ON THE GALOIS GROUP OF 2-EXTENSIONS WITH RESTRICTED RAMIFICATION

DENIS VOGEL

Abstract. In this paper we study the relation structure of the Galois group of the maximal outside a given set S of primes unramified 2-extension $\mathbb{Q}_S(2)$ of $\mathbb{Q}$ and of the Galois group of the 2-class field tower of a quadratic number field. We complete Morishita's calculations of the triple Milnor invariants for $\mathbb{Q}_S(2)$ and obtain the relation structure of $G(\mathbb{Q}_S(2)/\mathbb{Q})$ modulo the fourth step of the Zassenhaus filtration. We use this result results in order to deduce information on the Galois group of the 2-class field tower of a quadratic number field.

1. Introduction

The objective of this paper is the study of relations in certain Galois groups, namely the Galois group of the maximal 2-extension of $\mathbb{Q}$ unramified outside a set of primes S and the 2-class field tower of a quadratic number field. Let us explain this now in more detail.

We consider the Galois group $G_S(2)$ of the maximal 2-extension $\mathbb{Q}_S(2)$ of $\mathbb{Q}$ which is unramified outside a set S of odd primes which is given by

$$S = \{l_1, \dots, l_n, \infty\}.$$

For $1 \leq i \leq n$ let $\mathfrak{l}_i$ be a fixed extension of l_i to $\mathbb{Q}_S(2)/\mathbb{Q}$, and let σ_i be an element of $G_S(2)$ with the following properties:

(i) σ_i is a lift of the Frobenius automorphism of $\mathfrak{l}_i$,
(ii) the restriction of σ_i to the maximal abelian subextension $\mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q}$ of $\mathbb{Q}_S(2)/\mathbb{Q}$ is equal to $(\lambda_i, \mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q})$, where λ_i denotes the idèle whose l_i-component equals l_i and all other components are 1.

For $1 \leq i \leq n$ let τ_i denote an element of $G_S(2)$ such that

(i) τ_i is a generator of the inertia group $T_{\mathfrak{l}_i}$ of $\mathfrak{l}_i$ in $\mathbb{Q}_S(2)/\mathbb{Q}$,
(ii) the restriction of τ_i to $\mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q}$ equals $(\alpha_i, \mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q})$, where α_i denotes the idèle whose l_i-component is a primitive root modulo l_i and all other components are 1.

By a well-known result due to Fröhlich and Koch [9], there is a minimal presentation

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G_S(2) \longrightarrow 1$$

Date: 17.03.04.

Key words and phrases. restricted ramification, 2-class field tower, Massey products.

During this research, the author has been supported by the DFG Forschergruppe "Arithmetik" at the Mathematisches Institut, Heidelberg.

of $G_S(2)$, where F is the free pro-2-group on generators $x_1, \dots, x_n$ and π is given by $x_i \mapsto \tau_i$, $1 \leq i \leq n$. A minimal generating system of R as a normal subgroup of F is given by $\mathcal{R} = \{\rho_m\}_{1 \leq m \leq n}$ with

$$\rho_m = x_m^{l_m - 1}(x_m^{-1}, y_m^{-1}),$$

where $y_m \in F$ is any preimage of σ_m for $1 \leq m \leq n$. Here, we write $(a, b) = a^{-1}b^{-1}ab$ for elements $a, b \in F$. We have

$$\rho_m \equiv x_m^{l_m - 1} \prod_{1 \leq i < j \leq n} (x_i, x_j)^{e_{i,j,m}} \mod F_{(3)}$$

for all $1 \leq m \leq n$, where $F_{(3)}$ denotes the third step of the Zassenhaus filtration of F which will be explained later and

$$(-1)^{e_{i,j,m}} = \begin{cases} \left(\dfrac{l_i}{l_j}\right) & \text{if} \quad m = i, \\ \left(\dfrac{l_j}{l_i}\right) & \text{if} \quad m = j, \end{cases}$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol. If the relation subgroup R lies inside $F_{(3)}$, one may ask what the relations $\{\rho_m\}_{1 \leq m \leq n}$ look like when they are considered modulo $F_{(4)}$.

The second question we are going to deal with is given by the following. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field, where D is a squarefree integer. We assume that $D \equiv 1 \mod 4$, or equivalently, that 2 is unramified in $K/\mathbb{Q}$. Let $S = \{l_1, \dots, l_n, \infty\}$ be the set of primes of $\mathbb{Q}$ which consists of all primes which are ramified in $K/\mathbb{Q}$ and the infinite prime ∞. We denote by K_{S_∞} the maximal 2-extension of K which is unramified outside the archimedean primes of K. For an imaginary quadratic number field this is the same as $K_\varnothing$, the maximal unramified 2-extension of K. There is the following theorem due to Koch[9]. We have a minimal presentation

$$1 \longrightarrow \mathfrak{R} \longrightarrow \mathfrak{H} \longrightarrow G(K_{S_\infty}/K) \longrightarrow 1$$

of $G(K_{S_\infty}/K)$ by the free pro-2-group $\mathfrak{H}$ on generators $w_1, \dots, w_{n-1}$. The subgroup $\mathfrak{R}$ of $\mathfrak{H}$ can be generated as a normal subgroup by certain elements $\{r_m\}_{1 \leq m \leq n}$ which fulfill the congruences

$$\begin{aligned} r_m &\equiv w_m^{2\ell_{m,n}} \prod_{\substack{1 \leq j \leq n-1 \\ j \neq m}} (w_m^2 w_j^2 (w_m, w_j))^{\ell_{m,j}} \mod \mathfrak{H}_{(3)}, \quad 1 \leq m \leq n-1, \\ r_n &\equiv \prod_{j=1}^{n-1} (w_j^2)^{\ell_{n,j}} \mod \mathfrak{H}_{(3)}, \end{aligned}$$

where

$$(-1)^{\ell_{m,j}} = \left(\frac{l_m}{l_j}\right)$$

for all $1 \leq m \leq n$. Once again, one may ask what happens if $\mathfrak{R}$ lies inside $\mathfrak{H}_{(3)}$. What do the $\{r_m\}_{1 \leq m \leq n}$ look like modulo $\mathfrak{H}_{(4)}$?

Let us explain the techniques used to settle these questions. One important ingredient is the theory of the Fox differential calculus on free pro-p-groups. This

is a theory which is developed in analogy to the theory of the Fox differential calculus on free discrete groups. Let F be the free pro-p-group on generators $x_1, \ldots, x_n$ and $\mathbb{Z}_p[\![F]\!]$ the completed group algebra of F over $\mathbb{Z}_p$. By a theorem of Ihara [8], there exist unique continuous $\mathbb{Z}_p$-linear maps, the free derivatives

$$\frac{\partial}{\partial x_i} : \mathbb{Z}_p[\![F]\!] \to \mathbb{Z}_p[\![F]\!],$$

such that every element $\alpha \in \mathbb{Z}_p[\![F]\!]$ can be uniquely written as

$$\alpha = \varepsilon_{\mathbb{Z}_p[\![F]\!]}(\alpha)1 + \sum_{i=1}^{n} \frac{\partial \alpha}{\partial x_i}(x_i - 1),$$

where $\varepsilon_{\mathbb{Z}_p[\![F]\!]} : \mathbb{Z}_p[\![F]\!] \to \mathbb{Z}_p$ denotes the augmentation homomorphism. For $I = (i_1, \ldots, i_r)$ we set

$$\varepsilon_{I,p}(f) = \varepsilon_{(i_1,\ldots,i_r),p}(f) = \varepsilon_{\mathbb{Z}_p[\![F]\!]}\left(\frac{\partial^r f}{\partial x_{i_1} \ldots \partial x_{i_r}}\right)$$

and denote by $\varepsilon_{I,p} : F \to \mathbb{Z}/p\mathbb{Z}$ the reduction of ε_I modulo p. For $n \geq 1$ let the ideal $I^n(F)$ of $\mathbb{F}_p[\![F]\!]$ be the n-th power of the augmentation ideal $I(F)$. The filtration

$$F_{(n)} = \{f \mid f - 1 \in I^n(F)\}, \quad n \geq 1,$$

is called the Zassenhaus filtration of F. We have that

$$f \in F_{(k)} \text{ if and only if } \varepsilon_{I,p}(f) = 0 \text{ for all } I \text{ with } |I| < k.$$

We construct bases for the quotients $F_{(k)}/F_{(k+1)}$ as $\mathbb{F}_p$-vector spaces. Assume we are given an element $f \in F_{(k)}$ and know the $\varepsilon_{I,p}(f)$ for all multi-indices I of length k. We study how f modulo $F_{(k+1)}$ can be expressed in terms of our basis of $F_{(k)}/F_{(k+1)}$.

We mention that by results of Morishita [12], the Fox differential calculus has a cohomological interpretation in terms of Massey products. We studied this connection independently. In the appendix, we give a new proof of one of Morihita's results.

We now come back to the arithmetical questions we started with. Morishita [11] introduced the notion of Milnor invariants of the group $G_S(2)$. Let $r \geq 1$ and $1 \leq i_1, \ldots, i_r \leq n$. The Milnor μ_2-invariant of $G_S(2)$ corresponding to $I = (i_1, \ldots, i_r)$ is defined by

$$\mu_2(I) = \varepsilon_{I',2}(y_{i_r}),$$

where $I' = (i_1, \ldots, i_{r-1})$. We remark that it is shown in [11] that the Milnor invariants are independent of the choices we made and are invariants of $G_S(2)$. We want to calculate the third order Milnor invariants of $G_S(2)$. The group R of relations of $G_S(2)$ lies inside $F_{(3)}$ if and only if all l_i are $\equiv 1 \mod 4$ and we have

$$\left(\frac{l_i}{l_j}\right) = 1 \text{ for all } 1 \leq i, j \leq n, \ i \neq j.$$

In this setting Morishita has calculated the third order Milnor invariants $\mu_2(i, j, k)$ for $1 \leq i, j, k \leq n$ pairwise distinct. We determine the third order Milnor invariants also in the remaining cases. This gives us a description of the sought-after

relation structure of $G_S(2)$. It turns out that the third order Milnor invariants are described by the so-called Rédei symbol which was introduced in the 1930's by Rédei [14]. This triple symbol $[p_1, p_2, p_3]$ for primes p_1, p_2, p_3 taking values ± 1 describes a prime decomposition law in a certain dihedral extension of degree 8. We prove the following

Theorem (Theorem 3.12)**.** *Let* $S = \{l_1, \dots, l_n, \infty\}$ *where* $l_i \equiv 1 \mod 4$, $i = 1, \dots, n$, *and assume that*

$$\left(\frac{l_i}{l_j}\right) = 1 \text{ for all } 1 \leq i, j \leq n,\ i \neq j.$$

Let $1 \leq i, j, k \leq n$. *The third order Milnor invariants of* $G_S(2)$ *are given by*

$$(-1)^{\mu_2(i,j,k)} = \begin{cases} [l_i, l_j, l_k] & \text{if } \gcd(l_i, l_j, l_k) = 1, \\ 1 & \text{if } i = j = k. \end{cases}$$

For each $1 \leq m \leq n$ *we have*

$$\rho_m \equiv \prod_{\substack{1 \leq i < j \leq n, \\ k < j}} ((x_i, x_j), x_k)^{e_{i,j,k,m}} \mod F_{(4)},$$

where

$$(-1)^{e_{i,j,k,m}} = \begin{cases} [l_i, l_j, l_k] & \text{if } m = j \text{ and } m \neq k, \\ [l_i, l_j, l_k] & \text{if } m \neq j \text{ and } m = k, \\ [l_i, l_j, l_k] & \text{if } m = i \text{ and } j = k, \\ [l_i, l_j, l_k] & \text{if } m = j = k, \\ 1 & \text{otherwise.} \end{cases}$$

We also give several examples in which we calculate the relations modulo $F_{(4)}$.

We apply the results about $G_S(2)$ to the study of the 2-class field tower of certain quadratic number fields. We follow Koch's construction from [9], and using the Fox differential calculus, in particular a chain rule which is proved in the first chapter, we are able to give a partial description of sought-after relation structure of $G(K_{S_\infty}/K)$. We prove the following theorem.

Theorem (Theorem 4.4)**.** *Let* $K = \mathbb{Q}(\sqrt{D})$ *be a quadratic number field where* D *satisfies one of the following conditions:*

(i) $D = l_1 \cdot \ldots \cdot l_n$ *and all* l_i *are congruent* 1 *modulo* 4,
(ii) $D = -l_1 \cdot \ldots \cdot l_n$, *where* $l_1, \dots, l_{n-1}$ *are congruent* 1 *modulo* 4 *and* l_n *is congruent* 3 *modulo* 4,

and assume that

$$\left(\frac{l_i}{l_j}\right) = 1 \text{ for all } 1 \leq i, j \leq n,\ i \neq j.$$

If we write the relations r_m, $1 \leq m \leq n$ *modulo* $\mathfrak{H}_{(4)}$ *as*

$$r_m \equiv \prod_{\substack{1 \leq i < j \leq n-1, \\ k \leq j}} ((w_i, w_j), w_k)^{e_{i,j,k,m}} \mod \mathfrak{H}_{(4)},$$

then for $1 \leq i < j \leq n-1$, $k < j$, $i \neq k$ *and* $1 \leq m \leq n-1$ *(in case (i) also* $m = n$ *is allowed) we have*

$$(-1)^{e_{i,j,k,m}} = \begin{cases} [l_i, l_j, l_k] & \text{if} \quad m = j \text{ or } m = k, \\ 1 & \text{otherwise.} \end{cases}$$

We remark that for imaginary quadratic number fields there is an isomorphism

$$H^1(G(K_{S_\infty}), \mathbb{Z}/2\mathbb{Z}) = H^1(G(K_\varnothing/K), \mathbb{Z}/2\mathbb{Z}) \cong (\mathrm{Cl}(K)/2)^*,$$

where $\mathrm{Cl}(K)$ denotes the ideal class group of K and * denotes the Pontryagin dual. In the situation of the theorem, we have a triple Massey product on $H^1(G(K_\varnothing), \mathbb{Z}/2\mathbb{Z})$. The pairings

$$H^1(G(K_\varnothing/K)) \times H^1(G(K_\varnothing/K)) \times H^1(G(K_\varnothing/K)) \overset{\langle \cdot,\cdot,\cdot \rangle}{\to} H^2(G(K_\varnothing/K)) \overset{\mathrm{tr}_{r_k}}{\to} \mathbb{Z}/2\mathbb{Z}$$

(here the coefficients are $\mathbb{Z}/2\mathbb{Z}$) induced by the Massey product and the trace maps (see the appendix), are therefore pairings

$$(\mathrm{Cl}(K)/2)^* \times (\mathrm{Cl}(K)/2)^* \times (\mathrm{Cl}(K)/2)^* \to \mathbb{Z}/2\mathbb{Z}.$$

By virtue of our above theorem, we give examples where these pairings are non-trivial.

I would like to thank my supervisor Kay Wingberg for his suggestion to study these problems and his constant encouragement. Furthermore, I would like to thank Alexander Schmidt and Otmar Venjakob for numerous discussions on the subject.

2. Algebraic prerequisites

Originally, the Fox differential calculus has been developed for discrete free groups. It is possible to carry it over to free pro-p-groups, see [8] and [11].

Let F be the free pro-p-group on generators $x_1, \ldots, x_n$ and let $\mathbb{Z}_p[\![F]\!]$ be the completed group algebra of F over $\mathbb{Z}_p$. Let $\varepsilon_{\mathbb{Z}_p[\![F]\!]} : \mathbb{Z}_p[\![F]\!] \to \mathbb{Z}_p$ be the augmentation homomorphism. We use the following result due to Ihara which essentially states that free derivatives exist as in the case of discrete free groups and share the same properties.

Theorem 2.1. *([8], Thm.2.1) For each* i *with* $1 \leq i \leq n$ *there exists a uniquely determined continuous* $\mathbb{Z}_p$*-linear map, the free derivative*

$$\frac{\partial}{\partial x_i} : \mathbb{Z}_p[\![F]\!] \to \mathbb{Z}_p[\![F]\!],$$

such that every element $\alpha \in \mathbb{Z}_p[\![F]\!]$ *can be uniquely written as*

$$\alpha = \varepsilon_{\mathbb{Z}_p[\![F]\!]}(\alpha)1 + \sum_{i=1}^{n} \frac{\partial \alpha}{\partial x_i}(x_i - 1).$$

For properties of the free derivatives we refer to [8] and [11]. Before we continue we introduce a notion that is needed in all what follows. Here and in the rest of the exposition we mean by a **multi-index** I of **height** n a tuple of elements

$I = (i_1, \dots, i_r)$ where r is a natural number and $1 \leq i_k \leq n$ for all $1 \leq k \leq r$. Usually we will assume that the height is clear from the context and omit it from the notation. For a multi-index $I = (i_1, \dots, i_r)$ we denote by $|I| = r$ the **length** of I. If multi-indices $I_1 = (i_1, \dots, i_r)$, $I_2 = (j_1, \dots, j_s)$ are given, we denote by

$$I_1 I_2 = (i_1, \dots, i_r, j_1, \dots, j_s)$$

the concatenation of I_1 and I_2. We denote the set of multi-indices of height n by $\mathcal{M}^n$ and the set of multi-indices of height n and length k by $\mathcal{M}^n_k$.

The completed group algebra $\mathbb{Z}_p[\![F]\!]$ is isomorphic to the ring $\mathbb{Z}_p\langle\langle X_1, \dots, X_n\rangle\rangle$ of formal power series in n non-commuting variables $X_1, \dots, X_n$ over $\mathbb{Z}_p$, and an isomorphism is given by

$$\psi : \mathbb{Z}_p[\![F]\!] \to \mathbb{Z}_p\langle\langle X_1, \dots, X_n\rangle\rangle, \ x_i \mapsto 1 + X_i.$$

The **Magnus expansion** $M(f)$ of $f \in F$ is given by

$$M(f) = \psi(f) = 1 + \sum_{I \in \mathcal{M}^n} \varepsilon_I(f) X_I, \ \varepsilon_I(f) \in \mathbb{Z}_p,$$

For each multi-index $I \in \mathcal{M}^n$ this gives us a map

$$\varepsilon_I : F \to \mathbb{Z}_p.$$

This map stands in the following relation to free differential calculus, cf. [11],§2.

Proposition 2.2. *Let $f \in F$ and $I = (i_1, \dots, i_r) \in \mathcal{M}^n$. Then*

$$\varepsilon_I(f) = \varepsilon_{\mathbb{Z}_p[\![F]\!]} \left(\frac{\partial^r f}{\partial x_{i_1} \dots \partial x_{i_r}} \right).$$

Definition 2.3. The **basic commutators** of weight one are $x_1, \dots, x_n$, and their ordering is $x_1 > \dots > x_n$. Assume we have defined the basic commutators together with their ordering for all weights $< k$. Then the basic commutators of weight k are the elements of F of the form (c_1, c_2) where c_1, c_2 are basic commutators of weights k_1, k_2. Moreover we require $c_1 > c_2$, and if $c_1 = (c_3, c_4)$ we also require that $c_2 \leq c_4$. The ordering among the commutators of weight k is lexicographically, i.e. $(c_1, c_2) < (c_1', c_2')$ if and only if $c_1 < c_1'$, or $c_1 = c_1'$ and $c_2 < c_2'$. Commutators of weight k are greater than all commutators of smaller weight.

Example 2.4. The basic commutators of weight 3 are given by $((x_i, x_j), x_k)$, $1 \leq i < j \leq n$, $k \leq j$.

For a pro-p-group G we denote by $\{G_k\}_{k \geq 1}$ the descending central series of G which is defined recursively by $G_1 = G$, $G_{k+1} = (G_k, G)$ where (G_k, G) denotes the closed subgroup of G generated by the commutators $(a, b) = a^{-1}b^{-1}ab$ for $a \in G_k$, $b \in G$. We have the following theorem, which follows directly from an analogous statement for discrete free groups, cf. [6], Thm. 11.2.4, by completion.

Theorem 2.5. *The basic commutators of weight k represent a basis of F_k/F_{k+1} as a free $\mathbb{Z}_p$-module.*

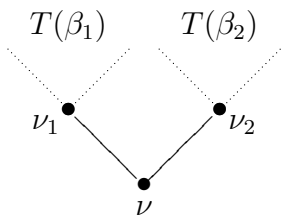
We want to study the effect of ε_I on the basic commutators or more generally on the so-called bracket arrangements. We collect some definitions from [5].

Definition 2.6. A **bracket arrangement** consists of brackets and asterisks (which act as place holders) and comes assigned with a weight. The only bracket arrangement of weight one is $(*) = *$. Assume all bracket arrangements of weight $< k$ have been defined. The bracket arrangements of weight k are of the form $\beta = (\beta_1, \beta_2)$, where β_1, β_2 are bracket arrangements of weight k_1, k_2 and $k = k_1 + k_2$. The weight of a bracket arrangement β is denoted by $\omega(\beta)$. Suppose a bracket arrangement β with $\omega(\beta) = k$ and a multi-index $I = (i_1, \ldots, i_k)$ are given. Then $\beta(I)$ denotes the commutator in F_k, which is obtained from β by substitution of $x_{i_1}, \ldots, x_{i_k}$ in consecutive locations.

To each bracket arrangement β we will associate a tree $T(\beta)$ with a root.

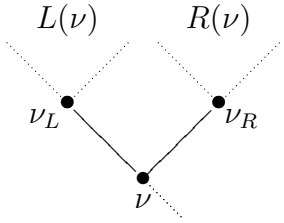
Definition 2.7. If $\omega(\beta) = 1$ then the **tree** $T(\beta)$ consists of a single vertex, which is the root. Assume these trees have been defined for all weights $< k$, and β is of the form $\beta = (\beta_1, \beta_2)$ und has weight k. Then $T(\beta)$ is the tree in figure 1 and ν is its root, where ν_1 and ν_2 are the roots of $T(\beta_1)$ and $T(\beta_2)$, respectively. We orient the trees in such a way that left-right ordering is preserved and that the new root is at the bottom. The weight of $T(\beta)$ is defined as $\omega(\beta)$. We denote the set of these trees by $\mathcal{T}$.

FIGURE 1. $T(\beta)$



If ν is a vertex in $T \in \mathcal{T}$, we can pick out an upper tree $U(\nu)$, a left-hand tree $L(\nu)$ and a right-hand tree $R(\nu)$, see fig. 2.

FIGURE 2



$U(\nu) = L(\nu) \cup R(\nu)$
$\nu_L =$ left-hand vertex
$\nu_R =$ right-hand vertex

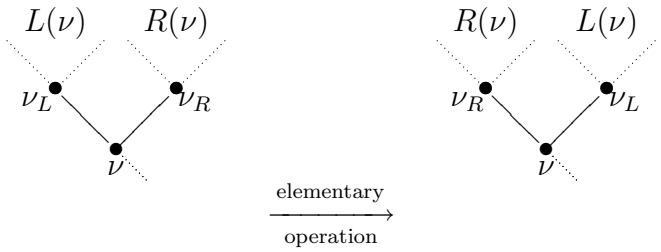
Definition 2.8. Let $\beta(I) \in F_k - F_{k+1}$ (this is e.g. the case if $\beta(I)$ is basic). To $\beta(I)$ we associate a **labelled tree** $T(\beta, I)$ which is just $T(\beta)$ with each vertex having a label from the free group F. The labelling is defined inductively as follows: If $\omega(\beta) = 1$ and $I = i$, then $T(\beta, I) = {}^{x_i}\cdot$. Assume the labelling has been

accomplished for all trees of weight $< k$ and $\beta = (\beta_1, \beta_2)$ has weight k. We break I up in $I = I_1 I_2$ with $l(I_1) = \omega(\beta_1)$, $I_2 = \omega(\beta_2)$. Then the sub-trees $T(\beta_1)$ und $T(\beta_2)$ are labelled and the root of $T(\beta)$ is labelled with the commutator (L_1, L_2) where L_1 and L_2 are the labels of the roots of $T(\beta_1)$ and $T(\beta_2)$, respectively. We denote the set of labelled trees of this type by $\mathcal{T}_k$. If a tree $T = T(\beta, I)$ is given we set $\mathcal{I}(T) = I$ and $\mathcal{B}(T) = \beta(I)$. The monomial $u(T)$ of a labelled tree $T(\beta, I)$ is defined by

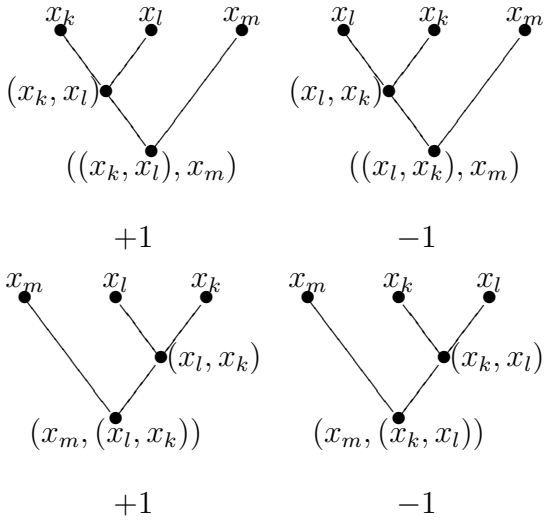
$$u(T) = X_I = X_{i_1} \cdot \ldots \cdot X_{i_r}.$$

Definition 2.9. The **admissible operations** on $T \in \mathcal{T}$ are generated by the following elementary operations: For a vertex $\nu \in T$ we interchange $L(\nu)$ and $R(\nu)$ and preserve the left-right and up-down orderings within $L(\nu)$, $R(\nu)$ while keeping ν and $T - U(\nu)$ fixed (see fig.3). The sign of an elementary operation is -1 and the sign of an admissible operation is the product the signs of its elementary operations. An admissible operation on $T \in \mathcal{T}_k$ is an admissible operation on T where T is interpreted as an element of $\mathcal{T}$. The labelling is preserved by each elementary operation in the sense that the labels remain attached to the vertices they were originally attached to. We denote the set of admissible operations on T by $\mathrm{Op}(T)$.

FIGURE 3. elementary operation



Example 2.10. Let $1 \leq k, l, m \leq n$, $k \neq l$. There are four admissible operations on the labelled tree $T = T(((*, *), *), (k, l, m))$. Their effect on T can be seen in the following picture. The corresponding signs are noted below the trees.



For $f \in F$ let $\mathcal{L}(f)$ denote the leading polynomial of the Magnus expansion $M(f)$ of f. If $f \in F_k - F_{k+1}$ it obviously holds that

$$\mathcal{L}(f) = \sum_{l(I)=k} \varepsilon_I(f) X_I.$$

In complete analogy to [5], lemma 5.5, we obtain the following result.

Proposition 2.11. *Let β be a bracket arrangement of weight $k \geq 1$ and $I = (i_1, \ldots, i_k) \in \mathcal{M}^n$, such that $\beta(I) \in F_k - F_{k+1}$. Let $T = T(\beta, I)$. Then*

$$\mathcal{L}(\beta(I)) = \sum_{\sigma \in \mathrm{Op}(T)} \mathrm{sgn}(\sigma) u(\sigma(T)).$$

Example 2.12. Let $\beta = ((*,*),*)$, $I = (k,l,m)$ with $k \neq l$. From the above example we obtain

$$\mathcal{L}(((x_k, x_l), x_m)) = X_{klm} + X_{mlk} - X_{mkl} - X_{lkm}.$$

Let $\mathcal{C}_k$ denote the free $\mathbb{Z}_p$-module on the set C_k of basic commutators of weight k. In later applications we will need a description of the map

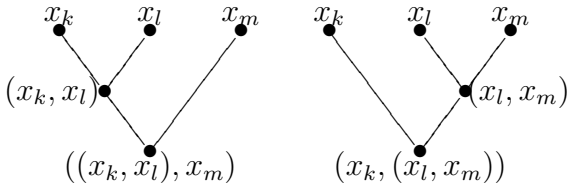
$$\eta_k : \mathcal{M}_k^n \to \mathcal{C}_k, \quad I \mapsto \sum_{\beta \in C_k} \varepsilon_I(\beta(I))\beta.$$

It is easily seen that the previous proposition implies the following result.

Proposition 2.13. *The map η_k is given by*

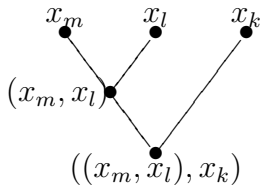
$$\eta_k(I) = \sum_{\substack{T \in \mathcal{T}_k \\ \mathcal{I}(T) = I}} \sum_{\substack{\sigma \in \mathrm{Op}(T) \\ \sigma(T) \in C_k}} \mathrm{sgn}(\sigma) \mathcal{B}(\sigma(T)).$$

Example 2.14. Let $I = (k,l,m)$ with $1 \leq k,l,m \leq n$ and assume that $l > k$, $l > m$ and $k \neq m$. There are two trees $T_1, T_2 \in \mathcal{T}_3$ with $\mathcal{I}(T_i) = I$, $i = 1, 2$:



T_1 $\qquad$ T_2

The labelled tree T_1 corresponds to a basic commutator, and no nontrivial admissible operation will produce a labelled tree from T_1 that corresponds to a basic commutator as well. The labelled tree T_2 does not correspond to a basic commutator, but the labelled tree



obtained from T_2 by an admissible operation of sign $+1$ is the only one obtained from T_2 that does. Hence

$$\eta_3(I) = ((x_k, x_l), x_m) + ((x_m, x_l), x_k).$$

Let G be a finitely generated pro-p-group, and for $k \geq 1$ let the ideal $I^k(G)$ of $\mathbb{F}_p[\![G]\!]$ be the k-th power of the augmentation ideal $I(G)$. The filtration

$$G_{(k)} = \{g \mid g - 1 \in I^k(G)\}, \quad k \geq 1,$$

is called the **Zassenhaus filtration** of G. There are the following results on the Zassenhaus filtration, see [3], Thm. 12.9 and [3], Thm. 11.2, respectively.

Theorem 2.15. (i) *The Zassenhaus filtration can be recursively described as follows:*

$$G_{(k)} = G_{(\lceil k/p \rceil)}^p \prod_{\substack{i,j \geq 1 \\ i+j=k}} (G_{(i)}, G_{(j)}),$$

where $\lceil k/p \rceil$ denotes the least integer m such that $pm \geq k$.

(ii) *For each k,*

$$G_{(k)} = \prod_{\substack{i,j \geq 0 \\ ip^j \geq k}} G_i^{p^j}.$$

These results last allows us in particular to write down bases for the quotients $F_{(k)}/F_{(k+1)}$ as $\mathbb{F}_p$-vector spaces using the description of the bases of F_k/F_{k+1} as given in 2.5. We denote by C_k the set of basic commutators of weight k and we set $C_k^a = \{c^a \mid c \in C_k\}$. We remark that if $F_i^{p^j} \subset F_{(k)}$, then $F_{i+1}^{p^j} \subset F_{(k+1)}$. If $i \nmid k$, then $F_i^{p^j} \subset F_{(k)}$ implies $F_i^{p^j} \subset F_{(k+1)}$. In particular we have the following

Corollary 2.16. *For each $k \geq 1$ there exists a uniquely determined set*

$$V_k \subseteq \{(i, j) \in \mathbb{Z} \times \mathbb{Z} \mid i, j \geq 0, ip^j = k\}$$

such that

$$B_k = C_{i_1}^{p^{j_1}} \dot{\cup} C_{i_2}^{p^{j_2}} \dot{\cup} \ldots \dot{\cup} C_{i_m}^{p^{j_m}}, \quad (i_r, j_r) \in V_k \text{ for all } r = 1, \ldots, m$$

represents a basis for $F_{(k)}/F_{(k+1)}$ as an $\mathbb{F}_p$-vector space.

Example 2.17. We have that

$$F_{(3)}/F_{(4)} = \begin{cases} F_3/F_3^p F_4 & \text{if} \quad p \neq 3, \\ F^3F_3/F^9F_2^3F_4 & \text{if} \quad p = 3. \end{cases}$$

For $p \neq 3$ the set C_3 of basic commutators of weight 3 represents a basis of $F_{(3)}/F_{(4)}$ as an $\mathbb{F}_p$-vector space. For $p = 3$ such a basis is represented by $C_1^3 \cup C_3$.

Let $\varepsilon_{I,p} : F \to \mathbb{Z}/p\mathbb{Z}$ denote the reduction of ε_I modulo p. For the following technical result, see [5].

Proposition 2.18. *Let $\alpha, \beta \in F$, $f \in F_{(i)}$, $g \in F_{(j)}$ and let $I \in \mathcal{M}^n$. Then the following assertions hold:*

(i)
$$\varepsilon_{I,p}(\alpha\beta) = \sum_{I_1 I_2 = I} \varepsilon_{I_1,p}(\alpha)\varepsilon_{I_2,p}(\beta).$$
(ii) *If* $|I| < i$, *then* $\varepsilon_{I,p}(f) = 0$.
(iii) *If* $|I| \leq \min(i,j)$, *then* $\varepsilon_{I,p}(fg) = \varepsilon_{I,p}(f) + \varepsilon_{I,p}(g)$.
(iv) *If* $|I| = i + j$, $I = I_1 I_2 = I_2' I_1'$, *where* I_1, I_2, I_1', I_2' *are multi-indices with* $|I_1| = |I_1'| = i$, $|I_2| = |I_2'| = j$, *then*
$$\varepsilon_{I,p}((f,g)) = \varepsilon_{I_1,p}(f)\varepsilon_{I_2,p}(g) - \varepsilon_{I_1',p}(f)\varepsilon_{I_2',p}(g).$$

The next result gives a characterization of the descending central series and the Zassenhaus filtration by means of differential calculus.

Lemma 2.19. *Let* $f \in F$. *Then:*

(i) $f \in F_k$ *if and only if* $\varepsilon_I(f) = 0$ *for all multi-indices* I *with* $|I| < k$.
(ii) $f \in F_{(k)}$ *if and only if* $\varepsilon_{I,p}(f) = 0$ *for all multi-indices* I *with* $|I| < k$.

Proof. (i) follows as in the discrete case, see [4], 4.4.5. (ii) follows by looking at the Magnus expansion of f modulo p and a consideration of the generators of $I^n(F)$. □

Let I be a multi-index of length k. The results above allow us to reduce the calculation of $\varepsilon_{I,p}$ on $F_{(k)}$ to a calculation of $\varepsilon_{I,p}$ applied to a basis of $F_{(k)}$ modulo $F_{(k+1)}$ as given in 2.16. We have already studied the effect of the ε_I on basic commutators. The next result shows that this is sufficient for the calculation of $\varepsilon_{I,p}$ on $F_{(k)}$.

Proposition 2.20. *The linear map*
$$F_{(k)}/F_{(k+1)} \to (\mathbb{Z}/p\mathbb{Z})^{\mathcal{M}_k^n}, \quad f \mod F_{(k+1)} \mapsto (\varepsilon_{I,p}(f))_{I \in \mathcal{M}_k^n}$$
is injective, and its representation matrix with respect to B_k *and the standard basis of* $(\mathbb{Z}/p\mathbb{Z})^{\mathcal{M}_k^n}$ *can be computed in terms of the maps* η_i, $i \in \mathrm{pr}_1 V_k$.

Proof. Linearity and injectivity of the above map follow from 2.18 and 2.19, respectively. Let $c^{p^r} \in C_s^{p^r}$ where $sp^r = k$. Then
$$\varepsilon_{I,p}(c^{p^r}) = \sum_{I = I_1 \ldots I_{p^r}} \varepsilon_{I_1,p}(c) \cdot \ldots \cdot \varepsilon_{I_{p^r},p}(c)$$
We call the decomposition $I = I_1 \ldots I_{p^r}$ of type w, where w is a natural number, if w of the multi-indices $I_1, \ldots, I_{p^r}$ are empty. There is exactly one decomposition of type 0. It is given by
$$I = (i_1, \ldots, i_s)(i_{s+1}, \ldots, i_{2s}) \ldots (i_{(p^r-1)s}, \ldots, i_{p^r s})$$
To a decomposition $I = I_1 \ldots I_{p^r}$ of type w we associate a reduced decomposition $\tilde{I} = \tilde{I}_1 \ldots \tilde{I}_{p^r - w}$ of type 0 by leaving out the empty multi-indices. We may then write
$$\varepsilon_{I,p}(c^{p^r}) = \sum_{w=0}^{p^r-1} \sum_{\substack{I = I_1 \ldots I_{p^r} \\ \text{of type } w}} \varepsilon_{\tilde{I}_1,p}(c) \cdot \ldots \cdot \varepsilon_{\tilde{I}_{p^r-w},p}(c)$$

Each reduced decomposition $\tilde{I} = \tilde{I}_1 \dots \tilde{I}_{p^r-w}$ occurs exactly $\binom{p^r}{w}$ times in the above summation. Since

$$v_p(\binom{p^r}{w}) = r - v_p(w) > 0$$

for $w = 0, \dots, p^r - 1$, where v_p denotes the p-adic valuation, it follows that

$$\varepsilon_{I,p}(c^{p^r}) = \varepsilon_{(i_1,\dots,i_s),p}(c) \cdot \dots \varepsilon_{(i_{(p^r-1)s},\dots,i_{p^r s}),p}(c),$$

hence $\varepsilon_{I,p}(c^{p^r})$ is determined by the knowledge of the map η_s from 2.13. □

Example 2.21. Let $f \in F_{(3)}$. Then we have

$$f \equiv \prod_{\substack{1\le k<l\le n\\ m\le l}} ((x_k,x_l),x_m)^{p-\varepsilon_{(l,k,m),p}(f)} \prod_{1\le k<l\le n} ((x_k,x_l),x_l)^{\varepsilon_{(k,l,l),p}(f)} \mod F_{(4)}$$

if $p \neq 3$, and

$$f \equiv \prod_{k=1}^{n} x_k^{3\varepsilon_{(k,k,k),3}(f)} \prod_{\substack{1\le k<l\le n\\ m\le l}} ((x_k,x_l),x_m)^{3-\varepsilon_{(l,k,m),3}(f)} \prod_{1\le k<l\le n} ((x_k,x_l),x_l)^{\varepsilon_{(k,l,l),3}(f)} \mod F_{(4)}$$

if $p = 3$.

A useful tool for making explicit calculations is the following chain rule.

Definition 2.22. Let F be the free pro-p group on $x_1, \dots, x_n$ and let F' be the free pro-p-group on $x'_1, \dots, x'_m$. Let $\phi : F \to F'$ be a homomorphism. We will denote by $\varepsilon^F_{I,p}$ and $\varepsilon^{F'}_{I,p}$ the corresponding maps $\varepsilon_{I,p}$ in order to avoid confusion. We set

$$\phi_i^j = \varepsilon^{F'}_{(i),p}(\phi(x_j)), \quad 1 \le i \le m,\ 1 \le j \le n,$$

and call the matrix $(\phi_i^j)_{i,j}$ the **Jacobi matrix** of ϕ.

$$\phi^{j_1,\dots,j_k}_{i_1,\dots,i_k} = \phi^{j_1}_{i_1}\phi^{j_2}_{i_2} \cdot \dots \cdot \phi^{j_k}_{i_k}.$$

Proposition 2.23. *Let the notation be as in 2.22, and let $f \in F_{(k)}$. Then*

$$\varepsilon^{F'}_{(i_1,\dots,i_k),p}(\phi(f)) = \sum_{j_1,\dots,j_k} \phi^{j_1,\dots,j_k}_{i_1,\dots,i_k} \varepsilon^F_{(j_1,\dots,j_k),p}(f).$$

Proof. This is easily proved by induction on k and makes use of 2.15(i) and 2.18. □

We mention a special case in which much more holds than the above chain rule. Let F be the free pro-p-group on $x_1, \dots, x_n$. We denote by N the normal subgroup generated by $x_{h+1}, \dots, x_n$ where $h \ge 0$, and by $\phi : F \to F' = F/N$ the canonical projection. We set $x'_i = x_i N$ for $i = 1, \dots, h$. Then for each multi-index $I \in \mathcal{M}^h$ of height h, and each $f \in F$, it holds that $\varepsilon^{F'}_{I,p}(\phi(f)) = \varepsilon^F_{I,p}(f)$. This follows immediately from the definition of $\varepsilon_{I,p}$.

In our applications we will make use of the shuffle property of the $\varepsilon_{I,p}$. For that purpose we introduce the notion of shuffles, cf. [1].

Definition 2.24. Let $I = (a_1, \ldots, a_l)$ and $J = (b_1, \ldots, b_m)$ be multi-indices. A **shuffle** of I and J is a pair (α, β) of sequences $\alpha = (\alpha(1), \ldots \alpha(l))$ and $\beta = (\beta(1), \ldots, \beta(m))$ such that $1 \leq \alpha(1) < \alpha(2) < \ldots < \alpha(l) \leq m+l$ and $1 \leq \beta(1) < \beta(2) < \ldots < \beta(m) \leq m+l$. If $\alpha(i)$ is always distinct from $\beta(j)$ the shuffle will be called a **proper shuffle**. We denote the set of shuffles of I and J by $\mathcal{S}(I, J)$ and the set of proper shuffles of I and J by $\hat{\mathcal{S}}(I, J)$. A multi-index $K = (c_1, \ldots, c_n)$ is called the **result of a shuffle** $(\alpha, \beta) \in \mathcal{S}(I, J)$ if

(i) $c_{\alpha(i)} = a_i$ for $i = 1, \ldots, l$ and $c_{\beta(j)} = b_j$ for $j = 1, \ldots, m$.
(ii) Each index $k = 1, \ldots, n$ is either an $\alpha(i)$ for some i or an $\beta(j)$ for some j or both.

For $s \in \mathcal{S}$ we denote by $K = \mathfrak{R}(s)$ the set of results of the shuffle s. If s is a proper shuffle then $\mathcal{R}(s)$ consists of one element which we denote by $\mathfrak{r}(s)$.

We note that if K is the result of a proper shuffle of I and J, then $|K| = |I| + |J|$. For multi-indices I and J we define the map $\varepsilon_{I,p} \cdot \varepsilon_{J,p}$ as

$$(\varepsilon_{I,p} \cdot \varepsilon_{J,p})(f) = \varepsilon_{I,p}(f)\varepsilon_{J,p}(f), \ f \in F.$$

The following lemma comes from the classical theory of the free differential calculus, see [1], lemma 3.3, and carries over directly to our situation.

Proposition 2.25. *Let I and J be multi-indices. Then*

$$\varepsilon_{I,p} \cdot \varepsilon_{J,p} = \sum_{s \in \mathcal{S}(I,J)} \sum_{K \in \mathfrak{R}(s)} \varepsilon_{K,p}.$$

In particular, if $f \in F_{(k)}$ with $k = |I| + |J|$, then

$$\sum_{s \in \hat{\mathcal{S}}(I,J)} \varepsilon_{\mathfrak{r}(s),p} = 0.$$

3. The maximal 2-extension of $\mathbb{Q}$ with restricted ramification

Let $S = \{l_1, \ldots, l_n, \infty\}$ be a finite set consisting of odd prime numbers $l_1, \ldots, l_n$ and the infinite prime ∞ of $\mathbb{Q}$. In this section we study the relation structure of the Galois group of the maximal outside S unramified 2-extension $\mathbb{Q}_S(2)$ of $\mathbb{Q}$. For $i = 1, \ldots, n$ let $\mathfrak{l}_i$ be a fixed prime over l_i in $\mathbb{Q}_S(2)$, and let σ_i be an element of $G_S(2) = G(\mathbb{Q}_S(2)/\mathbb{Q})$ with the following properties:

(i) σ_i is a lift of the Frobenius automorphism of $\mathfrak{l}_i$,
(ii) the restriction of σ_i to the maximal abelian subextension $\mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q}$ of the extension $\mathbb{Q}_S(2)/\mathbb{Q}$ is equal to $(\lambda_i, \mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q})$, where λ_i denotes the idèle whose l_i-component equals l_i and all other components are 1.

For $1 \leq i \leq n$ let τ_i denote an element of $G_S(2)$ such that

(i) τ_i is a generator of the inertia group $T_{\mathfrak{l}_i}$ of $\mathfrak{l}_i$ in $\mathbb{Q}_S(2)/\mathbb{Q}$,
(ii) the restriction of τ_i to $\mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q}$ equals $(\alpha_i, \mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q})$, where α_i denotes the idèle whose l_i-component is a primitive root modulo l_i and all other components are 1.

The following result is well-known.

Theorem 3.1 (Fröhlich, Koch)**.** *Let F be the free pro-2-group on generators $x_1, \dots, x_n$. Then $G_S(2)$ has a minimal presentation*

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G_S(2) \longrightarrow 1,$$

where π is given by $x_i \mapsto \tau_i$, $1 \leq i \leq n$, and a minimal generating system of R as a normal subgroup of F is given by $\mathcal{R} = \{\rho_m\}_{1 \leq m \leq n}$ with

$$\rho_m = x_m^{l_m - 1}(x_m^{-1}, y_m^{-1}),$$

where y_m is any preimage of σ_m. We have that

$$\rho_m \equiv x_m^{l_m - 1} \prod_{j \neq m} (x_m, x_j)^{\ell_{m,j}} \mod F_{(3)},$$

where

$$(-1)^{\ell_{m,j}} = \left(\frac{l_m}{l_j}\right).$$

It is easily verified that the above congruences for the relations may be rewritten as

$$\rho_m \equiv x_m^{l_m - 1} \prod_{1 \leq i < j \leq n} (x_i, x_j)^{e_{i,j,m}} \mod F_{(3)}$$

for all $1 \leq m \leq n$, where

$$(-1)^{e_{i,j,m}} = \begin{cases} \left(\frac{l_i}{l_j}\right) & \text{if} \quad m = i, \\ \left(\frac{l_j}{l_i}\right) & \text{if} \quad m = j. \end{cases}$$

There is the following definition due to Morishita [11].

Definition 3.2. Let $I = (i_1, \dots, i_r) \in \mathcal{M}^n$ be a multi-index. We define the **Milnor μ_2-invariant of $G_S(2)$ corresponding to I** by

$$\mu_2(I) = \varepsilon_{I',2}(y_{i_r}),$$

where $I' = (i_1, \dots, i_{r-1})$. By convention we set $\mu_2(I) = 0$ for any multi-index I of length 1.

We remark that it is shown in [11] that the Milnor invariants are independent of the choices we made and are invariants of $G_S(2)$. The following remark, see [11], Rem. 3.1.6.(2), will be useful in our calculations.

Remark 3.3. Let $S = \{l_1, \dots, l_n, \infty\}$ be a subset of $\tilde{S} = \{l_1, \dots, l_n, l_{n+1}, \dots, l_m, \infty\}$ and let $I \in \mathcal{M}^m$ be a multi-index. If $I \in \mathcal{M}^n$ then the Milnor invariants $\mu_2(I)$ defined via the Galois groups $G_S(2)$ resp. $G_{\tilde{S}}(2)$ coincide.

There is a shuffle property for Milnor invariants which follows from 2.25. As it is stated slightly incorrect in [11] we will restate it here.

Remark 3.4. Let $I = I_1 I_2 \in \mathcal{M}^n$ be a multi-index of length m. Then for all $1 \leq i \leq n$ we have

$$\sum_{s \in \hat{\mathcal{S}}} \sum_{K \in \mathfrak{R}(s)} \mu_2(K(i)) = 0,$$

where $K(i)$ denotes the concatenation of the multi-indices K and (i). In particular, if $\mu_2(J) = 0$ for all multi-indices J with $J \leq m$, then

$$m\mu_2(\underbrace{j, \ldots, j}_{m}, i) = 0$$

for all $1 \leq i, j \leq n$.

(It is the factor m that has been forgotten in [11], Thm. 3.1.8. In particular, that result would imply that under the hypothesis that the second order Milnor invariants vanish, the third order Milnor invariants of type $\mu_2(j, j, i)$ would vanish as well. We will later give examples for the nonvanishing of such Milnor invariants.)

We are interested in the case where $R \subseteq F_{(3)}$ which we assume from now on. By 3.1 this is the case if and only if

$$\binom{l_m - 1}{2} = 0$$

for all m with $1 \leq m \leq n$ and

$$\left(\frac{l_m}{l_j}\right) = 1 \quad \text{for all} \quad 1 \leq m, j \leq n, \ m \neq j.$$

The first condition is satisfied if and only if all l_m are congruent 1 modulo 4.

Rédei introduced a triple symbol $[p_1, p_2, p_3]$ for primes p_1, p_2, p_3 taking values ± 1 which describes a prime decomposition law in a certain dihedral extension of degree 8 (actually, his symbol is even a bit more general). In [11], a connection is given between the Rédei symbols $[l_i, l_j, l_k]$ and the Milnor invariants $\mu_2(i, j, k)$ of $G_S(2)$ for pairwise distinct primes $l_i, l_j, l_k \in S$. We will generalize the result of [11] to the case where some of the l_i, l_j, l_k may coincide. This allows us to give a complete description of the relation structure of $G_S(2)$ modulo $F_{(4)}$. Unfortunately the presentation in [11] is incorrect in the sense that a dihedral extension of degree 8 is constructed which is claimed to be unramified outside $\{p_1, p_2\}$ but which may also ramify at 2 depending on some parameters, and the extension explicitly given in [11], Ex. 3.2.6 is indeed ramified at 2. This makes the calculation of the Milnor numbers in [11] incorrect. Fortunately, the construction can be rescued if we stay closer to the original work of [14]. For this reason we have decided to give a more detailed view of the aforementioned construction and the definition of the Rédei symbol.

Definition 3.5. Let k be a number field, $\alpha \in k$ and $\mathfrak{p}$ be a nonzero prime ideal of the ring of integers $\mathcal{O}_k$ of k. Then we set

$$\left(\frac{\alpha | k}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits} \\ 0 & \text{if } \mathfrak{p} \text{ is ramified} \\ -1 & \text{if } \mathfrak{p} \text{ is inert} \end{cases}$$

in $k(\sqrt{\alpha})$.

We obtain the following result as a special case of [14], Satz 1.

Proposition 3.6. *Let p_1, p_2, p_3 be prime numbers with $\gcd(p_1, p_2, p_3) = 1$ and $p_i \equiv 1 \mod 4$, $i = 1, 2, 3$ with*

$$\left(\frac{p_i}{p_j}\right) = 1 \quad \text{if} \quad p_i \neq p_j \text{ and } 1 \leq i, j \leq 3.$$

Then there exists an element $\alpha_2 \in k_1 := \mathbb{Q}(\sqrt{p_1})$ with the following properties:

(i) $N_{k_1/\mathbb{Q}}\alpha_2 = p_2$,
(ii) $N_{k_1/\mathbb{Q}}(D_{k_1(\sqrt{\alpha_2})/k_1}) = p_2$ *where $D_{k_1(\sqrt{\alpha_2})/k_1}$ is the discriminant of the extension $k_1(\sqrt{\alpha_2})/k_1$.*

If α_2 has the above properties then there exists a prime $\mathfrak{p}_3$ in k_1 over p_3 such that

$$\left(\frac{\alpha_2|k_1}{\mathfrak{p}_3}\right) \neq 0,$$

and for all choices of α_2 and $\mathfrak{p}_3$ such that the above symbol does not vanish, it has the same value.

We remark that by [14], α_2 may be chosen as $\alpha_2 = x + y\sqrt{p_1}$ where x, y are integral solutions to the equation

$$x^2 - p_1 y^2 - p_2 z^2 = 0$$

which have the property that $\gcd(x, y, z) = 1$, $2|y$ and $x - y \equiv 1 \mod 4$.

Definition 3.7. Let p_1, p_2, p_3 be prime numbers with $p_i \equiv 1 \mod 4$, $i = 1, 2, 3$, and

$$\left(\frac{p_i}{p_j}\right) = 1 \quad \text{if} \quad p_i \neq p_j \text{ and } 1 \leq i, j \leq 3.$$

Then the **Rédei symbol** is defined as

$$[p_1, p_2, p_3] := \left(\frac{\alpha_2|k_1}{\mathfrak{p}_3}\right),$$

where α_2 and $\mathfrak{p}_3$ are given as in 3.6.

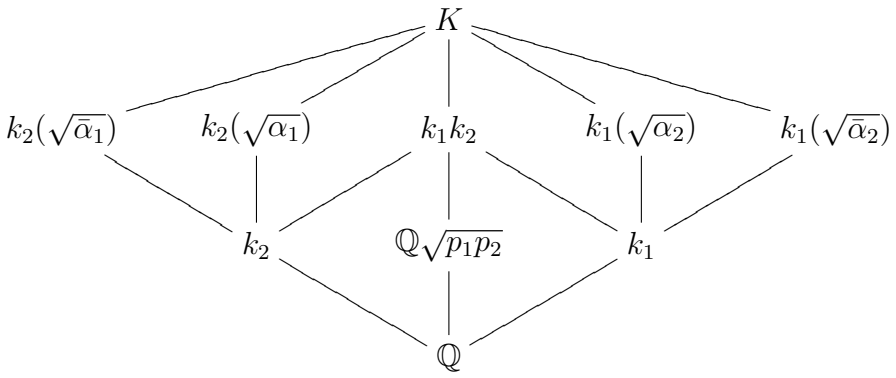
We will later need the following lemma, which follows directly from [14], Satz 2, Satz 4.

Lemma 3.8. *For any permutation $\gamma \in S_3$ we have*

$$[p_1, p_2, p_3] = [p_{\gamma(1)}, p_{\gamma(2)}, p_{\gamma(3)}].$$

Let $\alpha_1 := \alpha_2 + \bar{\alpha}_2 + 2\sqrt{p_2} \in k_2 := \mathbb{Q}(\sqrt{p_2})$ where $\bar{\alpha}_2$ denotes the conjugate of α_2. As remarked in [14], p.5, α_1 fulfils the conditions (i) and (ii) of 3.6 where the obvious replacements have to be made. Let $K := k_1 k_2(\sqrt{\alpha_2})$.

We consider the case where $p_1 \neq p_2$. Then we have the following diagram of fields:



where $\bar{\alpha}_1$ and $\bar{\alpha}_2$ denote the conjugates of α_1 and α_2, respectively. It is shown in [14], p.6 that $K/\mathbb{Q}$ is a Galois extension of degree 8 whose Galois group is the dihedral group of order 8. The Galois group of $K/\mathbb{Q}$ is generated by elements s and t which are defined by

$$s : \sqrt{p_2} \mapsto -\sqrt{p_2}, \quad t : \sqrt{p_1} \mapsto -\sqrt{p_1},\ \sqrt{\alpha_2} \mapsto -\sqrt{\bar{\alpha}_2},\ \sqrt{p_2} \mapsto -\sqrt{p_2}$$

and correspond to the subfields $k_1(\sqrt{\alpha_2})$ and $\mathbb{Q}(\sqrt{p_1p_2})$, respectively. The relations between s and t are given by

$$s^2 = t^4 = 1,\ sts^{-1} = t^{-1}.$$

It follows from the consideration in [14] that the discriminant of K is given by

$$D_{K/\mathbb{Q}} = p_1^4 p_2^4,$$

hence K is unramified outside $\{p_1, p_2, \infty\}$. (In [11] the conditions on α_2 are somewhat less restrictive which may result in K being ramified at 2.)

By our assumptions p_2 is completely decomposed in k_1. If we apply 3.6 to the triple (p_1, p_2, p_3), we see that there exists a prime $\mathfrak{p}_2$ in k_2 over p_2 which is unramified in $k_1(\sqrt{\alpha_2})$. Therefore we may choose a prime $\mathfrak{P}_2$ of K such that the inertia group $T_{\mathfrak{P}_2}(K/\mathbb{Q})$ is generated by s. A similar argument using the above remark concerning α_1 shows that we may choose a prime $\mathfrak{P}_1$ of K such that the inertia group $T_{\mathfrak{P}_1}(K/\mathbb{Q})$ is generated by st, which corresponds to the subfield $k_2(\sqrt{\alpha_1})$. Setting $a_1 = st$, $a_2 = s$, we have the following presentation of $G(K/\mathbb{Q})$:

$$G(K/\mathbb{Q}) = \langle a_1, a_2 \mid a_1^2 = a_2^2 = 1, (a_1a_2)^4 = 1 \rangle.$$

Now we set $p_1 = l_i$, $p_2 = l_j$, $p_3 = l_k$ where $l_i, l_j, l_k \in S - \{\infty\}$. By our assumptions, the Rédei symbol $[l_i, l_j, l_k]$ is well-defined. We choose the primes $\mathfrak{l}_i$, $\mathfrak{l}_j$ of $\mathbb{Q}_S(2)$ such that $\mathfrak{l}_i \cap \mathcal{O}_K = \mathfrak{P}_1$, $\mathfrak{l}_j \cap \mathcal{O}_K = \mathfrak{P}_2$. We have a projection

$$\pi :\ F \to G_S(2) \to G(K/\mathbb{Q})$$

where F is the free pro-2-group generated by $x_1, \ldots, x_n$ as in 3.1. By the choice of the $\mathfrak{l}_i$ we know that $x_i \mapsto a_1$, $x_j \mapsto a_2$, $x_m \mapsto 1$, for $m \neq i, j$. We obtain Thm. 3.2.5 of [M].

Proposition 3.9 (Morishita)**.** *Let $1 \leq i, j, k \leq n$ be pairwise distinct. Then*

$$(-1)^{\mu_2(i,j,k)} = [l_i, l_j, l_k].$$

We drop the assumption that l_i, l_j, l_k are pairwise distinct.

Proposition 3.10. *Let $1 \leq i, j \leq n$. If $i \neq j$ then*

$$\begin{aligned}(-1)^{\mu_2(i,j,j)} &= [l_i, l_j, l_j],\\ (-1)^{\mu_2(j,i,j)} &= [l_j, l_i, l_j].\end{aligned}$$

Proof. We claim that it is sufficient to prove the first assertion. Indeed, by 2.25 we obtain

$$\begin{aligned}0 &= \varepsilon_{(j,i,j),2}(\rho_j) + \varepsilon_{(i,j,j),2}(\rho_j) + \varepsilon_{(i,j,j),2}(\rho_j)\\ &= \varepsilon_{(j,i,j),2}(\rho_j)\\ &= \varepsilon_{(j,i,j),2}((x_j^{-1}, y_j^{-1}))\\ &= \varepsilon_{(i,j),2}(y_j^{-1}) + \varepsilon_{(j,i),2}(y_j^{-1})\\ &= \mu_2(i,j,j) + \mu_2(j,i,j).\end{aligned}$$

By 3.8 the claim is proved. We set $p_1 = l_i$, $p_2 = p_3 = l_j$. The inertia field of $\mathfrak{P}_2$ over $\mathbb{Q}$ is given by $k_1(\sqrt{\alpha_2})$. If $[p_1, p_2, p_2] = 1$, then p_2 decomposes in $k_1(\sqrt{\alpha_2})$ as

$$p_2\mathcal{O}_{k_1(\sqrt{\alpha_2})} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3^2,$$

where $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3$ are primes ideals of $\mathcal{O}_{k_1(\sqrt{\alpha_2})}$ with $\mathfrak{P}_2|\mathfrak{q}_1$ or $\mathfrak{P}_2|\mathfrak{q}_2$ because we know that p_2 is ramified in $k_1(\sqrt{\alpha_2})$. Hence $\pi(y_j) = 1$ in this case. If $[p_1, p_2, p_2] = -1$, then p_2 decomposes in $k_1(\sqrt{\alpha_2})$ as

$$p_2\mathcal{O}_{k_1(\sqrt{\alpha_2})} = \mathfrak{q}_1\mathfrak{q}_2^2,$$

where $\mathfrak{q}_1, \mathfrak{q}_2$ are primes ideals of $\mathcal{O}_{k_1(\sqrt{\alpha_2})}$ with $\mathfrak{P}_2|\mathfrak{q}_1$, so the Frobenius automorphism of the extension $k_1(\sqrt{\alpha_2})|k_1$ is given by the nontrivial automorphism. Therefore $\rho = \pi(y_j)$ is given by

$$\rho : \sqrt{p_1} \mapsto \sqrt{p_1},\ \sqrt{\alpha_2} \mapsto -\sqrt{\alpha_2},\ \sqrt{p_2} \mapsto \sqrt{p_2}$$

or

$$\rho : \sqrt{p_1} \mapsto \sqrt{p_1},\ \sqrt{\alpha_2} \mapsto -\sqrt{\alpha_2},\ \sqrt{p_2} \mapsto -\sqrt{p_2}.$$

By definition of σ_j the restriction of σ_j to the maximal abelian subextension $\mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q}$ of $\mathbb{Q}_S(2)/\mathbb{Q}$ is equal to $(\lambda_j, \mathbb{Q}_S(2)^{\mathrm{ab}}/\mathbb{Q})$, where λ_j denotes the idèle whose l_j-component equals l_j and all other components are 1. By local class field theory it follows that $\sigma_j(\sqrt{p_2}) = \sqrt{p_2}$, thus we obtain that $\pi(y_j) = t^2$. Let $\tilde{R}$ be defined by the exact sequence

$$1 \longrightarrow \tilde{R} \longrightarrow F \xrightarrow{\pi} G(K/\mathbb{Q}) \longrightarrow 1.$$

It is generated by $x_i^2, x_j^2, (x_ix_j)^4$ and the x_m for $m \neq i, j$ as a normal subgroup of F. The Magnus expansions of the generators are given by

$$\begin{aligned} x_i^2 &= 1 + X_i^2, \\ x_j^2 &= 1 + X_j^2, \\ (x_ix_j)^4 &\equiv 1 \mod \deg \geq 4, \\ x_m &= 1 + X_m \end{aligned}$$

For all generators it holds that $\varepsilon_{(i,j),2}$ as well as $\varepsilon_{(i),2}$ and $\varepsilon_{(j),2}$ vanish on them. By 2.18 and the continuity of $\varepsilon_{(i,j),2}$ we conclude that $\varepsilon_{(i,j),2}$, $\varepsilon_{(i),2}$, $\varepsilon_{(j),2}$ vanish on $\tilde{R}$. If $\pi(y_j) = 1$ then $y_j \in \tilde{R}$, hence $\mu_2(i,j,j) = \varepsilon_{(i,j),2}(y_j) = 0$. If $\pi(y_j) = (a_1a_2)^2$ then $y_j = (x_ix_j)^2 r$ with an element $r \in R$. We obtain

$$\begin{aligned} \mu_2(i,j,j) &= \varepsilon_{(i,j),2}((x_ix_j)^2) + \varepsilon_{(i,j),2}(r) + \varepsilon_{(i),2}((x_ix_j)^2)\varepsilon_{(j),2}(r) \\ &= 1, \end{aligned}$$

because the Magnus expansion of $(x_ix_j)^2$ is given by

$$(x_ix_j)^2 \equiv 1 + X_i^2 + X_j^2 + X_iX_j + X_jX_i \mod \deg \geq 3.$$

This proves the proposition. □

Now we deal with the Milnor invariants $\mu_2(i,i,j)$. Suppose that in the setting of 3.6, 3.7 we have $p_1 = p_2$. Then we have the following diagram of fields:

$$\begin{array}{c} K = k_1(\sqrt{\alpha_2}) \\ | \\ k_1 \\ | \\ \mathbb{Q} \end{array}$$

Here $K/\mathbb{Q}$ is a cyclic Galois extension of degree 4. From the considerations in [14] it follows that

$$D_{K/\mathbb{Q}} = p_1^3,$$

hence $K/\mathbb{Q}$ is unramified outside $\{p_1, \infty\}$. We set $p_1 = p_2 = l_i$, $p_3 = l_j$. Using the projection map

$$\pi : \ F \to G_S(2) \to G(K/\mathbb{Q})$$

we may choose the generator t of $G(K/\mathbb{Q})$ such that $\pi(y_i) = t$.

Proposition 3.11. *Let $1 \leq i, j \leq n$. If $i \neq j$ then*

$$(-1)^{\mu_2(i,i,j)} = [l_i, l_i, l_j].$$

Furthermore,

$$\mu_2(i,i,i) = 0.$$

Proof. By the definition of the Rédei symbol we know that

$$\pi(y_j) = \begin{cases} t^2 & \text{if } [l_i, l_i, l_j] = -1, \\ 1 & \text{if } [l_i, l_i, l_j] = 1. \end{cases}$$

Let $\tilde{R}$ be defined by the exact sequence

$$1 \longrightarrow \tilde{R} \longrightarrow F \xrightarrow{\pi} G(K/\mathbb{Q}) \longrightarrow 1.$$

It is generated by x_i^4 and the x_m for $m \neq i$ as a normal subgroup of F. By 2.18 it follows that $\varepsilon_{(i,i),2}$ as well as $\varepsilon_{(i),2}$ vanish on $\tilde{R}$. If $\pi(y_j) = 1$, then $y_j \in \tilde{R}$, hence $\mu_2(i,i,j) = \varepsilon_{(i,i),2}(y_j) = 0$. If $\pi(y_j) = t^2$, then $y_j = x_i^2 r$ with an element $r \in R$. We obtain

$$\begin{aligned} \varepsilon_{(i,i),2}(y_j) &= \varepsilon_{(i,i),2}(x_i^2) + \varepsilon_{(i,i),2}(r) + \varepsilon_{(i),2}(x_i^2)\varepsilon_{(i),2}(r) \\ &= 1, \end{aligned}$$

which proves the first statement. The extension K/k is totally ramified at p_1, hence $\pi(y_i) = 1$. Therefore $y_i \in \tilde{R}$, which implies that

$$\mu_2(i,i,i) = \varepsilon_{(i,i),2}(y_i) = 0.$$

Hence the proposition is proved. □

We summarize our results in the following theorem.

Theorem 3.12. *Let $S = \{l_1, \ldots, l_n, \infty\}$ where $l_i \equiv 1 \mod 4$, $i = 1, \ldots, n$, and assume that*

$$\left(\frac{l_i}{l_j}\right) = 1 \text{ for all } 1 \leq i, j \leq n,\ i \neq j.$$

Let $1 \leq i, j, k \leq n$. The third order Milnor invariants of $G_S(2)$ are given by

$$(-1)^{\mu_2(i,j,k)} = \begin{cases} [l_i, l_j, l_k] & \text{if } \gcd(l_i, l_j, l_k) = 1, \\ 1 & \text{if } i = j = k. \end{cases}$$

For each $1 \leq m \leq n$ we have

$$\rho_m \equiv \prod_{\substack{1 \leq i < j \leq n, \\ k < j}} ((x_i, x_j), x_k)^{e_{i,j,k,m}} \mod F_{(4)},$$

where

$$(-1)^{e_{i,j,k,m}} = \begin{cases} [l_i, l_j, l_k] & \text{if} \quad m = j \text{ and } m \neq k, \\ [l_i, l_j, l_k] & \text{if} \quad m \neq j \text{ and } m = k, \\ [l_i, l_j, l_k] & \text{if} \quad m = i \text{ and } j = k, \\ [l_i, l_j, l_k] & \text{if} \quad m = j = k, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. The first result follows from 3.9, 3.10, 3.11. For $1 \leq i < j \leq n, k < j$ we have

$$\begin{aligned} \varepsilon_{(j,i,k),2}(\rho_m) &= \varepsilon_{(j,i,k),2}(x_m^{l_m - 1}(x_m^{-1}, y_m^{-1})) \\ &= \varepsilon_{(j,i,k),2}((x_m^{-1}, y_m^{-1})) \\ &= \delta_{i,m}\mu_2(i,k,j) + \delta_{k,m}\mu_2(j,i,k), \end{aligned}$$

where we have made use of 2.18. By 2.21,

$$(-1)^{e_{i,j,k,m}} = (-1)^{\varepsilon_{(j,i,k),2}(\rho_m)} = [l_i, l_k, l_j]^{\delta_{j,m}} + [l_j, l_i, l_k]^{\delta_{k,m}}.$$

A similar calculation shows that

$$(-1)^{e_{i,j,j,m}} = (-1)^{\varepsilon_{(i,j,j),2}(\rho_m)} = [l_j, l_j, l_i]^{\delta_{i,m}} + [l_i, l_j, l_j]^{\delta_{j,m}}.$$

This implies the second result. □

By the results of the appendix, the above theorem gives in particular a complete description of pairings

$$\langle \cdot, \cdot, \cdot \rangle : H^1(G_S(2)) \times H^1(G_S(2)) \times H^1(G_S(2)) \to H^2(G_S(2)) \overset{\mathrm{tr}_{\rho_m}}{\to} \mathbb{Z}/2\mathbb{Z}$$

induced by the Massey triple product and the trace maps, where the coefficients are $\mathbb{Z}/2\mathbb{Z}$.

Example 3.13. (cf. [11], Ex. 3.2.6) Set $l_1 = 5$, $l_2 = 41$, $l_3 = 61$, so $S = \{5, 41, 61, \infty\}$. We may choose α_2 as $\alpha_2 = -11 + 4\sqrt{5}$ (note that this differs from [11] where it is chosen inappropriately). Computer calculations yield that the Rédei symbol $[l_i, l_j, l_k]$ is -1 exactly for all permutations of the triples (i, j, k) where $(i, j, k) = (1, 2, 3)$, $(1, 2, 2)$, $(1, 3, 3)$, $(2, 2, 3)$, $(2, 3, 3)$. Hence

$$\begin{aligned}
\rho_1 &\equiv ((x_1, x_2), x_2)((x_1, x_3), x_3)((x_2, x_3), x_1) \mod F_{(4)},\\
\rho_2 &\equiv ((x_1, x_2), x_2)((x_1, x_3), x_2)((x_2, x_3), x_2)((x_2, x_3), x_3) \mod F_{(4)},\\
\rho_3 &\equiv ((x_1, x_3), x_2)((x_1, x_3), x_3)((x_2, x_3), x_1)((x_2, x_3), x_2)((x_2, x_3), x_3) \mod F_{(4)}.
\end{aligned}$$

In [11] the triple $(5, 41, 61)$ is called a triple of Borromean primes modulo 2.

Example 3.14. Set $l_1 = 13$, $l_2 = 61$, $l_3 = 937$. The Rédei symbol $[l_i, l_j, l_k]$ is -1 exactly for all permutations of $(i, j, k) = (1, 2, 3)$. Therefore we have

$$\begin{aligned}
\rho_1 &\equiv ((x_2, x_3), x_1) \mod F_{(4)},\\
\rho_2 &\equiv ((x_1, x_3), x_2) \mod F_{(4)},\\
\rho_3 &\equiv ((x_1, x_3), x_2)((x_2, x_3), x_1) \equiv ((x_1, x_2), x_3) \mod F_{(4)}
\end{aligned}$$

We call $(13, 61, 937)$ a triple of proper Borromean primes modulo 2.

Example 3.15. Set $l_1 = 5$, $l_2 = 101$, $l_3 = 8081$. Then all Rédei symbols $[l_i, l_j, l_k]$ for $i, j, k \in \{1, 2, 3\}$ vanish. This implies that the relations of $G_S(2)$ are inside $F_{(4)}$. Hence we have that

$$G_S(2)/G_S(2)_{(4)} \cong F/F_{(4)}$$

4. The 2-class field tower of a quadratic number field

Let K be a quadratic number field. Let $S = \{l_1, \ldots, l_n, \infty\}$ be the set of primes of $\mathbb{Q}$ which consists of all primes which are ramified in $K/\mathbb{Q}$ and the infinite prime ∞. We denote by K_{S_∞} the maximal 2-extension of K which is unramified outside the archimedean primes of K. For an imaginary quadratic number field this is the same as $K_\varnothing$, the maximal unramified 2-extension of K.

We descend from $G_S(2)$ to $G(K_{S_\infty}/\mathbb{Q})$ using the following lemma, see [9], Prop. 7.1. As in the last section, let $\mathfrak{l}_m$ be a fixed prime over l_m in $\mathbb{Q}_S(2)$ for each $1 \le m \le n$. We denote the inertia group of $\mathfrak{l}_m$ in $\mathbb{Q}_S(2)/\mathbb{Q}$ by $T_{\mathfrak{l}_m}$.

Lemma 4.1. *Let N_S be the normal subgroup of $G_S(2)$ generated by the groups $T_{\mathfrak{l}_\mathfrak{m}} \cap G(\mathbb{Q}_S(2)/K)$ for $1 \le m \le n$. Then there is an exact sequence*

$$1 \longrightarrow N_S \longrightarrow G_S(2) \longrightarrow G(K_{S_\infty}/\mathbb{Q}) \longrightarrow 1.$$

We want to apply the results from the last section concerning $G_S(2)$ to the study of the 2-class field tower of K. Therefore we have to ensure that S does not contain 2. We write $K = \mathbb{Q}(\sqrt{D})$ where D is a squarefree integer which we decompose as

$$D = \pm d_1 \cdot \ldots \cdot d_n$$

where the d_i are different prime numbers. We recall that the set $\mathrm{Ram}_f(K/\mathbb{Q})$ of finite ramified primes of the extension $K/\mathbb{Q}$ is given by

$$\mathrm{Ram}_f(K/\mathbb{Q}) = \begin{cases} \{d_1, \ldots, d_n\} & \text{if} \quad D \equiv 1 \mod 4, \\ \{2, d_1, \ldots, d_n\} & \text{otherwise.} \end{cases}$$

There are two cases in which 2 does not occur in $\mathrm{Ram}_f(K/\mathbb{Q})$:

(i) $D = l_1 \cdot \ldots \cdot l_n$, all l_i are odd and the cardinality of the set $\{l_i | l_i \equiv 3 \mod 4,\ 1 \leq i \leq n\}$ is even.
(ii) $D = -l_1 \cdot \ldots \cdot l_n$, all l_i are odd and the cardinality of the set $\{l_i | l_i \equiv 3 \mod 4,\ 1 \leq i \leq n\}$ is odd.

We assume from now on that one of these cases applies. We order the l_m in such a way that $l_1, \ldots, l_r$ are congruent 1 modulo 4 and $l_{r+1}, \ldots, l_n$ are congruent 3 modulo 4.

For each $1 \leq m \leq n$ the group $T_{\mathfrak{l}_m} \cap G(\mathbb{Q}_S(2)/K)$ is generated by τ_m^2. Using the minimal presentation

$$1 \longrightarrow R \longrightarrow F \longrightarrow G_S(2) \longrightarrow 1$$

of $G_S(2)$ from Thm.3.1 we obtain an exact sequence

$$1 \longrightarrow R_a \longrightarrow F \longrightarrow G(K_{S_\infty}/\mathbb{Q}) \longrightarrow 1,$$

where F is the free pro-2-group on $x_1, \ldots, x_n$, and R_a is generated as a normal subgroup by R and by the preimages x_m^2 of τ_m^2, $1 \leq i \leq n$. The following theorem, see [9], Thm. 7.1, is an easy consequence.

Theorem 4.2 (Fröhlich)**.** *The group $G(K_{S_\infty}/\mathbb{Q})$ has a minimal presentation*

$$1 \longrightarrow R_a \longrightarrow F \longrightarrow G(K_{S_\infty}/\mathbb{Q}) \longrightarrow 1,$$

where F is the free pro-2-group generated by $x_1, \ldots, x_n$, and a system of generators of R_a as a normal subgroup of F is given by

$$\begin{aligned} x_m^2, &\quad 1 \leq m \leq n, \\ \rho_m = (x_m, y_m), &\quad 1 \leq m \leq n. \end{aligned}$$

We have that

$$\rho_m \equiv \prod_{\substack{1 \leq j \leq n \\ j \neq m}} (x_m, x_j)^{\ell_{m,j}} \mod F_{(3)}$$

where $\ell_{m,j}$ has been defined in the previous section.

We turn our attention to the group $G(K_{S_\infty}/K)$. Its preimage in F is the free pro-2-group H with the generator system

$$x_1 x_n, x_2 x_n, \ldots, x_{n-1} x_n, x_1^2, x_2^2, \ldots, x_n^2,$$

because the primes in S are ramified in $K/\mathbb{Q}$. R_a is generated as a normal subgroup of H by the relations

$$x_m^2,\ \rho_m,\ x_m^{-1}\rho_m x_m,\quad m=1,\dots,n.$$

An elementary calculation shows that R_a can be generated as a normal subgroup of H already by the elements x_m^2, ρ_m, $1 \le m \le n$. If we pass to the factor group $\mathfrak{H}$ of H with respect to the normal subgroup N generated by $x_1^2,\dots,x_n^2$, we get a presentation

$$1 \longrightarrow \mathfrak{R} \longrightarrow \mathfrak{H} \longrightarrow G(K_{S_\infty}/K) \longrightarrow 1,$$

where $\mathfrak{H}$ is the free pro-2-group on generators

$$w_m = x_m x_n N,\quad m=1,\dots,n-1,$$

and generating relations $\rho_m N$, $m=1,\dots,n$. Following these lines, Koch proved the following theorem, see [9], Thm. 7.3.

Theorem 4.3 (Koch)**.** *There is a minimal presentation*

$$1 \longrightarrow \mathfrak{R} \longrightarrow \mathfrak{H} \longrightarrow G(K_{S_\infty}/K) \longrightarrow 1$$

of $G(K_{S_\infty}/K)$ by the free pro-2-group $\mathfrak{H}$ on generators $w_1,\dots,w_{n-1}$ and defining relations

$$r_m = \rho_m N \equiv w_m^{2\ell_{m,n}} \prod_{\substack{1\le j\le n-1\\ j\ne m}} (w_m^2 w_j^2 (w_m,w_j))^{\ell_{m,j}} \mod \mathfrak{H}_{(3)},\quad 1\le m\le n-1,$$

$$r_n = \rho_n N \equiv \prod_{m=1}^{n-1} (w_m^2)^{\ell_{n,m}} \mod \mathfrak{H}_{(3)}.$$

From now on we assume that $\mathfrak{R} \subseteq \mathfrak{H}_{(3)}$, i.e.

$$\left(\frac{l_i}{l_j}\right) = 1 \ \text{ for all } \ 1\le i,j\le n,\ i\ne j.$$

By Gauss reciprocity this gives further restrictions on the l_i which means that one of the following two cases applies:

(i) $D = l_1\cdot\ldots\cdot l_n$ and all l_i are congruent 1 modulo 4,
(ii) $D = -l_1\cdot\ldots\cdot l_n$, where $l_1,\dots,l_{n-1}$ are congruent 1 modulo 4 and l_n is congruent 3 modulo 4.

This follows because if S contained two primes l_i, l_j which are congruent 3 modulo 4, then by quadratic reciprocity it would follow that $\ell_{i,j}+\ell_{j,i}=1$.

Theorem 4.4. *Let $K=\mathbb{Q}(\sqrt{D})$ be a quadratic number field where D satisfies one of the following conditions:*

(i) *$D = l_1\cdot\ldots\cdot l_n$ and all l_i are congruent 1 modulo 4,*
(ii) *$D = -l_1\cdot\ldots\cdot l_n$, where $l_1,\dots,l_{n-1}$ are congruent 1 modulo 4 and l_n is congruent 3 modulo 4,*

and assume that

$$\left(\frac{l_i}{l_j}\right) = 1 \text{ for all } 1 \leq i, j \leq n,\ i \neq j.$$

If we write the relations r_m, $1 \leq m \leq n$, modulo $\mathfrak{H}_{(4)}$ as

$$r_m \equiv \prod_{\substack{1 \leq i < j \leq n-1, \\ k \leq j}} ((w_i, w_j), w_k)^{e_{i,j,k,m}} \mod \mathfrak{H}_{(4)},$$

then for $1 \leq i < j \leq n-1$, $k < j$, $i \neq k$ and $1 \leq m \leq n-1$ (in case (i) also $m = n$ is allowed) we have

$$(-1)^{e_{i,j,k,m}} = \begin{cases} [l_i, l_j, l_k] & \text{if } \ m = j \text{ or } m = k, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let $\iota : H \to F$ be the inclusion map. Its Jacobi matrix $(\iota_{i,j})$ with respect to the bases

$$x_1x_n, x_2x_n, \ldots, x_{n-1}x_n, x_1^2, x_2^2, \ldots, x_n^2$$

of H and

$$x_1, \ldots, x_n$$

of F is given by the $n \times (2n-1)$-matrix of the form

$$(\iota_i^j)_{i,j} = \begin{pmatrix} 1 & 0 & 0 & & \ldots & & & 0 \\ 0 & 1 & 0 & & & & & \\ \vdots & & \ddots & & & & & \vdots \\ 0 & 0 & 0 & 1 & 0 & & & \\ 1 & 1 & \ldots & 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Let $\theta : H \to \mathfrak{H}$ be the projection map. Its Jacobi matrix $(\theta_{i,j})$ with respect to the bases

$$x_1x_n, x_2x_n, \ldots, x_{n-1}x_n, x_1^2, x_2^2, \ldots, x_n^2$$

of H and

$$w_1, \ldots, w_{n-1}$$

of $\mathfrak{H}$ is given by the $(n-1) \times (2n-1)$-matrix of the form

$$(\theta_i^j)_{i,j} = \begin{pmatrix} 1 & 0 & 0 & & \ldots & & 0 \\ 0 & 1 & 0 & & & & \\ \vdots & & \ddots & & & & \vdots \\ 0 & 0 & 0 & 1 & 0 & \ldots & 0 \end{pmatrix}$$

By the chain rule 2.23 we obtain that for $h \in H_{(r)}$ and multi-indices $I = (i_1, \ldots, i_r)$ with pairwise distinct $i_1, \ldots, i_r$ with $1 \leq i_1, \ldots, i_r \leq n-1$ the following relations hold:

$$\varepsilon^{\mathfrak{H}}_{I,2}(hN) = \varepsilon^H_{I,2}(h), \quad \varepsilon^F_{I,2}(h) = \varepsilon^H_{I,2}(h).$$

We remark that for I as above the map $\varepsilon^F_{I,2}$ vanishes on N. The vanishing on the generators is trivial and the vanishing on the whole of N follows by induction on the length of I from 2.18. Let $I = (i, j, k)$, and let $1 \leq m \leq n$. By our

assumptions we obtain that $\rho_m \in F_{(3)}$, hence by [9], Lemma 7.2, we may write $\rho_m N = \tilde{\rho}_m N$ with $\tilde{\rho}_m \in H_{(3)}$. Therefore we have

$$\begin{aligned}\varepsilon^{\mathfrak{H}}_{(j,i,k),2}(r_m) &= \varepsilon^{\mathfrak{H}}_{(j,i,k),2}(\rho_m N) = \varepsilon^{\mathfrak{H}}_{(j,i,k),2}(\tilde{\rho}_m N)\\ &= \varepsilon^{H}_{(j,i,k),2}(\tilde{\rho}_m) = \varepsilon^{F}_{(j,i,k),2}(\tilde{\rho}_m)\\ &= \varepsilon^{F}_{(j,i,k),2}(\rho_m).\end{aligned}$$

Hence, for $m \leq n-1$ (and $m \leq n$ in case (i)) we obtain

$$e_{i,j,k,m} = \varepsilon^{\mathfrak{H}}_{(j,i,k),2}(r_m) = \delta_{j,m}\mu_2(i,k,j) + \delta_{k,m}\mu_2(j,i,k).$$

This implies the result by 3.12 □

The above theorem gives a partial description of the pairings

$$\begin{aligned}P_m:\ H^1(G(K_{S_\infty}/K)) \times H^1(G(K_{S_\infty}/K)) \times H^1(G(K_{S_\infty}/K)) &\\ \xrightarrow{\langle\cdot,\cdot,\cdot\rangle} \quad H^2(G(K_{S_\infty}/K)) &\\ \xrightarrow{\mathrm{tr}_{r_m}} \quad \mathbb{Z}/2\mathbb{Z} &\end{aligned}$$

induced by the triple Massey product and the trace maps (see the appendix), where the coefficients are $\mathbb{Z}/2\mathbb{Z}$. We remark that for imaginary quadratic number fields K the cohomology groups $H^i(G(K_{S_\infty}/K)) = H^i(G(K_\varnothing/K))$ have the following interpretations:

$$H^1(G(K_\varnothing/K)) = (\mathrm{Cl}(K)/2)^*$$

where $\mathrm{Cl}(K)$ denotes the ideal class group of K and * the Pontryagin dual, and $H^2(G(K_\varnothing/K))$ can be described by the exact sequence

$$0 \longrightarrow \{\pm 1\} \longrightarrow H^2(G(K_\varnothing/K))^* \longrightarrow {}_2\,\mathrm{Cl}(K) \longrightarrow 0.$$

In this case the above pairings are therefore pairings

$$(\mathrm{Cl}(K)/2)^* \times (\mathrm{Cl}(K)/2)^* \times (\mathrm{Cl}(K)/2)^* \to \mathbb{Z}/2\mathbb{Z}.$$

Example 4.5. For the quadratic number fields

$$\begin{aligned}&\mathbb{Q}(\sqrt{13\cdot 17\cdot 53\cdot 433}),\ \mathbb{Q}(\sqrt{17\cdot 89\cdot 373\cdot 257}), \mathbb{Q}(\sqrt{5\cdot 29\cdot 181\cdot 241}),\\ &\mathbb{Q}(\sqrt{-5\cdot 41\cdot 61\cdot 131}),\ \mathbb{Q}(\sqrt{-5\cdot 29\cdot 181\cdot 59}), \mathbb{Q}(\sqrt{-13\cdot 17\cdot 53\cdot 43})\end{aligned}$$

the pairings P_1, P_2, P_3 are nontrivial.

In particular, this yields new examples for nontrivial triple Massey products in the Galois cohomology of number fields.

We remark that the appearance of the above pairings is much more natural in the following context. Let p be an odd prime number, and K be a quadratic number field. We denote the the p-class field tower of K by $K_\varnothing$. There is an operation of $G(K/\mathbb{Q})$ on the cohomology groups $H^i(G(K_\varnothing/K)) = H^i(G(K_\varnothing/K), \mathbb{Z}/p\mathbb{Z})$. We have a decomposition

$$H^i(G(K_\varnothing/K)) = H^i(G(K_\varnothing/K))^+ \oplus H^i(G(K_\varnothing/K))^-$$

into eigenspaces. It is well-known, see [15], lemma 4.1, that

$$H^1(G(K_\varnothing/K))^+ = H^2(G(K_\varnothing/K))^+ = 0.$$

In particular, the cup product

$$H^1(G(K_\varnothing/K)) \times H^1(G(K_\varnothing/K)) \overset{\cup}{\to} H^2(G(K_\varnothing/K))$$

is trivial, since it is $G(K/\mathbb{Q})$-equivariant. In particular, there are triple Massey products on $H^1(G(K_\varnothing))$, which, together with the trace maps with respect to relations r_m as in the case of $p = 2$, induce pairings

$$\begin{aligned} P_m : H^1(G(K_\varnothing/K)) \times H^1(G(K_\varnothing/K)) \times H^1(G(K_\varnothing/K)) & \\ \overset{\langle\cdot,\cdot,\cdot\rangle}{\longrightarrow} & \ H^2(G(K_\varnothing/K)) \\ \overset{\mathrm{tr}_{r_m}}{\longrightarrow} & \ \mathbb{Z}/p\mathbb{Z}. \end{aligned}$$

For imaginary quadratic number fields K, these are pairings of the form

$$P_m : (\mathrm{Cl}(K)/p)^* \times (\mathrm{Cl}(K)/p)^* \times (\mathrm{Cl}(K)/p)^* \overset{\langle\cdot,\cdot,\cdot\rangle}{\to} ({}_p\mathrm{Cl}(K))^* \overset{\mathrm{tr}_{r_m}}{\to} \mathbb{Z}/p\mathbb{Z}$$

It would be interesting to find examples where these pairings are nontrivial.

Appendix A. Massey products

In this appendix we give an account of the connection between Massey products and Fox differential calculus. This has been studied by us independently from Morishita, whose results have appeared in [12]. We prove a statement that is contained in Cor. 2.2.3 of [12], but our approach seems different. This result is sufficient to obtain a cohomological interpretation of our arithmetical results.

Let G be a pro-p-group and let A be a commutative ring considered as a trivial discrete G-module. In this exposition we will be merely concerned with Massey products on the group $H^1(G, A)$, hence we will give a definition of Massey products only in this restricted sense. For a general definition of Massey products on the level of cochains we refer to [2], §1 and [10]. We denote by $C^*(G, A)$ the standard inhomogeneous cochain complex. We recall some definitions from [4].

Definition A.1. Let $v_1, \dots, v_m$ be elements of $H^1(G, A)$. A collection $a = (a_{ij})$, $1 \le i, j \le m$, $(i, j) \ne (1, m)$ of cochains in $C^1(G, A)$ is called a **defining set** for the Massey product $\langle v_1, \dots, v_m\rangle$ if the following conditions are fulfilled:

(i) $a_{ii} = v_i$ for all $1 \le i \le m$.
(ii) If $\tilde{a}_{ij}$ is defined by

$$\tilde{a}_{ij} = \sum_{l=i}^{j-1} a_{il} \cup a_{l+1j}, \quad 1 \le i < j \le m,$$

then for $(i, j) \ne (1, m)$ it holds that $\tilde{a}_{ij} = \partial a_{ij}$.

The element $\tilde{a}_{1m}$ is a cocycle as well and its cohomology class in $H^2(G, A)$ is called the value of the defining set a. We say that the **Massey product $\langle v_1, \dots, v_m\rangle$ is defined** if there exists a defining system for it. In this case the **Massey product** is just the set of the values of all of its defining sets. The single Massey product $\langle v_1\rangle$ is v_1 by definition. The **indeterminacy** $\mathrm{In}\langle v_1, \dots, v_m\rangle$ is defined as

$$\mathrm{In}\langle v_1, \dots, v_m\rangle = \{a - b \mid a, b \in \langle v_1, \dots, v_m\rangle\}.$$

The Massey product $\langle v_1, \dots, v_m \rangle$ is called **uniquely defined** if $\mathrm{In}\langle v_1, \dots, v_m \rangle = 0$. It is called **strictly defined** if for all i, j with $1 \leq j - i \leq m - 2$ we have that $\langle v_i, \dots, v_j \rangle = 0$.

Let

$$1 \to R \to F \to G \to 1$$

be a minimal presentation of G, where F is the free pro-p-group on generators $x_1, \dots, x_n$. Then the inflation map

$$\inf : H^1(G, \mathbb{Z}/p\mathbb{Z}) \to H^1(F, \mathbb{Z}/p\mathbb{Z})$$

is an isomorphism by which we identify both groups. Since F is free we have $H^2(F, \mathbb{Z}/p\mathbb{Z}) = 0$, and from the exact 5-term sequence we obtain an isomorphism

$$\mathrm{tg} : H^1(R, \mathbb{Z}/p\mathbb{Z})^G \to H^2(G, \mathbb{Z}/p\mathbb{Z}).$$

Therefore any element $\rho \in R$ gives rise to a map

$$\mathrm{tr}_\rho : H^2(G, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z},$$

which is defined by $\varphi \mapsto (\mathrm{tg}^{-1}\, \varphi)(\rho)$ and is called the **trace map** with respect to ρ.

The following lemma is obtained as in [4]. For $v_1, \dots, v_m \in H^1(G, \mathbb{Z}/p\mathbb{Z})$ and a multi-index $I = (i_1, \dots, i_r) \in \mathcal{M}_r^n$ we write $\langle v_I \rangle$ for the Massey product $\langle v_{i_1}, \dots, v_{i_r} \rangle$.

Lemma A.2. *Let $\chi_1, \dots, \chi_n$ be a basis of $H^1(G, \mathbb{Z}/p\mathbb{Z})$. Assume that $0 \in \langle \chi_J \rangle$ for all multi-indices $J \in \mathcal{M}_r^n$ with $1 < r < m$. Let $v_1, \dots, v_m \in H^1(G, \mathbb{Z}/p\mathbb{Z})$. Then the Massey product $\langle v_1, \dots, v_m \rangle$ is strictly and uniquely defined. In particular this gives a multilinear map*

$$\langle \cdot, \dots, \cdot \rangle : H^1(G, \mathbb{Z}/p\mathbb{Z})^m \to H^2(G, \mathbb{Z}/p\mathbb{Z}).$$

If the conclusion of the above lemma holds we say that there is a **well-defined m-fold Massey product on $H^1(G, \mathbb{Z}/p\mathbb{Z})$**.

We are now ready to state the main result of this appendix.

Theorem A.3. *Assume that $R \subseteq F_{(m)}$. Then there is a well-defined m-fold Massey product*

$$\langle \cdot, \dots, \cdot \rangle : H^1(G, \mathbb{Z}/p\mathbb{Z})^m \to H^2(G, \mathbb{Z}/p\mathbb{Z})$$

Let $v_1, \dots, v_m \in H^1(G, \mathbb{Z}/p\mathbb{Z}) = H^1(F, \mathbb{Z}/p\mathbb{Z})$. We have that

$$\mathrm{tr}_f \langle v_1, \dots, v_m \rangle = (-1)^{m-1} \sum_{I=(i_1,\dots,i_m) \in \mathcal{M}_m^n} v_1(x_{i_1}) \cdot \ldots \cdot v_m(x_{i_m}) \varepsilon_{I,p}(f)$$

for all $f \in R$.

Proof. Using A.2, we will establish the first assertion using the dual basis $\chi_1, \dots, \chi_n$ of $H^1(F, \mathbb{Z}/p\mathbb{Z})$ of the basis $x_1, \dots, x_n$ of F. It is easily seen that in order to obtain the second statement, it suffices to show that

$$\varepsilon_{I,p}(f) = (-1)^{m-1} \mathrm{tr}_f \langle \chi_I \rangle$$

for each $I \in \mathcal{M}_m^n$.

For a multi-index $I = (i_1, \dots, i_r) \in \mathcal{M}^n$ and $1 \leq k < l \leq r$ let

$$I_{kl} = (i_k, \dots, i_l).$$

For $I \in \mathcal{M}^n$ with $|I| < m$ we set

$$a_{ij} = (-1)^{j-i} \varepsilon_{I_{ij},p} \text{ for } 1 \leq i < j \leq |I|.$$

We remark that this element of $C^1(F, \mathbb{Z}/p\mathbb{Z})$ factorizes through F/R because of our assumptions and can therefore be interpreted as an element of $C^1(G, \mathbb{Z}/p\mathbb{Z})$ as well. For $I \in \mathcal{M}^n$ with $1 \leq |I| \leq m$ we will show by induction on $|I|$ that the following claim holds:

(i) The (a_{ij}) form a defining set for $\langle \chi_I \rangle \subseteq H^2(G, \mathbb{Z}/p\mathbb{Z})$ (resp. $H^1(G, \mathbb{Z}/p\mathbb{Z})$ if $|I| = 1$).
(ii) For $1 < |I| = r$ in $C^2(F, \mathbb{Z}/p\mathbb{Z})$ there is the following identity:

$$\inf_G^F \tilde{a}_{1r} = (-1)^{r-1} \partial \varepsilon_{I,p}.$$

Let $|I| = 1$, say $I = (k)$. Because of 2.18 $\varepsilon_{(k),p}$ is a homomorphism from F to $\mathbb{Z}/p\mathbb{Z}$, and we have that

$$\varepsilon_{(i),p}(x_j) = \delta_{ij} = \chi_i(x_j).$$

Hence $\varepsilon_{(i),p} = \chi_i$ which implies the claim for $|I| = 1$. Let $I = (i_1, \dots, i_r)$, $1 < r \leq m$. From the case $|I| = 1$ it follows that

$$a_{kk} = \varepsilon_{(i_k),p} = \chi_{i_k}.$$

We have to show that

$$\tilde{a}_{kl} = \partial a_{kl}$$

holds for all $1 \leq k < l \leq r$, $(k, l) \neq (1, r)$. Inductively, we obtain that

$$\inf_G^F \tilde{a}_{kl} = (-1)^{l-k} \partial \varepsilon_{I_{kl},p}.$$

Due to our assumptions $\varepsilon_{I_{kl},p}$ factorizes over R and we even have that

$$\tilde{a}_{kl} = (-1)^{l-k} \partial \varepsilon_{I_{kl},p} = \partial a_{kl} \in C^2(G, \mathbb{Z}/p\mathbb{Z}).$$

At this point we remark that this implies in particular that $0 \in \langle \chi_I \rangle$. It remains to show that

$$\inf_G^F \tilde{a}_{1r} = (-1)^{r-1} \partial \varepsilon_{I,p}.$$

We set

$$b = (-1)^{r-1} \inf_G^F \tilde{a}_{1r}.$$

Since $H^2(F, \mathbb{Z}/p\mathbb{Z}) = 0$, there exists an element $u_I \in C^1(F, \mathbb{Z}/p\mathbb{Z})$ with

$$b = \partial u_I.$$

By subtracting the homomorphism

$$h : F \to \mathbb{Z}/p\mathbb{Z},\ h(x_j) = u_I(x_j)$$

we may assume that

$$u_I(x_j) = 0 \text{ for } j = 1, \dots, n.$$

The element $b \in H^2(F, \mathbb{Z}/p\mathbb{Z})$ is by definition given by

$$\begin{aligned} b(x,y) &= (-1)^{r-1} \sum_{l=1}^{r-1} a_{1l}(x) a_{l+1,r}(y) \\ &= (-1)^{r-1} \sum_{l=1}^{r-1} (-1)^{l-1} \varepsilon_{I_{1l},p}(x) (-1)^{r-l-1} \varepsilon_{I_{l+1,r},p}(y) \\ &= -\sum_{l=1}^{r-1} \varepsilon_{I_{1l},p}(x) \varepsilon_{I_{l+1,r},p}(y). \end{aligned}$$

Hence we obtain

$$\begin{aligned} u_I(xy) - \varepsilon_{I,p}(xy) &= u_I(x) + u_I(y) + \sum_{l=1}^{r-1} \varepsilon_{I_{1l},p}(x) \varepsilon_{I_{l+1,r},p}(y) - \varepsilon_{I,p}(xy) \\ &= u_I(x) - \varepsilon_{I,p}(x) + u_I(y) - \varepsilon_{I,p}(y) \end{aligned}$$

for all $x, y \in F$. This equation implies

$$\varepsilon_{I,p}(x_i^{-1}) = u_I(x_i^{-1})$$

for all $i = 1, \ldots, n$. Furthermore it holds that

$$u_I(x_i) = \varepsilon_{I,p}(x_i) = 0$$

for all $i = 1, \ldots, n$. An induction on the reduced word length using the above equation shows that $\varepsilon_{I,p}$ and u_I coincide on the discrete free group generated by $x_1, \ldots, x_n$. Due to the continuity of both maps they are identical on F. Therefore the claim is proved.

By the induction we have additionally obtained that $0 \in \langle \chi_I \rangle$ for all $I \in \mathcal{M}^n$ with $|I| < m$. By A.2 this implies

$$\langle \chi_I \rangle = 0 \text{ for all } I \in \mathcal{M} \text{ with } 1 < |I| < m$$

and that $\langle \chi_I \rangle$ is uniquely defined for $I \in \mathcal{M}^n$ with $|I| = m$. This implies the first statement of the theorem.

Next we will show that

$$\varepsilon_{I,p} \in H^1(R, \mathbb{Z}/p\mathbb{Z})^G$$

for all $I \in \mathcal{M}$ with $1 \leq |I| \leq m$. For $|I| < m$ this is obvious as $\varepsilon_{I,p}|_R = 0$. Assume that $I = (i_1, \ldots, i_m)$. The fact that $\varepsilon_{I,p}$ lies in $H^1(R, \mathbb{Z}/p\mathbb{Z})$ follows, using 2.18, from the vanishing of $\varepsilon_{J,p}$ on R for $|J| < m$. We will show the G-invariance. Let $x \in R, y \in F$. Then

$$\varepsilon_{I,p}(y^{-1}xy) = \varepsilon_{I,p}(x(x,y)) = \varepsilon_{I,p}(x) + \varepsilon_{I,p}((x,y)).$$

If we expand $\varepsilon_{I,p}((x,y))$ with the help 2.18 we obtain

$$\begin{aligned} \varepsilon_{I,p}((x,y)) &= \varepsilon_{I,p}(x) + \varepsilon_{I,p}(x^{-1}) + \varepsilon_{I,p}(y) + \varepsilon_{I,p}(y^{-1}) + \varepsilon_{i_1,p}(y) \varepsilon_{i_2 \ldots i_m,}(y^{-1}) \\ &\quad + \ldots + \varepsilon_{i_1 \ldots i_{m-1},p}(y) \varepsilon_{i_r,p}(y^{-1}) \\ &= \varepsilon_{I,p}(xx^{-1}) + \varepsilon_{I,p}(yy^{-1}) \\ &= 0 \end{aligned}$$

which implies the G-invariance. In order to finish the proof of the theorem we remark that

$$\inf_G^F \tilde{a}_{1r} = (-1)^{r-1}\partial\varepsilon_{I,p}I$$

in combination with the explicit construction of the transgression map, cf. [13] (1.6.5), yields

$$\mathrm{tg}(\varepsilon_{I,p}|_R) = [(-1)^{|I|-1}\tilde{a}_{1r}] = (-1)^{|I|-1}\langle\chi_I\rangle.$$

By the definition of the trace map we obtain the statement of the theorem. □

As is already remarked in the proof of the above theorem, for the dual basis $\chi_1, \ldots, \chi_n$ of $H^1(F, \mathbb{Z}/p\mathbb{Z})$ of the basis $x_1, \ldots, x_n$ of F we obtain the formula

$$\varepsilon_{I,p}(f) = (-1)^{m-1}\,\mathrm{tr}_f\langle\chi_I\rangle$$

for each $I \in \mathcal{M}_m^n$ and $f \in R$. In combination with 2.20 this shows that the relation structure of G modulo $F_{(m+1)}$ can be computed by Massey products. This was already pointed out 25 years ago in [9], Remark after (2.22), where a "connection between relations in $F_{(m)}$, for $m \geq 2$, and the Massey products" is mentioned, but no exact statement nor proof is given.

References

[1] Chen, K.T., Fox, R.H., Lyndon, R.C.: *Free differential calculus, IV. The quotient groups of the lower central series* Ann. of Math. 68, no.1(1958), 81-95

[2] Deninger, C.: *Higher order operations in Deligne cohomology.* Invent. Math. 120(1995), 289-315

[3] Dixon, J.D., du Sautoy, M.P.F., Mann, A., Segal, D.: *Analytic pro-p Groups* (2nd ed.), Cambridge Stud. Adv. Math. 61, Cambridge Univ. Press (1999)

[4] Fenn, R.: *Techniques of Geometric Topology.* London Math. Soc. Lect. Notes 57 Cambridge 1983

[5] Fenn, R., Sjerve, D.: *Basic commutators and minimal Massey products.* Can. J. Math. 36 (1984), 1119-1146

[6] Hall, M.: *The theory of groups.* Macmillan Company, New York 1968

[7] Haberland, K.: *Galois Cohomology of Algebraic Number Fields.*, Deutscher Verlag der Wiss., Berlin, 1978

[8] Ihara, Y.: *On Galois representations arising from towers of coverings of* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. Invent. Math. 86 (1986), 427-459

[9] Koch, H.: *On p-extensions with given ramification.* Appendix 1 in [7]

[10] Kraines, D.: *Massey higher products.* Trans. Am. Math. Soc. 124 (1996), 431-449

[11] Morishita, M.: *On certain analogies between knots and primes.* J. reine u. angew. Math. 550 (2002), 141-167

[12] Morishita, M.: *Milnor invariants and Massey products for prime numbers.* Compositio Math. 140 (2004), 69-83

[13] Neukirch, J., Schmidt, A., Wingberg, K.: *Cohomology of number fields.* Springer 2000

[14] Rédei, L. *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I.* J. reine u. angew. Math. 171 (1934), 55-60

[15] Schoof, R. *Infinite class field towers of quadratic fields* J. reine u. angew. Math. 372 (1986), 209-220

Universität Heidelberg, Mathematisches Institut, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany.

E-mail address: vogel@mathi.uni-heidelberg.de

URL: http://www.rzuser.uni-heidelberg.de/~dvogel2/