m}}(k^{\mathrm{s}}) \to 1 \quad \text{and} \quad 1 \to J[\phi] \to J(k^{\mathrm{s}}) \xrightarrow{\phi} J(k^{\mathrm{s}}) \to 1$$

induce connecting maps $J_{\mathfrak{m}}(k) \to \mathrm{H}^1(J_{\mathfrak{m}}[\phi])$ and $J(k) \to \mathrm{H}^1(J[\phi])$ that we both denote by δ_ϕ.

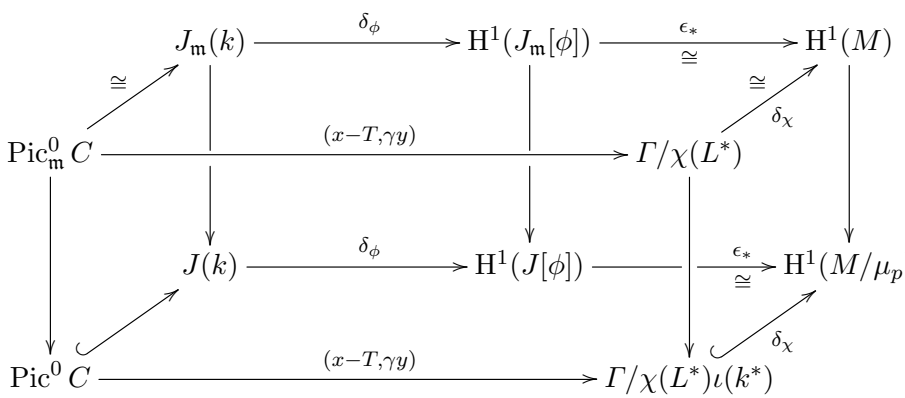
THEOREM 4.2. *The map*

$$(x-T, \gamma y)\colon \operatorname{Div}_{\perp}^{(p)} C^{\mathrm{s}} \to L^{\mathrm{s}*} \times k^{\mathrm{s}*}, \qquad D \mapsto ((x-T)(D), (\gamma y)(D)),$$

induces natural homomorphisms

$$\operatorname{Pic}_{\mathfrak{m}}^0 C \to \Gamma/\chi(L^*) \quad \textit{and} \quad \operatorname{Pic}^0 C \to \Gamma/\chi(L^*)\iota(k^*)$$

making the following diagram commutative:



Proof. For any good divisor $D = \sum_P n_P(P)$ of degree divisible by p we have, using (4.1),

$$N((x-T)(D)) = (N(x-T))(D) = (c^{-1}y^p)(D) = (\gamma y)(D)^p,$$

so $(x-T, \gamma y)$ induces a homomorphism $\mathrm{Div}_\perp^{(p)} C \to \Gamma$. Suppose $D \in \mathrm{Div}_\perp^0 C$ is principal, say $D = \mathrm{div}(h)$ for some $h \in \kappa(C)^*$. Then by Weil reciprocity we have

$$(x-T)(D) = (x-T)(\mathrm{div}(h)) = h(\mathrm{div}(x-T)) = h(pW-\mathfrak{m}) = h(W)^p \cdot h(\mathfrak{m})^{-1}$$

and

$$\begin{aligned}(\gamma y)(D) = y(\mathrm{div}(h)) = h(\mathrm{div}(y)) &= h\left(\mathrm{Tr}\, W - \frac{1}{p}(\deg f)\mathfrak{m}\right) \\ &= N(h(W)) \cdot h(\mathfrak{m})^{-(1/p)\deg f}.\end{aligned}$$

We therefore find

$$(x-T, \gamma y)(D) = \chi(h(W)) \cdot \iota(h(\mathfrak{m})^{-1}).$$

This is contained in $\chi(L^*)\iota(k^*)$ and if h is $1 \bmod \mathfrak{m}$ then in fact in $\chi(L^*)$. As every class in $\mathrm{Pic}^0 C$ and $\mathrm{Pic}^0_{\mathfrak{m}} C$ is represented by a good divisor, we obtain the claimed homomorphisms and see that the front face of the diagram commutes.

The commutativity of the right-side face follows from Proposition 3.1, while that of the back and left-side faces is obvious. For the top face, take any $\mathcal{D} \in \mathrm{Pic}^0_{\mathfrak{m}} C$, represented by a good divisor $D \in \mathrm{Div}^0_\perp C$, and choose a class $\mathcal{D}' \in \mathrm{Pic}^0_{\mathfrak{m}} C^{\mathrm{s}} \cong J_{\mathfrak{m}}(k^{\mathrm{s}})$ with $p\mathcal{D}' = \mathcal{D}$ and a good divisor $D' \in \mathrm{Div}^0_\perp C^{\mathrm{s}}$ representing $\mathcal{D}'$. Then $\phi(\psi\mathcal{D}') = p\mathcal{D}' = \mathcal{D}$, so $\delta_\phi(\mathcal{D})$ is represented by the cocycle that sends $\sigma \in G_k$ to $\sigma(\psi\mathcal{D}') - \psi\mathcal{D}' = \psi(\sigma(\mathcal{D}') - \mathcal{D}')$ and $\epsilon_*(\delta_\phi(\mathcal{D}))$ is represented by $\sigma \mapsto \epsilon(\psi(\sigma(\mathcal{D}') - \mathcal{D}'))$. Let h be a function that is $1 \bmod \mathfrak{m}$, satisfying

$$\mathrm{div}(h) = pD' - D,$$

so that $\mathrm{div}(\sigma(h)/h) = p(\sigma(D') - D')$. Therefore, by Proposition 4.1, the class $\epsilon_*(\delta_\phi(\mathcal{D}))$ is represented by the cocycle that sends σ to

$$\epsilon(\psi(\sigma(\mathcal{D}') - \mathcal{D}')) = \alpha(\sigma(\mathcal{D}') - \mathcal{D}') = \frac{(x-T)(\sigma(D') - D')}{(\sigma(h)/h)(W)} = \frac{\sigma(\theta)}{\theta}$$

for all $\sigma \in G_k$, with

$$\theta = \frac{(x-T)(D')}{h(W)}.$$

We now show that $\chi(\theta) = (\theta^p, N(\theta))$ equals $(x-T, \gamma y)(D)$. In the first component, we have

$$\theta^p = \frac{(x-T)(D')^p}{h(W)^p} = \frac{(x-T)(pD')}{h(pW)} = \frac{(x-T)(\operatorname{div}(h)+D)}{h\big(\operatorname{div}(x-T)+\frac{1}{p}(\deg f)\mathfrak{m}\big)}$$
$$= (x-T)(D)$$

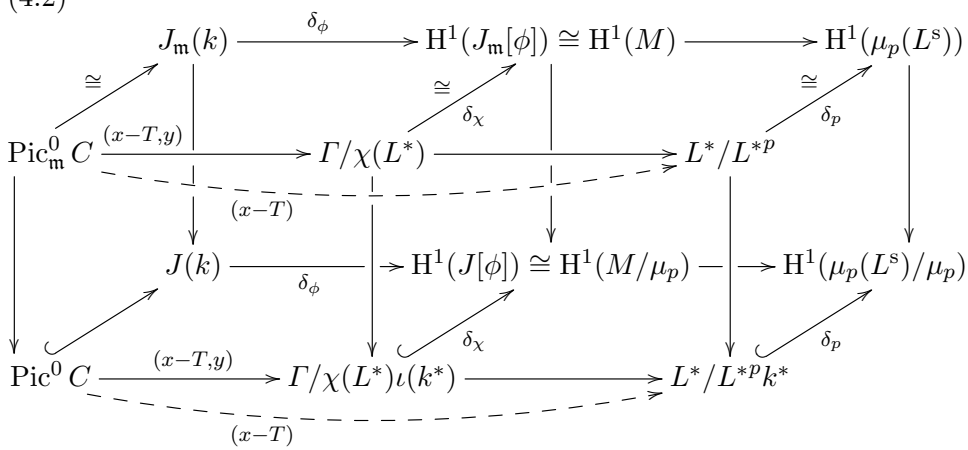
by Weil reciprocity and the fact that $h(\mathfrak{m}) = 1$. In the second component, we similarly have

$$N(\theta) = \frac{N\big((x-T)(D')\big)}{N(h(W))} = \frac{y(D')^p}{h(\operatorname{Tr} W)} = \frac{y(pD')}{h\big(\operatorname{div}(y)+\frac{1}{p}(\deg f)\mathfrak{m}\big)}$$
$$= \frac{y(\operatorname{div}(h)+D)}{h\big(\operatorname{div}(y)+\frac{1}{p}(\deg f)\mathfrak{m}\big)} = y(D).$$

This implies that $\delta_\chi((x-T,\gamma y)(\mathcal{D}))$ is represented by the cocycle $\sigma \mapsto \sigma(\theta)/\theta$ as well, so the top face of the diagram commutes indeed. Finally, commutativity of the bottom face of the diagram follows from commutativity of the other faces and the fact that the map $\operatorname{Pic}^0_{\mathfrak{m}} C \to \operatorname{Pic}^0 C$ is surjective. ∎

The diagrams of Proposition 3.1 and Theorem 4.2 combine to the following diagram:

(4.2)



The two compositions of the horizontal maps in the front face of this diagram, indicated by dashed arrows, are the $(x-T)$ maps that play a major role in [PS]. Indeed, if we replace the front face by the diagram

$$\begin{array}{ccc} \operatorname{Pic}^0_{\mathfrak{m}} C & \xrightarrow{(x-T)} & L^*/L^{*p} \\ \downarrow & & \downarrow \\ \operatorname{Pic}^0 C & \xrightarrow{(x-T)} & L^*/L^{*p}k^* \end{array}$$

then all information in this restricted diagram can already be found in [PS].

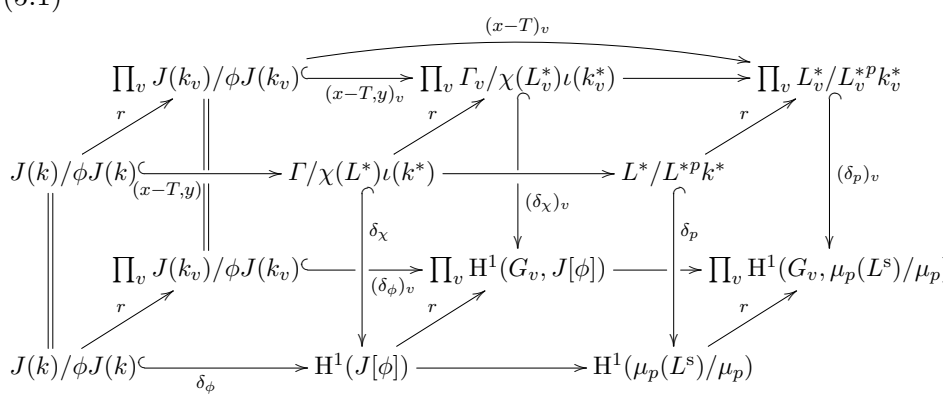
REMARK 4.3. As explained in [PS, Section 10], the group $\mathrm{Pic}^0 C$ is the largest subgroup of $J(k)$ whose image under the map $J(k) \to \mathrm{H}^1(\mu_p(L^{\mathrm{s}})/\mu_p)$ is contained in the image of $L^*/L^{*p}k^*$. Similarly, it is the largest subgroup whose image under $J(k) \to \mathrm{H}^1(J[\phi])$ is contained in the image of $\Gamma/\chi(L^*)\iota(k^*)$.

5. 'Unfaking' the fake Selmer group. In this section, we make the additional assumption that k is a global field. For each place v of k, we let k_v denote the completion at v, with absolute Galois group $G_v = \mathrm{Gal}(k_v^{\mathrm{s}}/k_v)$; we set $L_v = L \otimes_k k_v$ and

$$\Gamma_v = \{(\delta, n) \in L_v^* \times k_v^* \mid N(\delta) = n^p\}.$$

We also assume that for each place v of k, the curve C has a k_v-rational divisor class of degree 1. As mentioned in [PS, Section 13], this assumption is automatically satisfied when the genus $g(C) = (d-2)(p-1)/2$ satisfies $g(C) \not\equiv 1 \pmod{p}$. It implies that the injection $\mathrm{Pic}^0 C \to J(k)$ is an isomorphism (see [PS, Prop. 3.2 and 3.3]). As before, we will abbreviate the product over all places of k to $\prod_v$. The bottom face of diagram (4.2) then yields the front face of the following diagram, where, as before, we have identified $\mathrm{H}^1(J[\phi])$ with $\mathrm{H}^1(M/\mu_p)$:

(5.1)



For each map in this front face, there is an analogous map over each completion k_v of k. Taking the product over all places gives the back face of the diagram, while r denotes each map from a global group to the product of the analogous local groups.

The image of $J(k)/\phi J(k)$ in each of the four global groups is contained in the inverse image under r of the image of $\prod_v J(k_v)/\phi J(k_v)$ in the corresponding product of local groups. We give three of these inverse images a name:

$$\mathrm{Sel}^{\phi}(J,k) = r^{-1}\Big(\mathrm{im}\Big((\delta_\phi)_v\colon \prod_v J(k_v)/\phi J(k_v) \to \prod_v \mathrm{H}^1(G_v, J[\phi])\Big)\Big),$$

$$\mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k) = r^{-1}\Big(\mathrm{im}\Big((x-T)_v\colon \prod_v J(k_v)/\phi J(k_v) \to \prod_v L_v^*/L_v^{*p}k_v^*\Big)\Big),$$

$$\mathrm{Sel}^{\phi}_{\mathrm{explicit}}(J,k) = r^{-1}\Big(\mathrm{im}\Big((x-T,y)_v\colon \prod_v J(k_v)/\phi J(k_v) \to \prod_v \Gamma_v/\chi(L_v^*)\iota(k_v^*)\Big)\Big).$$

The *Selmer group* $\mathrm{Sel}^{\phi}(J,k)$ is commonly known. The *fake Selmer group* $\mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$ was introduced by Poonen and Schaefer in [PS]. The two groups are related by an exact sequence

$$\mu_p \to \mathrm{Sel}^{\phi}(J,k) \to \mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k) \to 0,$$

and it is also known when the first map is injective (see [PS, Thm. 13.2]). However, it is not always obvious whether the image of $J(k)/\phi J(k)$ in $\mathrm{Sel}^{\phi}(J,k)$ maps injectively to $\mathrm{Sel}^{\phi}_{\mathrm{fake}}(J,k)$. This means that although the fake Selmer group is more practical to work with explicitly, in doing so information may be lost. The following theorem shows that no information is lost when we work instead with the *explicit Selmer group* $\mathrm{Sel}^{\phi}_{\mathrm{explicit}}(J,k)$, which is just as easy to work with as the fake Selmer group.

THEOREM 5.1. *The map δ_χ induces an isomorphism*

$$\mathrm{Sel}^{\phi}_{\mathrm{explicit}}(J,k) \to \mathrm{Sel}^{\phi}(J,k).$$

Proof. The fact that δ_χ maps $\mathrm{Sel}^{\phi}_{\mathrm{explicit}}(J,k)$ injectively to $\mathrm{Sel}^{\phi}(J,k)$ is clear, so it remains to prove surjectivity. Note that we have an isomorphism $\mathrm{H}^2(\mu_p) \cong \mathrm{Br}(k)[p]$. Therefore, identifying $\mathrm{H}^1(J[\phi])$ with $\mathrm{H}^1(M/\mu_p)$ through ϵ_* as before, the long exact sequences associated to the vertical short exact sequences in diagram (3.1), together with the results of Proposition 3.1, give rise to a commutative diagram with exact columns:

$$\begin{array}{ccc}
\Gamma/\chi(L^*)\iota(k^*) & \longrightarrow & L^*/L^{*p}k^* \\
\big\downarrow{\scriptstyle \delta_\chi} & & \big\downarrow{\scriptstyle \delta_p} \\
H^1(J[\phi]) & \longrightarrow & H^1(\mu_p(L^{\mathrm{s}})/\mu_p) \\
\big\downarrow{\scriptstyle \delta_1} & & \big\downarrow{\scriptstyle \delta_2} \\
\mathrm{Br}(k)[p] & = & \mathrm{Br}(k)[p]
\end{array}$$

An analogous statement holds for every completion k_v of k. Now suppose we have an element $\xi \in \mathrm{Sel}^{\phi}(J,k)$. Then by definition $r(\xi)$ is contained in the image of $(\delta_\phi)_v$ and therefore in the image of $(\delta_\chi)_v$ (see diagram (5.1)). It follows that $r(\xi)$ maps to 0 in $\prod_v \mathrm{Br}(k_v)[p]$ under the product of the

local versions of δ_1. Since the map $\mathrm{Br}(k)[p] \to \prod_v \mathrm{Br}(k_v)[p]$ is injective, we conclude $\delta_1(\xi) = 0$, so there is an element $\eta \in \Gamma/\chi(L^*)\iota(k^*)$ with $\delta_\chi(\eta) = \xi$. A short diagram chase shows $\eta \in \mathrm{Sel}^\phi_{\mathrm{explicit}}(J,k)$, so $\delta_\chi\colon \mathrm{Sel}^\phi_{\mathrm{explicit}}(J,k) \to \mathrm{Sel}^\phi(J,k)$ is indeed surjective. ∎

Remark 5.2. Similarly, the map δ_p induces an isomorphism from $\mathrm{Sel}^\phi_{\mathrm{fake}}(J,k)$ to the group

$$r^{-1}\Big(\mathrm{im}\Big(\prod_v J(k_v)/\phi J(k_v) \to \prod_v \mathrm{H}^1(G_v, \mu_p(L^{\mathrm{s}})/\mu_p)\Big)\Big).$$

Proof of Theorem 1.1. The map $(x-T, y)\colon J(k) \to \Gamma/\chi(L^*)\iota(k^*)$ factors as

$$J(k) \to J(k)/\phi J(k) \to \mathrm{Sel}^\phi_{\mathrm{explicit}}(J,k) \subset \Gamma/\chi(L^*)\iota(k^*).$$

Theorem 1.1 therefore follows immediately from Theorem 5.1. ∎

References

[BPS] N. Bruin, B. Poonen, and M. Stoll, *Generalized explicit descent and its application to curves of genus 3*, arXiv:1205.4456v1.

[Ca1] J. W. S. Cassels, *The Mordell–Weil group of curves of genus 2*, in: Arithmetic and Geometry, Vol. I, Progr. Math., 35, Birkhäuser, Boston, 1983, 27–60.

[Ca2] J. W. S. Cassels, *Second descents for elliptic curves*, J. Reine Angew. Math. 494 (1998), 101–127.

[FTvL] E. V. Flynn, D. Testa and R. van Luijk, *Two-coverings of Jacobians of curves of genus 2*, Proc. London Math. Soc. (3) 104 (2012), 387–429.

[PS] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. 488 (1997), 141–188.

[ScSt] E. F. Schaefer and M. Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. 356 (2004), 1209–1231.

[Se] J.-P. Serre, *Local Fields*, Grad. Texts in Math. 67, Springer, New York, 1979.

Michael Stoll
Mathematisches Institut
Universität Bayreuth
95440 Bayreuth, Germany
E-mail: Michael.Stoll@uni-bayreuth.de

Ronald van Luijk
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA, Leiden, The Netherlands
E-mail: rvl@math.leidenuniv.nl

Received on 26.9.2012
and in revised form on 15.2.2013 (7207)