Cent. Eur. J. Math. • 11(12) • 2013 • 2138-2149
DOI: 10.2478/s11533-013-0319-4

VERSITA

Central European Journal of **Mathematics**

Effective lifting of 2-cocycles for Galois cohomology

Research Article

Thomas Preu[1]*

1 *Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190, 8057 Zürich, Switzerland*

Received 12 April 2012; accepted 25 March 2013

Abstract: We give explicit formulas for reducing the problem of determining whether a given 2-cocycle is a coboundary and if so finding a lifting 1-cochain to a system of norm equations.

MSC: 12G05

Keywords: Galois cohomology • Local invariants

© *Versita Sp. z o.o.*

1. Motivation and introduction

The vanishing of certain Galois cohomology groups of function fields and number fields, which are of interest in arithmetic geometry, is quite well established: e.g., there is Hilbert's Theorem 90 which gives the effective vanishing of $H^1(K/k, K^*)$ for any finite Galois extension, or Tsen's Theorem which when applicable implies the analogous vanishing of H^2. The goal is to provide effective and detailed versions of these results. We will describe the algorithms that will reduce the problem of exhibiting a cocycle explicitly as a coboundary if possible to solving norm equations. We are concerned specifically with the following problem.

Problem 1.1.
Given a finite group G and a G-module A, determine for an arbitrary cohomology class $[f] \in H^2(G, A)$ represented by an explicit 2-cocycle f of the standard cochain complex whether $[f] = 0$ and if so find a 1-cochain f' such that $\partial^1 f' = f$.

The analogous problem for r-cocycles (with $r \in \mathbb{N}$) will be denoted by 1.1_r. We prove

* *E-mail: preu@math.uzh.ch*

Theorem 1.2.
Let G be the Galois group of a finite Galois extension K/k and A the usual G-module $K^* = K\setminus\{0\}$, both effectively given. Then we can effectively reduce Problem 1.1 for G and A to solving norm equations $N_{\widetilde{K}/\widetilde{k}}(x) = a$ for cyclic intermediate field extensions $\widetilde{K}/\widetilde{k}$ and $a \in \widetilde{k}^*$.

There will be three sections devoted to reduction steps introducing well-known results and general tools. The first of them relates Problem 1.1 in the case G is cyclic to solving norm equations. The second reduces Problem 1.1 for a general G to the case of finite p-groups, for various prime numbers p. The last of them reduces Problem 1.1 for G solvable to cyclic groups (and is presented last since it uses ingredients of the other reduction steps). This section is the only one depending strongly on the special case of Galois cohomology, specifically Hilbert's Theorem 90. A final section summarizes results in the proof of Theorem 1.2. Additionally we show how to compute invariants in local fields explicitly, focusing on an application for number fields:

Proposition 1.3.
Let K/k be a finite Galois extension of number fields with Galois group Γ. Let v be a place of k and $f \in \mathrm{Map}(\Gamma^2, K^*)$ an explicitly given 2-cocycle. We can compute $\mathrm{inv}_v[f] \in \mathbb{Q}/\mathbb{Z}$ effectively.

We give an overview on the context of our results. In arithmetic geometry computing local invariants as in Proposition 1.3 is used in the Brauer–Manin obstruction. Example 4.4 is motivated by an instance of this setting in [9]. In [10] one finds an effective but rather indirect approach using the Hensel lifting on Brauer–Severi varieties. For the special case of Hilbert symbols there are explicit formulas based on convergent power series (cf. [12, V, (3.7) Theorem] or [3, VII]). Effective bounds for the rate of convergence in the case of Hilbert symbols of order p over $\mathbb{Q}_p$ can be found in [16] as conferred by a referee. Our Proposition 1.3 uses solubility of norm equations over local fields and is effective in full generality. Ramification in the associated Galois extensions increases only the precision needed in solutions of these norm equations and bounds for this can be read off from [3, III.1].

Another application is in minimizing representations as another referee pointed out. Recently Fieker in [5] gave an algorithm to solve this problem for number fields by reducing to Problem 1.1 and then solve S-unit equations. We give a comparison with our method in Remark 5.2.

The results of the following three sections are well known at least on the level of cohomology (cf. [2, 7] or [15]) and partially also on the level of representing complexes. We provide all of the rather involved formulas needed for algorithms on the level of complexes. In particular the formulas referred to in Corollary 2.2, and Propositions 3.3 and 4.1 have not been found by us in the literature. It is also well known that formulas such as presented here can be applied as they are in the last part. The author's contribution is to actually do so.

2. Some complexes: from cyclic groups to norm equations

Let G be a finite group and A a G-module, both effectively given, and denote the action of $g \in G$ on $a \in A$ by $g.a$. Recall that the "standard complex" in homogeneous form resolves the trivial G-module $\mathbb{Z}$ by the free G-modules $\mathbb{Z}\big[G^{r+1}\big]$ endowed with diagonal action given by $g.(g_0,\dots,g_r) = (gg_0,\dots,gg_r)$ (cf. [2, I.5]). Here and later on we omit the augmentation map to $\mathbb{Z}$:

$$SR = \mathbb{Z}\big[G^1\big] \xleftarrow{\partial_0} \mathbb{Z}\big[G^2\big] \xleftarrow{\partial_1} \mathbb{Z}\big[G^3\big] \xleftarrow{\partial_2} \dots,$$

$$\partial_r\colon \mathbb{Z}\big[G^{r+2}\big] \to \mathbb{Z}\big[G^{r+1}\big], \qquad (g_0,\dots,g_{r+1}) \mapsto \sum_{k=0}^{r+1} (-1)^k (g_0,\dots,g_{k-1},g_{k+1},\dots,g_{r+1}).$$

When $G = \langle \alpha \rangle$ is cyclic of order $n \in \mathbb{N}$ we will also use the "efficient complex" [2, I, (6.3)], where x_r serve as symbols to reference the position in the complex:

$$ER = \mathbb{Z}[G]x_0 \xleftarrow{d_0} \mathbb{Z}[G]x_1 \xleftarrow{d_1} \mathbb{Z}[G]x_2 \xleftarrow{d_2} \dots, \qquad d_r(gx_{r+1}) = \begin{cases} (g - g\alpha)x_r, & r \text{ even}, \\ \left(\sum_{i=0}^{n-1} g\alpha^i\right)x_r, & r \text{ odd}. \end{cases}$$

We give a quasi-isomorphism of these two complexes by specifying morphisms of chain complexes $\tau = (\tau_r)_{r=0}^{\infty} \colon ER \to SR$ and $\sigma = (\sigma_r)_{r=0}^{\infty} \colon SR \to ER$ and a chain homotopy $h = (h_r)_{r=1}^{\infty}$, satisfying $\sigma \circ \tau = \mathrm{id}$ and $\mathrm{id} - \tau_r \circ \sigma_r = h_r \circ \partial_{r-1} + \partial_r v \circ h_{r+1}$. The following diagram illustrates the situation:

$$\begin{array}{ccccccccc}
\mathbb{Z}[G^1] & \xleftarrow{\partial_0} & \mathbb{Z}[G^2] & \xleftarrow{\partial_1} & \mathbb{Z}[G^3] & \xleftarrow{\partial_2} & \mathbb{Z}[G^4] & \longleftarrow & \dots \\
\downarrow{\scriptstyle \sigma_0} & \searrow{\scriptstyle h_1} & \downarrow{\scriptstyle \sigma_1} & \searrow{\scriptstyle h_2} & \downarrow{\scriptstyle \sigma_2} & \searrow{\scriptstyle h_3} & \downarrow{\scriptstyle \sigma_3} & & \\
\mathbb{Z}[G]x_0 & \xleftarrow{d_0} & \mathbb{Z}[G]x_1 & \xleftarrow{d_1} & \mathbb{Z}[G]x_2 & \xleftarrow{d_2} & \mathbb{Z}[G]x_3 & \longleftarrow & \dots \\
\downarrow{\scriptstyle \tau_0} & \searrow & \downarrow{\scriptstyle \tau_1} & \searrow & \downarrow{\scriptstyle \tau_2} & \searrow & \downarrow{\scriptstyle \tau_3} & & \\
\mathbb{Z}[G^1] & \xleftarrow{\partial_0} & \mathbb{Z}[G^2] & \xleftarrow{\partial_1} & \mathbb{Z}[G^3] & \xleftarrow{\partial_2} & \mathbb{Z}[G^4] & \longleftarrow & \dots
\end{array} \tag{1}$$

Proposition 2.1.
For a finite cyclic group $G = \langle \alpha \rangle$ of order n we get a quasi-isomorphism as in (1),

$$\sigma_{2m}\left(e, \alpha^{i_1}, \alpha^{i_1+i_2}, \dots, \alpha^{i_1+i_2+\dots+i_{2m}}\right) = \begin{cases} (-1)^m e x_{2m} & \text{if } i_{2k-1} + i_{2k} \geq n \text{ for all } k, \\ 0 & \text{otherwise;} \end{cases}$$

$$\sigma_{2m+1}\left(e, \alpha^{i_1}, \alpha^{i_1+i_2}, \dots, \alpha^{i_1+i_2+\dots+i_{2m+1}}\right) = \begin{cases} (-1)^{m+1}\left(\sum_{j=0}^{i_1-1} \alpha^j\right) x_{2m+1} & \text{if } i_{2k} + i_{2k+1} \geq n \text{ for all } k, \\ 0 & \text{otherwise;} \end{cases}$$

$$\tau_{2m}(ex_{2m}) = (-1)^m \sum_{0 \leq i_1, i_2, \dots, i_m < n} \left(e, \alpha^{i_1}, \alpha^{1+i_1}, \alpha^{i_1+i_2}, \alpha^{1+i_1+i_2}, \dots, \alpha^{i_1+i_2+\dots+i_m}, \alpha^{1+i_1+i_2+\dots+i_m}\right);$$

$$\tau_{2m+1}(ex_{2m+1}) = (-1)^{m+1} \sum_{0 \leq i_1, i_2, \dots, i_m < n} \left(e, \alpha, \alpha^{i_1}, \alpha^{1+i_1}, \alpha^{i_1+i_2}, \alpha^{1+i_1+i_2}, \dots, \alpha^{i_1+i_2+\dots+i_m}, \alpha^{1+i_1+i_2+\dots+i_m}\right);$$

$$h_1(e) = -(e, e); \qquad h_2(e, \alpha^{i_1}) = \left(e, \alpha^{i_1}, \alpha^{i_1}\right) - \sum_{j=0}^{i_1-1} \left(e, \alpha^j, \alpha^{j+1}\right);$$

$$h_k\left(e, \alpha^{i_1}, \alpha^{i_1+i_2}, \dots, \alpha^{i_1+\dots+i_{k-1}}\right) = (-1)^k \left(\left(e, \alpha^{i_1}, \dots, \alpha^{i_1+\dots+i_{k-1}}, \alpha^{i_1+\dots+i_{k-1}}\right) - \sum_{j=i_1+\dots+i_{k-2}}^{i_1+\dots+i_{k-1}-1} \left(e, \alpha^{i_1}, \dots, \alpha^{i_1+\dots+i_{k-2}}, \alpha^j, \alpha^{j+1}\right) \right)$$
$$+ \begin{cases} \sum_{j=0}^{n-1} \left(h_{k-2}\left(e, \dots, \alpha^{i_1+\dots+i_{k-3}}\right), \alpha^j, \alpha^{j+1}\right) & \text{if } i_{k-2} + i_{k-1} \geq n, \\ 0 & \text{otherwise,} \end{cases} \qquad k \geq 3.$$

Proof. It follows by induction on r that $(\sigma_r)_{r=0}^{\infty}$ is a chain map. It is then a straightforward exercise to check that $\sigma_r \circ \tau_r = \mathrm{id}$ and verify the other properties of a quasi-isomorphism. □

By applying the functor $\mathrm{Hom}_{\mathbb{Z}[G]}(\cdot, A)$ we get complexes whose homology is the group cohomology $H^r(G,A)$ of G with coefficients in A. We identify $\mathrm{Hom}_{\mathbb{Z}[G]}\left(\mathbb{Z}\left[G^{r+1}\right], A\right)$ with $\mathrm{Map}\left(G^r, A\right)$ (cf. [7, VI.13]) and get

$$\mathrm{Map}\left(G^0,A\right) \xrightarrow{\partial^0} \mathrm{Map}\left(G^1,A\right) \xrightarrow{\partial^1} \mathrm{Map}\left(G^2,A\right) \xrightarrow{\partial^2} \dots, \tag{2}$$
$$(\partial^r f)(g_1,\dots,g_{r+1}) = g_1.\left(f(g_2,\dots,g_{r+1})\right) + \sum_{k=1}^{r}(-1)^k f(g_2,\dots,g_kg_{k+1},\dots,g_{r+1}) + (-1)^{r+1} f(g_1,\dots,g_r).$$

For $G = \langle\alpha\rangle$ cyclic we identify $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A)$ with A to get from the efficient complex

$$Ax^0 \xrightarrow{d^0} Ax^1 \xrightarrow{d^1} Ax^2 \xrightarrow{d^2} \dots, \qquad d^r(ax^r) = \begin{cases} (a-\alpha.a)x^{r+1} = (\Delta(a))x^{r+1}, & r \text{ even}, \\ \left(\sum_{i=0}^{n-1}\alpha^i.a\right)x^{r+1} = (N(a))x^{r+1}, & r \text{ odd}. \end{cases}$$

We call Δ a difference map and N a norm map – they depend on the cyclic group and its given generator. An equation of the form $N(x) = a$, resp. $\Delta(x) = a$, is called a norm equation, resp. a difference equation, where x is the unknown and a is given. Note that $\ker d^2 = \ker\Delta = A^G \subset A$ where A^G denotes the G-invariants of A.

We get a quasi-isomorphism given by $(\tau^r)_{r=0}^{\infty}$ and $(\sigma^r)_{r=0}^{\infty}$, and a homotopy $(h^r)_{r=1}^{\infty}$ from $(\mathrm{id})_{r=0}^{\infty}$ to $(\sigma^r\circ\tau^r)_{r=0}^{\infty}$.

Corollary 2.2.

Let $G = \langle\alpha\rangle$ be a finite cyclic group of order n and $f \in \mathrm{Map}\left(G^2,A\right)$ a 2-cocycle for the G-module A. Via τ^2 we get $a = -\sum_{j=0}^{n-1} f(\alpha^j,\alpha) \in A^G$. Then f is a coboundary if and only if a lies in the image of the norm map. Furthermore if $a = N(a')$ we get a 1-cochain satisfying $\partial^1 f' = f$ which is given by

$$f'(\alpha^i) = \left(\sigma^1(a') + h^2(f)\right)(\alpha^i) = f(\alpha^i,e) - \sum_{j=0}^{i-1}\left(f(\alpha^j,\alpha) + \alpha^j.a'\right).$$

In this way, Problem 1.1 for cyclic groups is reduced to solving norm equations.

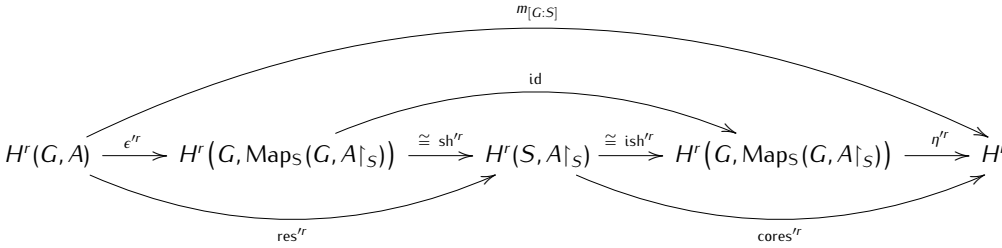
3. Shapiro's lemma, restriction and corestriction map: from general finite groups to p-groups

This section is mainly based on ideas in [15, Chapter 2]. For this section fix $r \in \mathbb{N}_0$. We give a solution to the following problem, and use it to reduce Problem 1.1_r for general G to Problem 1.1_r for p-groups for the primes p dividing the order of G. We consider the following intermediate task.

Problem 3.1.

Given a finite group G, a G-module A and a subgroup $S < G$ such that Problem 1.1_r is solvable for S. Denote by $A{\restriction}_S$ the S-module which is the restriction of A. Decide for a given r-cocycle f for the standard complex for A if the restriction of $[f]$ to $H^r(S, A{\restriction}_S)$ vanishes, and if so, exhibit explicitly an $(r-1)$-cochain $f' \in \mathrm{Map}\left(G^{r-1},A\right)$ such that $\partial^{r-1}f' = [G:S]f$, where $[G:S]$ denotes the index of S in G.

To make it easier for the reader to put the following pieces into an organized bigger picture, here is a commutative diagram, on which we elaborate afterwards:



(3)

These maps depend on S. Later we indicate this by a subscript S. For an S-module B we have a G-module:

$$\mathrm{Map}_S(G,B) = \big\{f \in \mathrm{Map}(G,B) : f(sg) = s.f(g) \text{ for all } g \in G,\ s \in S\big\};$$
$$(g.f)\colon G \to B, \qquad g' \mapsto f(g'g) \qquad \text{for all} \quad g \in G, \quad f \in \mathrm{Map}_S(G,B).$$

In the notation of [15, p. 27] we have $\pi^*_{S\to G}A = A{\restriction}_S$ and $\pi_{*S\to G}B = \mathrm{Map}_S(G,B)$, but we will use the more descriptive notation instead. Let $T \subset G$ be a set of right coset representatives for S. According to [15, p. 29] we get a monomorphism ϵ and an epimorphism η of G-modules:

$$\epsilon\colon A \to \mathrm{Map}_S(G,A{\restriction}_S), \qquad a \mapsto f\colon G \to A{\restriction}_S, \qquad g \mapsto g.a;$$
$$\eta\colon \mathrm{Map}_S(G,A{\restriction}_S) \to A, \qquad f \mapsto \sum_{t\in T} t^{-1}.f(t).$$

Note the use of left cosets in [15, p. 34] for contrast. The map η is independent of the choice of coset representatives T. Denoting the multiplication by $[G:S]$-map on a G-module by $m_{[G:S]}$, we have $\eta\circ\epsilon = m_{[G:S]}$. The morphisms η and ϵ induce morphisms on cochain complexes, respectively on cohomology groups, which we will indicate, e.g., by η^r, respectively η'^r, and satisfy

$$\eta^i \circ \epsilon^i = m_{[G:S]}. \tag{4}$$

We explain sh'^r and ish'^r in the following notation. For $\mathfrak{g} = (g', g_1, \dots, g_r) \in G^{r+1}$, define $\mathfrak{s} = (s_0, s_1, \dots, s_r) \in S^{r+1}$ and $\mathfrak{t} = (t_0, t_1, \dots, t_r) \in T^{r+1}$ by the condition below and define $\widetilde{s}_i$ and $\widetilde{t}_i$ in the same way for $(\widetilde{g}', \widetilde{g}_1, \dots, \widetilde{g}_r) \in G^{r+1}$:

$$g' = s_0 t_0 \qquad \text{and} \qquad t_{i-1} g_i = s_i t_i \qquad \text{for all} \quad i \in \{1, \dots, r\}.$$

The complexes we use below will all be derived from the standard resolution for G, respectively S. The situation is similar to the dual of (1). The name sh^i is reminiscent of the fact that these morphisms induce the isomorphisms of Shapiro's lemma on the level of cohomology groups and the ish^i induce the "inverse Shapiro isomorphisms", cf. [15, p. 31]. For the moment we will work with a general S-module B, though later we will take this to be $A{\restriction}_S$.

Proposition 3.2.

Define $(\mathrm{sh}^i)_{i=0}^\infty$, $(\mathrm{ish}^i)_{i=0}^\infty$ *and* $(k^i)_{i=1}^\infty$ *as follows:*

$$\mathrm{sh}^i\colon \mathrm{Map}\big(G^i, \mathrm{Map}_S(G,B)\big) \to \mathrm{Map}\big(S^i, B\big), \qquad \mathrm{sh}^i f = \big(S^i \to B,\ (g_1, \dots, g_i) \mapsto f_{(g_1,\dots,g_i)}(e)\big);$$
$$\mathrm{ish}^i\colon \mathrm{Map}(S^i, B) \to \mathrm{Map}\big(G^i, \mathrm{Map}_S(G,B)\big), \qquad \big(\mathrm{ish}^i f'\big)_{(g_1,\dots,g_i)} = \big(G \to B,\ g' \mapsto s_0.\big(f'(s_1, \dots, s_i)\big)\big);$$
$$k^i\colon \mathrm{Map}\big(G^i, \mathrm{Map}_S(G,B)\big) \to \mathrm{Map}\big(G^{i-1}, \mathrm{Map}_S(G,B)\big),$$
$$(k^i(f))_{(\widetilde{g}_1,\dots,\widetilde{g}_{i-1})} = \left(G \to B,\ \widetilde{g}' \mapsto \sum_{j=0}^{i-1} (-1)^j \widetilde{s}_0.\left(f_{(\widetilde{s}_1,\dots,\widetilde{s}_j,\widetilde{t}_j,\widetilde{g}_{j+1},\dots,\widetilde{g}_{i-1})}(e)\right)\right).$$

Then $(\mathrm{sh}^i)_{i=0}^\infty$ *and* $(\mathrm{ish}^i)_{i=0}^\infty$ *are quasi-isomorphisms via the homotopy* $(k^i)_{i=1}^\infty$ *from* $(\mathrm{id})_{i=0}^\infty$ *to* $(\mathrm{ish}^i \circ \mathrm{sh}^i)_{i=0}^\infty$*:*

$$\mathrm{id} - \mathrm{ish}^i \circ \mathrm{sh}^i = k^{i+1}\circ\partial^i + \partial^{i-1}\circ k^i, \tag{5}$$
$$\mathrm{id} = \mathrm{sh}^i \circ \mathrm{ish}^i. \tag{6}$$

Proof. One checks (5) and (6) by straightforward calculations. □

We remark that the definition of the k^i is inspired by [11, Lemma III.2.1].

The lower part of diagram (3) is just mentioned for completeness. The restriction map res'^r and corestriction cores'^r (called transfer in [15]) are defined to be the compositions $\mathrm{sh}'^r \circ \epsilon'^r$ and $\eta'^r \circ \mathrm{ish}'^r$ respectively; this is in accordance with [15]. Working with the refined factorization $m_{[G:S]} = \eta'^r \circ \mathrm{ish}'^r \circ \mathrm{sh}'^r \circ \epsilon'^r$ rather than the wellknown $m_{[G:S]} = \mathrm{res}'^r \circ \mathrm{cores}'^r$ allows us to apply the homotopy k^r to get explicit formulas for lifting cocycles.

Keep in mind, that $\eta^r, \mathrm{ish}^r, \mathrm{sh}^r, \epsilon^r$ form morphisms of complexes, i.e., we have $\eta^r \circ \partial^{r-1} = \partial^{r-1} \circ \eta^{r-1}$, etc.

For a given r-cocycle f of Problem 3.1 we have: $\mathrm{res}'^r[f] = [\mathrm{sh}^r \circ \epsilon^r f]$. By assumption we can check liftability of $\mathrm{sh}^r \circ \epsilon^r f$ and if so determine a lift $\widetilde{f} \in \mathrm{Map}\left(S^{r-1}, A\restriction_S\right)$ such that $\partial^{r-1}\widetilde{f} = \mathrm{sh}^r \circ \epsilon^r f$. For such an $\widetilde{f}$ we combine $\partial^r f = 0$, (4) and (5) to get

$$\begin{aligned}\partial^{r-1} \circ \eta^{r-1} \circ \mathrm{ish}^{r-1}\widetilde{f} &= \eta^r \circ \mathrm{ish}^r \circ \partial^{r-1}\widetilde{f} + \eta^r \circ k^{r+1} \circ \epsilon^{r+1} \circ \partial^r f = \eta^r \circ \left(\mathrm{ish}^r \circ \mathrm{sh}^r + k^{r+1} \circ \partial^r\right) \circ \epsilon^r f \\ &= \eta^r \circ \left(\mathrm{id} - \partial^{r-1} \circ k^r\right) \circ \epsilon^r f = [G:S]f - \partial^{r-1} \circ \eta^{r-1} \circ k^r \circ \epsilon^r f\end{aligned}$$

and so $f' = \eta^{r-1}\left(\mathrm{ish}^{r-1}\widetilde{f} + k^r(\epsilon^r f)\right)$ solves Problem 3.1. Summarizing, we have for $r = 2$,

Proposition 3.3.

Let G be a finite group, $S < G$ a subgroup with a set of right coset representatives T and $f \in \mathrm{Map}\left(G^2, A\right)$ a 2-cocycle. Let $\mathrm{res}^2_S f \colon S^2 \to A\restriction_S, (s_1, s_2) \mapsto f(s_1, s_2)$ denote the restricted 2-cocycle for S. Define auxiliary functions $\mathfrak{s} \colon G \to S$ and $\mathfrak{t} \colon G \to T$ by requiring $\mathfrak{s}(g)\mathfrak{t}(g) = g$. Then if $\mathrm{res}^2_S f$ is a 2-coboundary such that $\partial\widetilde{f} = \mathrm{res}^2_S f$ for $\widetilde{f} \in \mathrm{Map}(S, A\restriction_S)$ we get a 1-cochain f' satisfying $\partial^1 f' = [G:S]f$, defined by

$$f' \colon G \to A, \qquad g \mapsto \sum_{t \in T} t^{-1}.\left(\widetilde{f}(\mathfrak{s}(tg)) + f(t, g) - f(\mathfrak{s}(tg), \mathfrak{t}(tg))\right).$$

Corollary 3.4.

Let G be a finite group, $f \in \mathrm{Map}\left(G^2, A\right)$ a 2-cocycle and $|G| = \prod_{i=1}^u p_i^{q_i}$ a prime factorization. We can effectively reduce Problem 1.1 to Problem 1.1 for p_i-Sylow subgroups $S_i < G$, $A\restriction_{S_i}$ and restrictions $\mathrm{res}^2_{S_i} f \in \mathrm{Map}\left(S_i^2, A\restriction_{S_i}\right)$.

Proof. As $\mathrm{res}'^2_{S_i}$ is a group homomorphism it is clear that $[f] = 0$ implies $\left[\mathrm{res}^2_{S_i} f\right] = 0$ for all i. Assume we are given $r_i \in \mathrm{Map}\left(S_i, A\restriction_{S_i}\right)$ with $\partial^1 r_i = \mathrm{res}^2_{S_i} f$. Set $\widetilde{p}_i = |G|/p_i^{q_i} = [G:S_i]$ and choose $\widehat{p}_1, \ldots, \widehat{p}_u \in \mathbb{Z}$ such that $\sum_{i=1}^u \widehat{p}_i\widetilde{p}_i = 1$ (Chinese Remainder Theorem). By Proposition 3.3 we get $f_i \in \mathrm{Map}(G, A)$ such that $\partial^1 f_i = \widetilde{p}_i f$. If we set $f' = \sum_{i=1}^u \widehat{p}_i f_i'$ we have $\partial^1 f' = \sum_{i=1}^u \widehat{p}_i\widetilde{p}_i f = f$, thus $[f] = 0$ effectively. □

There are obvious analogs for $r \neq 2$. Formulas will get more complicated but are valid when accordingly modified.

4. LHS spectral sequence: from solvable groups to cyclic groups

Suppose we have $H \triangleleft G$ a (non-trivial) normal subgroup and set $Q = G/H$. We will denote elements of Q by $q = [g] = gH$, where $g \in G$ is a representative. The Lyndon–Hochschild–Serre (LHS) spectral sequence (cf. [7, VIII, Theorem 9.5]) will be denoted by $E = (E_s^{p,q})$ and is convergent: $E_2^{p,q} = H^p\left(Q, H^q(H, A)\right)$ implies $H^{p+q}(G, A)$.

There is the following G-action on $\mathrm{Map}\left(G^{i+1}, A\right)$ inducing a G-action on $\mathrm{Map}\left(G^{i+1}, A\right)^H$:

$$(g.f) \colon G^{i+1} \to A, \qquad (g_0, \ldots, g_i) \mapsto g.\left(f\left(g^{-1}g_0, \ldots, g^{-1}g_i\right)\right) \qquad \text{for all} \quad g \in G, \quad f \in \mathrm{Map}\left(G^{i+1}, A\right).$$

By H-invariance the G-action on $\mathrm{Map}\left(G^{i+1}, A\right)^H$ gives rise to a Q-action.

By first vertically forming the standard resolution for the G-module A, then taking H-invariants, which yields a complex of Q-modules as described in the last paragraph, we may resolve each term horizontally, then take Q-invariants and get E_0 as in (7). The differentials are induced by the differentials of the standard resolutions and a $(-1)^i$-factor is added to $d_0^{j,i}$ to ensure anticommutativity of the bicomplex:

$$\begin{array}{ccccccc}
 & \vdots & & \vdots & & \vdots & \\
 & \uparrow{\scriptstyle \partial_0^{0,2}} & & \uparrow{\scriptstyle \partial_0^{1,2}} & & \uparrow{\scriptstyle \partial_0^{2,2}} & \\
\mathrm{Map}\left(Q^0, \mathrm{Map}\left(G^3, A\right)^H\right) & \xrightarrow{d_0^{0,2}} & \mathrm{Map}\left(Q^1, \mathrm{Map}\left(G^3, A\right)^H\right) & \xrightarrow{d_0^{1,2}} & \mathrm{Map}\left(Q^2, \mathrm{Map}\left(G^3, A\right)^H\right) & \xrightarrow{d_0^{2,2}} & \cdots \\
\uparrow{\scriptstyle \partial_0^{0,1}} & & \uparrow{\scriptstyle \partial_0^{1,1}} & & \uparrow{\scriptstyle \partial_0^{2,1}} & & \\
\mathrm{Map}\left(Q^0, \mathrm{Map}\left(G^2, A\right)^H\right) & \xrightarrow{d_0^{0,1}} & \mathrm{Map}\left(Q^1, \mathrm{Map}\left(G^2, A\right)^H\right) & \xrightarrow{d_0^{1,1}} & \mathrm{Map}\left(Q^2, \mathrm{Map}\left(G^2, A\right)^H\right) & \xrightarrow{d_0^{2,1}} & \cdots \\
\uparrow{\scriptstyle \partial_0^{0,0}} & & \uparrow{\scriptstyle \partial_0^{1,0}} & & \uparrow{\scriptstyle \partial_0^{2,0}} & & \\
\mathrm{Map}\left(Q^0, \mathrm{Map}\left(G^1, A\right)^H\right) & \xrightarrow{d_0^{0,0}} & \mathrm{Map}\left(Q^1, \mathrm{Map}\left(G^1, A\right)^H\right) & \xrightarrow{d_0^{1,0}} & \mathrm{Map}\left(Q^2, \mathrm{Map}\left(G^1, A\right)^H\right) & \xrightarrow{d_0^{2,0}} & \cdots
\end{array} \tag{7}$$

One proves that $\ker d_0^{j+1,i} = \operatorname{im} d_0^{j,i}$, i.e., $\mathrm{Map}\left(G^{i+1}, A\right)^H$ are acyclic Q-modules, using Proposition 3.2 for $\{1_Q\} < Q$ componentwise in the $|G^i|$ components after applying the following morphism in all $|Q^j|$ components:

$$\mathrm{Map}\left(Q \times G^i, A\right) \xrightarrow{\sim} \mathrm{Map}\left(G^{i+1}, A\right)^H, \qquad f \mapsto \left(G^{i+1} \to A,\ (g_0, \ldots, g_i) \mapsto g_0.f\left(\left[g_0^{-1}\right], g_0^{-1}g_1, \ldots, g_{i-1}^{-1}g_i\right)\right).$$

For example, for $i = j = 0$, given $f\colon Q^1 \to \mathrm{Map}\left(G^1, A\right)^H$, $q \mapsto f_{(q)}$, satisfying $d_0^{1,0}(f) = 0$, we get

$$\widetilde{f}\colon Q^0 \to \mathrm{Map}\left(G^1, A\right)^H, \qquad (\,) \mapsto \left(G \to A,\ g \mapsto g.f_{(\left[g^{-1}\right])}(e)\right)$$

such that $d_0^{0,0}\widetilde{f} = f$. This induces a map from $\ker d_0^{1,0}$ to $\mathrm{Map}\left(Q^0, \mathrm{Map}\left(G^1, A\right)^H\right)$ denoted by ϕ.

The limiting term of the spectral sequence is the cohomology of the associated total complex. Since $\mathrm{Map}\left(G^{i+1}, A\right)^H$ are acyclic the total complex is quasi-isomorphic to the complex given by the abelian groups $\left(\mathrm{Map}\left(G^{i+1}, A\right)^H\right)^Q = \mathrm{Map}\left(G^{i+1}, A\right)^G \cong \mathrm{Map}\left(G^i, A\right)$, i.e., to the complex (2) that computes $H^*(G, A)$. Therefore we can represent a cohomology class $[f] \in H^p(G, A)$ as follows:

$$\mathrm{Map}(G^p, A) \to \bigoplus_{j+i=p} \mathrm{Map}\left(Q^j, \mathrm{Map}\left(G^{i+1}, A\right)^H\right),$$
$$f \mapsto \left(f'\colon Q^0 \to \mathrm{Map}\left(G^{p+1}, A\right)^H,\ (\,) \mapsto G^{p+1} \to A,\ (g_0, \ldots, g_p) \mapsto g_0.f\left(g_0^{-1}g_1, \ldots, g_{p-1}^{-1}g_p\right),\ 0, \ldots, 0\right).$$

This map gives an isomorphism onto the subgroup $\left(\ker d_0^{0,p}\right) \oplus \bigoplus_{j+i=p, j\neq 0} 0$. Call this isomorphism ψ for $p = 1$ and ω for $p = 2$. For an $[f] \in H^2(G, A)$ define $(\alpha, 0, 0) = \omega(f)$. A map $H^2(G, A) \to H^2(H, A{\restriction_H})^Q$ is given on the cocycle level by $f \mapsto \mathrm{sh}^2\,\alpha_{(\,)}$ where sh^2 is Shapiro's morphism in the situation $H < G$ for the H-module $A{\restriction_H}$. Here we needed to regard $\alpha_{(\,)}$ as an element of $\mathrm{Map}\left(G^2, \mathrm{Map}_H(G, A{\restriction_H})\right)$ via

$$\chi^i\colon \mathrm{Map}\left(G^{i+1}, A\right)^H \xrightarrow{\sim} \mathrm{Map}\left(G^i, \mathrm{Map}_H(G, A{\restriction_H})\right),$$
$$f \mapsto \left(G^i \to \mathrm{Map}_H(G, A{\restriction_H}),\ (g_1, \ldots, g_i) \mapsto \left(G \to A{\restriction_H},\ g' \mapsto f(g', g'g_1, \ldots, g'g_1 \cdots g_i)\right)\right).$$

Proposition 4.1.
Let G be a finite group, A a G-module, $H \triangleleft G$ a normal subgroup and $Q = G/H$ the quotient group. Assume that:

1. *we have an algorithm to solve Problem 1.1 for the groups H, Q and modules $A\restriction_H$, respectively A^H,*
2. *we have $H^1(H, A\restriction_H) = 0$ effectively, i.e. an algorithm for producing for a given 1-cocycle a lifting 0-cochain.*

Then we can solve Problem 1.1 for G and A.

Proof. We give explicit formulas and leave checking to the reader. Let $f \in \mathrm{Map}\left(G^2, A\right)$ be a 2-cocycle as above. A necessary condition for $[f] = 0$ is $\left[\mathrm{sh}^2 \alpha_{(\,)}\right] = 0$ (Shapiro's situation as just before the proposition), where $(\alpha, 0, 0) = \omega(f)$. Assuming this, there is a 1-cochain $\widetilde{\delta}' \colon H \to A$ such that $\partial^1 \widetilde{\delta}' = \mathrm{sh}^2 \alpha_{(\,)}$, which can be found effectively by assumption 1. Define δ' satisfying $\partial_0^{0,1} \delta' = \alpha$ by

$$\delta' \colon Q^0 \to \mathrm{Map}\left(G^2, A\right)^H, \qquad (\,) \mapsto k^2 \alpha_{(\,)} + \mathrm{ish}^1 \widetilde{\delta}',$$

and set $\beta' = d_0^{0,1} \delta'$. By assumption 2., for each $q \in Q$ we get $\widetilde{\epsilon}''_{(q)} \in \mathrm{Map}\left(H^0, A\restriction_H\right)$ satisfying $\mathrm{sh}^1 \beta'_{(q)} = \partial^0 \widetilde{\epsilon}''_{(q)}$ and we set

$$\epsilon''_{(q)} = k^1 \beta'_{(q)} + \mathrm{ish}^0 \widetilde{\epsilon}''_{(q)}$$

for all q. Now define $\gamma'' = d_0^{1,0} \epsilon''$. Each $\gamma''_{(p_1,p_2)}$ has to be a constant map, so we get $\widetilde{\gamma}'' \in \mathrm{Map}\left(Q^2, A^H\right)$ where $\widetilde{\gamma}''_{(p_1,p_2)} = \gamma''_{(p_1,p_2)}(e) \in A^H$. By assumption 1. we can test if $\left[\widetilde{\gamma}''\right] = 0 \in H^2\left(Q, A^H\right)$. If not, then f is not a coboundary; this uses assumption 2. and the exact sequence in low degree terms of the LHS spectral sequence:

$$0 = H^1(H, A\restriction_H)^Q \to H^2\left(Q, A^H\right) \to \ker\left(H^2(G, A) \to H^2(H, A\restriction_H)^Q\right) \to H^1\left(Q, H^1(H, A\restriction_H)\right) = 0.$$

Otherwise we find $\widetilde{\epsilon}''' \in \mathrm{Map}\left(Q^1, A^H\right)$ which lifts $\widetilde{\gamma}''$. By regarding elements of A^H as constant maps in $\mathrm{Map}\left(G^1, A\right)^H$ we get an induced map

$$\epsilon''' \in \mathrm{Map}\left(Q^1, \mathrm{Map}\left(G^1, A\right)^H\right).$$

In summary, either we have $[f] \neq 0$ or we found $\delta = \delta' - \partial_0^{0,0} \phi(-\epsilon'' + \epsilon''') \in \ker d_0^{0,1}$ satisfying $\partial_0^{0,1} \delta = \alpha$. So we may apply the inverse of ψ to get a 1-cochain $f' \in \mathrm{Map}\left(G^1, A\right)$ that finally satisfies $\partial^1 f' = f$. Since every step is explicitly given this shows the effectivity of the procedure. □

Corollary 4.2.
Let G be the Galois group of a solvable finite field extension K/k and $A = K^* = K \setminus \{0\}$ the usual G-module. Then we can effectively reduce solving Problem 1.1 for G and A to solving Problem 1.1 for cyclic groups and associated group modules which arise from intermediate field extensions of K/k.

Proof. Since the statement is clearly true for cyclic groups we may use induction on the size of the Galois group. As G is solvable it has a normal subgroup H with abelian quotient Q and we may assume Q to be non-trivial cyclic. To H corresponds the Galois extension K/K^H, and $A\restriction_H$ is still K^*. To Q corresponds the cyclic Galois extension K^H/k and $A^H = \left(K^H\right)^*$.

By induction assumption 1. of Proposition 4.1 is satisfied and assumption 2. is satisfied by Hilbert's Theorem 90, and usual proofs (e.g., [15, p. 94]) give $H^1(H, A\restriction_H) = 0$ effectively. The above proposition now establishes the corollary. □

Remark 4.3.
In Corollary 4.2 one could replace cyclic by cyclic of prime order. Proposition 4.1 generalizes to higher $H^r(G, A)$ assuming effective vanishing of $H^i(H, A\restriction_H)$ for $0 < i < r$.

Example 4.4.

In the case G is a dihedral group of order $2n$, Corollary 4.2 translates into a simple procedure for solving Problem 1.1. Suppose that G is generated by elements g and h satisfying $g^n = h^2 = (gh)^2 = e$. In [9, Proposition 5] we find an efficient resolution whose initial terms we write as

$$\mathbb{Z}[G]x_0 \leftarrow \mathbb{Z}[G]x_1 \oplus \mathbb{Z}[G]y_1 \leftarrow \mathbb{Z}[G]x_2 \oplus \mathbb{Z}[G]y_2 \oplus \mathbb{Z}[G]z_2.$$

The 2-cocycles for this efficient resolution are triples (r, s, t) of nonzero elements $r \in K^g$, $s \in K^h$, $t \in K^{gh}$ satisfying $Nr = NsNt$. Here each N denotes a norm from the respective field to k, with the coboundaries the triples of the form $(N_g r', N_h s', N_{gh}(r'/s'))$ for $r', s' \in K^*$, where N_ℓ denotes the norm from K to K^ℓ for $\ell \in G$.

The procedure reduces to two tests, with the failure of either indicating the nontriviality of the cohomology class of (r, s, t). First, test if r is a norm for the extension K/K^g. If it is, let $r' \in K^*$ satisfy $N_g r' = r$, apply Hilbert's Theorem 90 to solve for $u \in K^*$ satisfying $u/(g.u) = st/N_{gh}r'$ and notice that $v = s/N_h u$ lies in k. The second test is if v is a norm for the extension K^g/k. If so, let $v' \in (K^g)^*$ satisfy $Nv' = v$. Then with $s' = h.(uv')$ we have

$$(r, s, t) = \left(N_g r', N_h s', N_{gh}\frac{r'}{s'}\right).$$

For the verification we work with the following homomorphism σ_2 (notation is as in Section 2; σ_1 is given in loc. cit.): $\sigma_2\left(e, g^i, g^{i+i'}h^{j'}\right) = -ex_2$ if $i + i' \geq n$ and otherwise is 0 for $i, i' \in \{0, \ldots, n-1\}$, $j' \in \{0, 1\}$, and

$$\sigma_2\left(e, g^i h, g^i h g^{i'} h^{j'}\right) = -\left(j' g^{i-i'} + \sum_{a=0}^{i'-1} g^{i-a}\right) y_2 - \sum_{a=1}^{i'} g^{i-a+j'} h^{j'} z_2 + \begin{cases} ex_2 & \text{if } i' > i, \\ 0 & \text{otherwise.} \end{cases}$$

Using σ_2 we obtain from (r, s, t) a 2-cocycle f for the standard resolution. Explicitly $f\left(g^i, g^{i'}h^{j'}\right)$ is r^{-1} if $i + i' \geq n$ and 1 otherwise, and $f\left(g^i h, g^{i'}h^{j'}\right)$ is the quotient of r if $i' > i$ and 1 otherwise by the quantity $\left(g^{i-i'}.s^{j'}\right)\prod_{a=1}^{i'}(g^{i-a}.(t\,(g.s)))$.

Following the proof of Proposition 4.1, the first step, testing the vanishing of $\left[\mathrm{sh}^2\alpha_{(\,)}\right]$, is achieved by Corollary 2.2, which in case of vanishing supplies the 1-cochain lift

$$\left(1, r'^{-1}, \ldots, r'^{-1}(g.r')^{-1} \cdots \left(g^{n-2}.r'\right)^{-1}\right).$$

We use the isomorphism χ^1 to write elements of $\mathrm{Map}\left(G^2, A\right)^H$ as $2n$-tuples of pairs $\left(w^{(0)}, w^{(1)}\right)$ of elements of K^* with action $g^i h^j.\left(w^{(0)}, w^{(1)}\right) = \left(g^i.w^{(j)}, g^{-i}.w^{(1-j)}\right)$, so that $\delta'_{(\,)}$ is expressed as

$$\left(\prod_{a=0}^{i-1}\left(g^a.r'^{-1}\right),\ \left(g^{-i}.s^{-j}\right)\prod_{a=0}^{i-1}\left(g^{-a}.s^{-1}\right)\prod_{a=1}^{i}\left(g^{-a}.\left(t^{-1}r'\right)\right)\right)_{i\in\{0,\ldots,n-1\},j\in\{0,1\}}.$$

Tedious but straightforward computations yield β', with β'_e trivial and β'_h expressed as

$$\left(\left(g^i.s^j\right)\prod_{a=0}^{i-1}\left(g^a.\left(str'^{-1}\right)\right)\prod_{a=1}^{i}\left(g^a h.r'^{-1}\right),\ \left(g^{-i}.s^{-j}\right)\prod_{a=0}^{i-1}\left(g^{-a}.\left(s^{-1}(h.r')\right)\right)\prod_{a=1}^{i}\left(g^{-a}.\left(t^{-1}r'\right)\right)\right)_{i,j}.$$

For $i = 1$, $j = 0$, the pair has first entry $st/N_{gh}r'$, and ϵ'' in the proof is produced using Hilbert's Theorem 90. The remainder of the argument is straightforward, so we omit details and mention only that the final step produces the 1-cocycle lift $f'(g^i h^j) = \left(g^i h.(uv')^{-j}\right)\prod_{a=0}^{i-1}\left(g^a.r'^{-1}\right)$ of f for the standard resolution, and this is converted using $\tau_1(ex_1) = -(e, g)$, $\tau_1(ey_1) = -(e, h)$ to the (r', s') given above.

5. Applications

First, we apply the previous results and prove Theorem 1.2.

Proof. Given $[f] \in H^2(G, A)$ we can reduce to solving Problem 1.1 for a finite collection of p-Sylow subgroups and their associated Galois extensions by Corollary 3.4. Since p-groups are solvable we reduce further to finitely many intermediate cyclic Galois extensions by Corollary 4.2. Finally Corollary 2.2 reduces this to solving cyclic norm equations. □

Remark 5.1.
(i) Remark 4.3 shows that we can assume the cyclic intermediate extensions to be of prime order.

(ii) The results stated in Corollary 3.4 and Corollary 2.2 generalize well to arbitrary group cohomology for finite groups and also arbitrary degree as indicated. Proposition 4.1 generalizes also with respect to both aspects but it requires rather strong effective vanishing conditions, and Corollary 4.2 generalizes as well under effective vanishing conditions. Consequently Theorem 1.2 generalizes in this situation also to higher cohomology groups.

(iii) For C_1-fields, norm equations are always solvable for intermediate extensions as in the theorem and all higher cohomology vanishes. For instance, Tsen's Theorem tells us that this is the case for function fields in one variable over an algebraically closed field. In this case an effective algorithm for solving such norm equations is well known and described, e.g., in [13, Theorem C.4.2]. So the effective methods of this paper give an algorithm for solving Problem 1.1 for this class of fields. Since difference equations can be effectively solved by Hilbert's Theorem 90 we have using (ii) inductively effective vanishing of all higher cohomology.

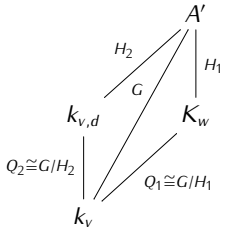
(iv) For number fields, cyclic norm equations are solvable if and only if there are no local obstructions by the Hasse Norm Theorem [6]. When a solution exists there are effective algorithms to produce a solution, e.g., [4], and these have been implemented for instance in the computer algebra program MAGMA. See Remark 5.2 for further comments on this case.

We give a procedure to evaluate local invariants [14, XIII, § 3] for number fields as stated in Proposition 1.3.

Proof. Let k_v be the completion of k at v. Since K/k is Galois there is only one place w in K extending v up to Galois conjugacy; denote the completion of K for w by K_w. Define $Q_1 = \mathrm{Gal}(K_w/k_v) < \Gamma$ and let $\widehat{f} \in \mathrm{Map}\left(Q_1^2, K_w^*\right)$ be the induced 2-cocycle.

For v an infinite place the Brauer group is either trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and being able to determine vanishing of a class suffices.

If v is finite let $d \,||Q_1|$ satisfy $d[\widehat{f}] = 0$, e.g., $d = |Q_1|$ (cf. [15, p. 35]). Let $k_{v,d}/k_v$ be the up to isomorphism unique unramified extension of degree d effectively constructable as a cyclotomic extension, v_d its valuation, $A' = k_{v,d} \cdot K_w$ a composition of fields and $A = A'^*$.



$$\begin{array}{ccccc} & & H^2\left(Q_2, A^{H_2}\right) & & \\ & & \downarrow{\scriptstyle \inf_2} & & \\ H^2\left(Q_1, A^{H_1}\right) & \xrightarrow{\inf_1} & H^2(G, A) & \xrightarrow{\mathrm{res}_1} & H^2\left(H_1, A\restriction_{H_1}\right)^{Q_1} \\ & & \downarrow{\scriptstyle \mathrm{res}_2} & & \\ & & H^2\left(H_2, A\restriction_{H_2}\right)^{Q_2} & & \end{array}$$

We get Galois extensions as indicated in the diagram with the corresponding Galois groups. By Hilbert's Theorem 90 all relevant H^1 vanish and by [15, p. 50] we get for each of the two field extension towers higher 5-term sequences, of which the first three terms of each constitute the diagram on the right.

By [14, XIII, § 3] we have $0 = d\,\mathrm{inv}_v\big(\mathrm{inf}_1[\widehat{f}]\big) = \mathrm{inv}_v\big(\mathrm{res}_2\big(\mathrm{inf}_1[\widehat{f}]\big)\big)$, thus $\mathrm{res}_2\big(\mathrm{inf}_1[\widehat{f}]\big) = 0$. As in the proof of Proposition 4.1 we get effectively a 2-cocycle $\widetilde{\gamma}'' \in \mathrm{Map}\big(Q_2^2, A^{H_2}\big)$ with $\mathrm{inf}_2[\widetilde{\gamma}''] = \mathrm{inf}_1[\widehat{f}]$. For this we need to lift a 2-coboundary in $\mathrm{Map}\big(H_2^2, A\restriction_{H_2}\big)$ to a 1-cochain in $\mathrm{Map}\big(H_2^1, A\restriction_{H_2}\big)$ which by Theorem 1.2 and Remark 5.1 (i) is reduced to solving norm equations for cyclic extensions of local fields of prime degree. This task is effectively solvable by computations over finite residue fields (cf. [3, III.1]). We get

$$\mathrm{inv}_v[f] = \mathrm{inv}_v[\widetilde{\gamma}''] = \frac{1}{d}\,v_d\big(\tau^2\big(\widetilde{\gamma}''\big)^{-1}\big) = \frac{1}{d}\,v_d\left(\prod_{j=0}^{d-1}\widetilde{\gamma}''(\alpha^j,\alpha)\right),$$

where α is the element of Q_2 inducing the Frobenius on the residue field, τ^2 as in Section 2 maps into $k_{v,d}^*$. □

Remark 5.2.

Fieker in [5] solves Problem 1.1 for number fields K/k by identifying a finite set of "critical" primes S_{crit} such that lifting a 2-coboundary with coefficients in K^* is reduced to lifting with coefficients in the associated S-units $U_{S,K}$. After representing $U_{S,K}$ as finitely generated abelian group an algorithm of Holt (cf. [8]) is used to find a lifting for $U_{S,K}$-coefficients. Reducing Problem 1.1 directly to S-unit equations was previously outlined in [1, Theorem 2/3] both over number fields and function fields. The choice of the set of critical primes differs slightly.

In our approach we reduce to a finite collection of cyclic norm equations. For these there are well established approaches with optimized implementations; some of them also use S-units.

Acknowledgements

The author was supported in part by a grant from the SNF.

References

[1] Bright M., Swinnerton-Dyer P., Computing the Brauer–Manin obstructions, Math. Proc. Cambridge Philos. Soc., 2004, 137(1), 1–16
[2] Brown K.S., Cohomology of Groups, Grad. Texts in Math., 87, Springer, New York–Berlin, 1982
[3] Fesenko I.B., Vostokov S.V., Local Fields and Their Extensions, Transl. Math. Monogr., 121, American Mathematical Society, Providence, 2002
[4] Fieker C., Über Relative Normgleichungen in Algebraischen Zahlkörpern, Dr. Rer. Nat. Dissertation, Technische Universität, Berlin, 1997
[5] Fieker C., Minimizing representations over number fields II: Computations in the Brauer group, J. Algebra, 2009, 322(3), 752–765
[6] Hasse H., Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, 1931, 64–69
[7] Hilton P.J., Stammbach U., A Course in Homological Algebra, 2nd ed., Grad. Texts in Math., 4, Springer, New York, 1997
[8] Holt D.F., Cohomology and group extensions in Magma, In: Discovering Mathematics with Magma, Algorithms Comput. Math., 19, Springer, Berlin, 2006, 221–241
[9] Kresch A., Tschinkel Yu., On the arithmetic of del Pezzo surfaces of degree 2, Proc. London Math. Soc., 2004, 89(3), 545–569
[10] Kresch A., Tschinkel Yu., Effectivity of Brauer–Manin obstructions, Adv. Math., 2008, 218(1), 1–27
[11] Milne J.S., Étale Cohomology, Princeton Math. Ser., 33, Princeton University Press, Princeton, 1980
[12] Neukirch J., Algebraische Zahlentheorie, Springer, Berlin–Heidelberg, 2007

[13] Reid M., Chapters on algebraic surfaces, In: Complex Algebraic Geometry, Park City, 1993, IAS/Park City Math. Ser., 3, American Mathematical Society, Providence, 1997, 3–159
[14] Serre J.-P., Corps Locaux, Publications de l'Institut de Mathématique de l'Université de Nancago, VIII, Actualités Sci. Indust., 1296, Hermann, Paris, 1962
[15] Shatz S.S., Profinite Groups, Arithmetic, and Geometry, Ann. of Math. Stud., 67, Princeton University Press, Princeton, 1972
[16] Yamamoto K., An explicit formula of the norm residue symbol in a local number field, Sci. Rep. Tokyo Woman's Christian College, 1972, 24-28, 302–334