INAUGURAL-DISSERTATION

zur

Erlangung der Doktorwürde

der

Naturwissenschaftlich-Mathematischen

Gesamtfakultät

der

Ruprecht-Karls-Universität

Heidelberg

vorgelegt von
Diplom-Mathematiker Denis Vogel
aus Karl-Marx-Stadt

Tag der mündlichen Prüfung: 10. Februar 2004

Massey products in the Galois cohomology of number fields

Gutachter: Prof. Dr. Kay Wingberg

Priv.-Doz. Dr. Alexander Schmidt

Inhaltsangabe

In dieser Arbeit untersuchen wir die Relationenstruktur der Galoisgruppe der maximal ausserhalb einer endlichen Primstellenmenge S unverzweigten p-Erweiterung $\mathbb{Q}_S(p)$ von $\mathbb{Q}$ sowie die der Galoisgruppe des p-Klassenkörperturms eines quadratischen Zahlkörpers, wobei p eine Primzahl ist. Diese Gruppen können durch Sätze von Koch über Erzeugende und Relationen angegeben werden. Bei den Relationen handelt es sich hierbei um Elemente der freien pro-p-Gruppe F auf einem bestimmten minimalen Erzeugendensystem jener Galoisgruppen. Sie können durch Klassenkörpertheorie modulo dem dritten Schritt der Zassenhaus-Filtrierung $F_{(3)}$ von F beschrieben werden.
Für den Fall, dass die Relationen in $F_{(3)}$ liegen, beschäftigen wir uns mit der Struktur der Relationen modulo dem vierten Schritt der Zassenhaus-Filtrierung $F_{(4)}$ von F. Für $p = 2$ geben wir eine explizite Beschreibung derselben. Unsere Überlegungen basieren darauf, dass die oben erwähnten Galoisgruppen in ihrer Struktur ähnlich zu Gruppen von Verschlingungen aus der Knotentheorie sind. Wir übertragen Techniken aus der Knotentheorie in unsere Situation. Insbesondere beschäftigen wir uns mit dem Fox-Differentialkalkül auf freien pro-p-Gruppen und Masseyprodukten in der Kohomologie von pro-p-Gruppen und geben eine kohomologische Interpretation jenes Differentialkalküls. Dies stellt eine Verallgemeinerung des bekannten Zusammenhangs zwischen dem Cupprodukt in der Kohomologie einer pro-p-Gruppe und ihrer Relationenstruktur dar. Dadurch ist es uns möglich, ein zahlentheoretisches Analogon des Satzes von Porter-Turaev aus der Knotentheorie zu zeigen. Es beschreibt einen Zusammenhang zwischen bestimmten Massey-Produkten auf der Kohomologie der Galoisgruppe von $\mathbb{Q}_S(p)/\mathbb{Q}$ und den von Morishita eingeführten Milnor-Invarianten auf jener Galoisgruppe.
Wir verallgemeinern Morishitas Ergebnisse über die Milnor-Invarianten von $G(\mathbb{Q}_S(2)/\mathbb{Q})$ und erhalten eine vollständige Beschreibung des dreifachen Masseyproduktes auf der Galoiskohomologiegruppe $H^1(G(\mathbb{Q}_S(2)/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$ und damit der Relationenstruktur von $G(\mathbb{Q}_S(2)/\mathbb{Q})$ modulo $F_{(4)}$.
Während die Relationenstruktur modulo $F_{(3)}$ nach Koch eng mit dem Legendresymbol auf der Primstellenmenge S zusammenhängt, ist die Relationenstruktur modulo $F_{(4)}$ mit dem sogenannten Rédei-Symbol auf S verknüpft. Jenes Dreier-Symbol wurde in den dreissiger Jahren des vergangenen Jahrhunderts von Rédei eigeführt.
Wir benutzen die Ergebnisse über die Galoisgruppe von $\mathbb{Q}_S(2)/\mathbb{Q}$, um mit Hilfe eines Abstiegsverfahrens Informationen über die Galoisgruppe des 2-Klassenkörperturms eines quadratischen Zahlkörpers zu erhalten. Wir geben eine partielle Beschreibung der gesuchten Relationenstruktur und zeigen, dass diese eng mit dem Rédei-Symbol auf der Menge der Primteiler der Diskriminante des quadratischen Zahlkörpers verbunden ist.

Abstract

In this thesis we study the relation structure of the Galois group of the maximal outside a given set S unramified p-extension $\mathbb{Q}_S(p)$ of $\mathbb{Q}$ and of the Galois group of the p-class field tower of a quadratic number field, where p is a prime number. These groups can be presented in terms of generators and relations by theorems due to Koch. Here the relations are elements of the free pro-p-group F on a certain minimal system of generators of the above Galois groups. They can be described by class field theory modulo the third step $F_{(3)}$ of the Zassenhaus filtration of F.

We assume that the relations lie inside $F_{(3)}$ and study the structure of the relations modulo the fourth step $F_{(4)}$ of the Zassenhaus filtration of F. For $p = 2$ we give an explicit description of these relations. Our approach is based on the observation that the above Galois groups have a similar structure as groups of links occuring in knot theory. We carry over techniques of knot theory to our situation. In particular we study the Fox differential calculus on free pro-p-groups and Massey products in the cohomology of pro-p-groups, and we give a cohomological interpretation of this differential calculus. This is a generalization of the well-known relationship between the cup product in the cohomology of a pro-p-group and its relation structure. Therefore we are able to show a number theoretic analogue of the theorem of Porter-Turaev from knot theory. It describes a connection between certain Massey products in the cohomology of the Galois group of $\mathbb{Q}_S(p)/\mathbb{Q}$ and the Milnor invariants of this group introduced by Morishita.

We generalize Morishita's results on the Milnor invariants for $\mathbb{Q}_S(2)$ and obtain a complete description of the triple Massey product on the cohomology group $H^1(G(\mathbb{Q}_S(2)/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$, and thereby of the relation structure of $G(\mathbb{Q}_S(2)/\mathbb{Q})$ modulo $F_{(4)}$.

While the relation structure modulo $F_{(3)}$ is closely linked to the Legendre symbol by Koch's results, the relation structure modulo $F_{(4)}$ is intimately connected to the so-called Rédei symbol on S. This triple symbol was introduced in the thirties of the last century by Rédei.

We use the results on the Galois group of $\mathbb{Q}_S(2)/\mathbb{Q}$ in order to deduce information on the Galois group of the 2-class field tower of a quadratic number field by means of a descent procedure. We give a partial description of the sought-after relation structure and show that is closely connected to the Rédei symbol on the set of prime divisors of the discriminant of the quadratic number field.

Contents

Introduction

Algebraic number theory takes inspirations from many fields, including analysis, geometry, group theory and algebraic topology. Over the last years it has been realized that several concepts of algebraic number theory bear a certain structural resemblance to parts of knot theory. This has led both number theorists and topologists to the new field of so-called arithmetic topology, which is dedicated to geometric analogies between knots and primes, between Galois groups of number fields and fundamental groups of three-manifolds and between Alexander and Iwasawa theory.
The objective of this thesis is the study of relations in certain Galois groups, namely the Galois group of the maximal p-extension of $\mathbb{Q}$ unramified outside a set of primes S and the 2-class field tower of quadratic number fields. These Galois groups will turn out to be quite similar to certain groups of links. In link theory, relations can be studied by means of the Fox differential calculus. This gives rise to the Milnor $\bar{\mu}$-invariants of links, which are intimately connected to Massey products in the cohomology of the link complement via the theorem of Porter-Turaev. For a more detailed view of this, we refer the reader to the appendix. We take up the link theoretical point of view and study the Fox differential calculus on free pro-p-groups. We prove a result which gives a cohomological interpretation of the Fox differential calculus in terms of Massey products in the cohomology of pro-p-groups. These results are then applied to the above mentioned Galois groups. We will explain all that now in more detail.
We fix a prime p and consider the Galois group $G_S(p)$ of the maximal pro-p-extension $\mathbb{Q}_S(p)$ of $\mathbb{Q}$ which is unramified outside a set of primes S which is given by

$$S = \{l_1, \dots, l_n, \infty\}, \quad l_i \equiv 1 \mod p, \ i = 1, \dots, n.$$

Let $\mathfrak{l}_i$ be a fixed extension of l_i to $\mathbb{Q}_S(p)/\mathbb{Q}$. For $1 \leq i \leq n$ let σ_i be an element in $G = G_S(p)$ with the following properties:

(a) σ_i is a lift of the Frobenius automorphism of $\mathfrak{l}_i$,

(b) the restriction of σ_i to the maximal abelian subextension $\mathbb{Q}_S(p)^{(2)}/\mathbb{Q}$ of $\mathbb{Q}_S(p)/\mathbb{Q}$ is equal to $(\lambda_i, \mathbb{Q}_S(p)^{(2)})/\mathbb{Q})$, 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 $G_S(p)$ such that

(a) τ_i is a generator of the inertia group $T_{\mathfrak{l}_i}$ of $\mathfrak{l}_i$ in $\mathbb{Q}_S(p)/\mathbb{Q}$;

(b) the restriction of τ_i to $\mathbb{Q}_S(p)^{(2)}/\mathbb{Q}$ equals $(\alpha_i, \mathbb{Q}_S(p)^{(2)}/\mathbb{Q})$, where α_i denotes the idèle whose l_i-component is a primitive root g_i modulo l_i and all other components are 1.

By a well-known result due to Fröhlich and Koch [K2] there is a minimal presentation

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

of $G_S(p)$ where F is a free pro-p-group on generators $x_1, \ldots, x_n$ 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 $\mathcal{R} = \{\rho_i\}_{1 \leq i \leq n}$ with

$$\rho_i = x_i^{l_i - 1}(x_i^{-1}, y_i^{-1}),$$

where y_i is a preimage of σ_i. Here, we write $(a, b) = a^{-1}b^{-1}ab$ for elements $a, b \in F$. It holds that

$$\rho_i \equiv x_i^{l_i - 1} \prod_{j \neq i} (x_i, x_j)^{\ell_{i,j}} \mod F_{(3)}$$

where $F_{(3)}$ denotes the third step of the Zassenhaus filtration of F which will be explained later and

$$\zeta_p^{\ell_{i,j}} = \left(\frac{l_i}{l_j}\right)_p \in \mu_p$$

where $(l_i/l_j)_p$ denotes the p-th power residue symbol in $\mathbb{Q}_{l_j}$ and μ_p is the group of p-th roots of unity. We recall that $(l_i/l_j)_p$ is defined as the p-th root of unity which is determined by

$$\left(\frac{l_i}{l_j}\right)_p \equiv l_i^{\frac{l_j - 1}{p}} \mod l_j \mathbb{Z}_{l_j}.$$

If the relations ρ_i sit inside $F_{(3)}$ one may ask what they look like when considered modulo $F_{(4)}$. Another number theoretical question that stimulated our considerations 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 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. For an imaginary quadratic number field this is the same as $K_\varnothing$, the maximal unramified 2-extension of K. We make use of the fact that one can descend from $G_S(2)$ to $G(K_{S_\infty}/\mathbb{Q})$ and then pass to the subgroup $G(K_{S_\infty}/K)$. There is the following theorem due to Koch, which is obtained by this process. 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-p-group $\mathfrak{H}$ with generators $w_1, \ldots, w_{n-1}$ where n denotes the number of prime factors of D. The defining relations are given by

$$\begin{aligned} r_i &\equiv w_i^{2\ell_{i,n}} \prod_{\substack{1\le j\le n-1\\ j\neq i}} (w_i^2 w_j^2 (w_i, w_j))^{\ell_{i,j}} \mod \mathfrak{H}_{(3)}, \quad 1 \le i \le n-1 \\ r_n &\equiv \prod_{i=1}^{n-1} (w_i^2)^{\ell_{n,i}} \mod \mathfrak{H}_{(3)} \end{aligned}$$

Once again, one may ask what happens if the relations lie inside $\mathfrak{H}_{(3)}$. What do they look like modulo $\mathfrak{H}_{(4)}$?

Let us explain the techniques used to settle these questions. As already mentioned, 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 [I], 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. Among others, they share the following properties, see also (1.1.1):

$$\frac{\partial x_i}{\partial x_j} = \delta_{ij}, \qquad \frac{\partial(\alpha\beta)}{\partial x_i} = \frac{\partial \alpha}{\partial x_i}\varepsilon_{\mathbb{Z}_p[\![F]\!]}(\beta) + \alpha\frac{\partial \beta}{\partial x_i}, \quad \alpha, \beta \in \mathbb{Z}_p[\![F]\!].$$

There is an isomorphism

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

where $\mathbb{Z}_p\langle\langle X_1, \ldots, X_n\rangle\rangle$ denotes the ring of formal power series over $\mathbb{Z}_p$ in n non-commuting variables $X_1, \ldots, X_n$. For elements $f \in F$ we consider the so-called Magnus expansion

$$\psi(f) = 1 + \sum_I \varepsilon_I(f) X_I, \quad \varepsilon_I(f) \in \mathbb{Z}_p,$$

where the summation runs over all integers $r \ge 1$ and all finite sequences $(i_1, \ldots, i_r)$ of integers $1 \le i_1, \ldots, i_r \le n$, and X_I denotes $X_{i_1} \cdot \ldots \cdot X_{i_r}$ for $I = (i_1, \ldots, i_r)$. It can be seen that

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

holds for all $f \in F$. We denote by $\varepsilon_{I,p} : F \to \mathbb{Z}/p\mathbb{Z}$ the reduction of ε_I modulo p. This map gives a nice characterization of a certain filtration on F, the so-called Zassenhaus filtration, which is defined as follows. For $n \geq 1$ let the ideal $I^n(F)$ of $\mathbb{F}_p[\![F]\!]$ be the n-th power of the augmentation ideal $I(F)$. Then the filtration

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

is called the Zassenhaus filtration of F. It holds 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 generating sets for the quotients $F_{(k)}/F_{(k+1)}$ which consist of powers of so-called basic commutators. If $f \in F_{(k)}$ is given in terms of these generators, we show that the determination of $\varepsilon_{I,p}(f)$ with $|I| = k$ can be reduced to a determination of maps that are given in a purely combinatorial way, see (1.1.15) and (1.1.25).

The Fox differential calculus has a nice cohomological interpretation in terms of Massey products. Cup products are cohomology operations of first order. If the cup product vanishes, secondary cohomology products are defined, so-called triple Massey products. Inductively one can define Massey products of higher order. We explain here the case of triple Massey products. Let G be a profinite group and A a discrete trivial G-module. Assume that the cup product

$$H^1(G, A) \times H^1(G, A) \stackrel{\cup}{\to} H^2(G, A)$$

vanishes. Then there exists a triple Massey product

$$\langle \cdot, \cdot, \cdot \rangle : H^1(G, A) \times H^1(G, A) \times H^1(G, A) \to H^2(G, A)$$

which is defined as follows. Denote by $C^*(G, A)$ the standard inhomogeneous cochain complex and by $\cup$ the cup product on the level of cochains. Let a_1, a_2, $a_3 \in H^1(G, A) \subseteq C^1(G, A)$. We choose α_{12}, $\alpha_{23} \in C^1(G, A)$ with $a_1 \cup a_2 = \partial\alpha_{12}$ and $a_2 \cup a_3 = \partial\alpha_{23}$, and define

$$\langle a_1, a_2, a_3 \rangle := [a_1 \cup \alpha_{23} + \alpha_{12} \cup a_3].$$

The triple Massey product is multilinear and it fulfills the following rules:

$$\langle a_1, a_2, a_3 \rangle = \langle a_3, a_2, a_1 \rangle, \quad \langle a_1, a_2, a_3 \rangle + \langle a_2, a_3, a_1 \rangle + \langle a_3, a_1, a_2 \rangle = 0.$$

For a general definition of Massey products, see chapter 1, §2. We point out that in general the target of Massey products is not $H^2(G, A)$, but a quotient of it. If the target is $H^2(G, A)$, we speak of so-called 'well-defined' Massey products. For a strict definition of this notion, see loc. cit.

Since we are interested in the relation structure of pro-p-groups and its connection to Massey products, we will consider the case $A = \mathbb{Z}/p\mathbb{Z}$ and consider m-fold (well-defined) Massey products of type

$$H^1(G, \mathbb{Z}/p\mathbb{Z})^m \to H^2(G, \mathbb{Z}/p\mathbb{Z}).$$

We prove the following theorem, which can be seen as an analogue of a key step in the proof of the theorem of Porter-Turaev from topology.

Theorem. *Let*

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

be a minimal presentation of the finitely generated pro-p-group G. Let $x_1, \ldots, x_n$ be a basis of F and let $\chi_1, \ldots, \chi_n$ be the dual $\mathbb{Z}/p\mathbb{Z}$-basis of $H^1(F, \mathbb{Z}/p\mathbb{Z}) = H^1(G, \mathbb{Z}/p\mathbb{Z})$, i.e. $\chi_i(x_j) = \delta_{ij}$. Assume that $R \subseteq F_{(m)}$. Then there are well-defined k-fold Massey products

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

for all $1 < k \leq m$. Let

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

denote the trace map corresponding to $f \in R$ which is defined in chapter 1,§2. For each multiindex $(i_1, \ldots, i_k)$ with $1 < k \leq m$ and $1 \leq i_r \leq n$, $r = 1, \ldots, k$, we have

$$\mathrm{tr}_f \langle \chi_{i_1}, \ldots, \chi_{i_k} \rangle = (-1)^{k-1} \varepsilon_{(i_1,\ldots,i_k),p}(f)$$

for all $f \in R$. In particular it holds that $R \subseteq F_{(m)}$ if and only if all k-fold Massey products on $H^1(G, \mathbb{Z}/p\mathbb{Z})$ vanish for $1 < k < m$.

We remark that by our results on the Fox differential calculus this gives a method to calculate these Massey products. In particular this result yields a generalization of the connection between cup products and relations of G in $F^{(2,p)}$ modulo $F^{(3,p)}$ where $F^{(2,p)}$ and $F^{(3,p)}$ denote the second and third step of the descending p-central series of F, respectively, see [NSW], Prop. 3.9.13.
We now come back to the arithmetical questions we started with. Morishita [M] introduced the notion of Milnor invariants of the group $G_S(p)$. This concept has its origin in link theory, where Milnor invariants of links are considered. The resemblance between the theorem of Chen-Milnor on link groups (see the appendix, Thm. (A.1)) and Koch's theorem on $G_S(p)$ explained above results in the following definition of Milnor invariants. Let $r \geq 1$ and $1 \leq i_1, \ldots, i_r \leq n$. The Milnor μ_p-invariant of $G_S(p)$ corresponding to $I = (i_1, \ldots, i_r)$ is defined by

$$\mu_p(I) = \varepsilon_{I',p}(y_{i_r}),$$

where $I' = (i_1, \ldots, i_{r-1})$. Note that we use the notation μ_p for the Milnor invariants as well as for the group of p-th roots of unity, but it should always be clear from the context what is meant. We remark that it is shown in [M] that the Milnor invariants are independent of the choices we made and are invariants of $G_S(p)$. In link theory the theorem of Porter-Turaev provides a connection between Milnor invariants and Massey products, see the appendix, Thm. (A.2) and Thm. (A.3). Using our algebraic result on the connection between the Fox differential calculus and Massey products, and the structure of the relations of $G_S(p)$, we obtain the following number theoretical analogue.

Theorem. *Let $1 < m \leq p^e$ where $e = \max\{r \geq 1 |\ p^r | (l_i - 1)$ for all $1 \leq i \leq n\}$ and assume that $\mu_p(J) = 0$ for all multiindices J with $1 < |J| < m$. Then we have a well-defined m-fold Massey product*

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

Let $I = (i_1, \ldots, i_m)$. Then

$$\begin{aligned} \mathrm{tr}_{\rho_{i_k}} \langle \chi_{i_1}, \ldots, \chi_{i_m} \rangle &= (-1)^m (\delta_{i_m i_k} \mu_p(i_1, \ldots, i_m) - \delta_{i_1 i_k} \mu_p(i_2, \ldots, i_m, i_1) \\ &\quad - \binom{l_{i_k} - 1}{m} \delta_{I=(i_1,\ldots,i_1)}). \end{aligned}$$

It is easy to see that for the second order Milnor invariants $\mu_p(i,j)$ it holds that

$$\zeta_p^{\mu_p(i,j)} = \zeta_p^{\ell_{j,i}} = \left(\frac{l_j}{l_i}\right)_p, \quad 1 \leq i \neq j \leq n$$

and that $\mu_p(i,i) = 0$ for all $1 \leq i \leq n$.
From now on we assume that $p = 2$. We want to understand triple Massey products, or, which is equivalent by our theorem above, third order Milnor invariants on $G_S(2)$. By the above result on second order Milnor invariants (or directly from the structure of the relations) the cup product

$$H^1(G_S(2)) \times H^1(G_S(2)) \xrightarrow{\cup} H^2(G_S(2))$$

(where from now on $H^i(G_S(2))$ denotes cohomology with $\mathbb{Z}/2\mathbb{Z}$-coefficients) vanishes if and only if all l_i are $\equiv 1 \mod 4$ and we have

$$\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \leq i, j \leq n,\ i \neq j.$$

In this situation triple Massey products are well-defined. Morishita has calculated the third order Milnor invariants $\mu_2(i,j,k)$ for $1 \leq i, j, k \leq n$ pairwise distinct. We calculate the third order Milnor invariants also in the remaining cases and therefore we get a complete description of the triple Massey product. It turns out that the third order Milnor invariants and the triple Massey product are described by the so-called Rédei symbol. In the 1930's Rédei introduced this 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. We prove the following

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

$$\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \leq i, j \leq n,\ i \neq j.$$

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

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

Let $\chi_1, \ldots, \chi_n$ be the $\mathbb{Z}/2\mathbb{Z}$-basis of $H^1(F, \mathbb{Z}/2\mathbb{Z}) = H^1(G_S(2))$ which corresponds to the basis $x_1, \ldots, x_n$ of F in the above minimal presentation of $G_S(2)$, i.e. $\chi_i(x_j) = \delta_{ij}$. The triple Massey product

$$\langle \cdot, \cdot, \cdot \rangle : H^1(G_S(2)) \times H^1(G_S(2)) \times H^1(G_S(2)) \to H^2(G_S(2))$$

is determined by

$$(-1)^{\mathrm{tr}_{\rho_m}\langle \chi_i, \chi_j, \chi_k \rangle} = \begin{cases} [l_i, l_j, l_k] & \text{if} \quad m = i \text{ and } m \neq k, \\ [l_i, l_j, l_k] & \text{if} \quad m \neq i \text{ and } m = k, \\ 1 & \text{otherwise.} \end{cases}$$

In particular this result allows a complete determination of the relations R of $G_S(2)$ modulo $F_{(4)}$.

This result enables us to give examples of S in which the triple Massey product on $H^1(G_S(2))$ does not vanish, as well as to give examples in which it is trivial. We also give some examples in which we calculate the relations explicitly 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, 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 the triple Massey product on the groups $H^1(G(K_{S_\infty}/K)) = H^1(G(K_{S_\infty}/K), \mathbb{Z}/2\mathbb{Z})$. We prove the following theorem.

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

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

and assume that $\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \leq i, j \leq n, \ i \neq j$. Then the cup product

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

vanishes completely. Let $\chi_1, \ldots, \chi_{n-1}$ be the dual $\mathbb{Z}/2\mathbb{Z}$-basis of $H^1(\mathfrak{H}, \mathbb{Z}/2\mathbb{Z}) = H^1(G(K_{S_\infty}/K), \mathbb{Z}/2\mathbb{Z})$ to the basis $w_1, \ldots, w_{n-1}$ of $\mathfrak{H}$ in the above minimal presentation of $G(K_{S_\infty}/K)$, i.e. $\chi_i(w_j) = \delta_{ij}$. For the triple Massey product

$$\langle \cdot, \cdot, \cdot \rangle : H^1(G(K_{S_\infty}/K)) \times H^1(G(K_{S_\infty}/K)) \times H^1(G(K_{S_\infty}/K)) \to H^2(G(K_{S_\infty}/K))$$

the following formula holds for pairwise distinct i, j, k with $1 \leq i, j, k \leq n-1$ and $1 \leq m \leq n$:

$$(-1)^{\mathrm{tr}_{r_m}\langle \chi_i, \chi_j, \chi_k \rangle} = \begin{cases} [l_i, l_j, l_k] & \text{if} \quad m = i \text{ or } m = k, \\ 1 & \text{otherwise.} \end{cases}$$

In particular we are able to give examples of both real and imaginary quadratic number fields which have nontrivial triple Massey products on the cohomology groups $H^1(G(K_{S_\infty}/K), \mathbb{Z}/2\mathbb{Z})$. We remark that for imaginary quadratic number fields there is an isomorphism

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

where $\mathrm{Cl}(K)$ denotes the ideal class group of K and * denotes the Pontryagin dual, hence the pairings

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

(here the coefficients are $\mathbb{Z}/p\mathbb{Z}$) induced by the Massey product and the trace maps are pairings

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

In the final section, we make a few comments about the situation for odd p.
In summary, one may say that the use of methods adapted from knot theory has given us some insight in the relation structure of pro-p-groups in general and in some arithmetic applications as well. We hope that in the future it will be possible to exploit some analogies further.

I would like to thank my supervisor Kay Wingberg for his suggestion to study Massey products and his constant encouragement. Furthermore, I would like to thank Tobias Horn, Alexander Schmidt and Otmar Venjakob for numerous discussions on the subject. Thanks go to the DFG for their financial support.

Chapter I

Algebraic part

§1 The Fox differential calculus on free pro-p-groups

In knot theory the Fox differential calculus on free groups is an important tool for the determination of knot invariants. We want to apply similar techniques for the determination of the structure of pro-p-groups. In this section we will provide the necessary facts about the Fox differential calculus.
Originally, the Fox differential calculus has been developed for discrete free groups. It is possible to carry it over to free pro-p-groups. Our presentation will be similar to the one in [F]. Many of the statements proved there for discrete groups have very elementary proofs which immediately carry over to our situation and which we will therefore omit here.
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.

(1.1.1) Theorem. *([I],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

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

The free derivatives have the following properties:

(a)

$$\frac{\partial x_i}{\partial x_j} = \delta_{ij},$$

(b)

$$\frac{\partial(\alpha\beta)}{\partial x_i} = \frac{\partial\alpha}{\partial x_i}\varepsilon_{\mathbb{Z}_p[\![F]\!]}(\beta) + \alpha\frac{\partial\beta}{\partial x_i}, \quad \alpha,\beta \in \mathbb{Z}_p[\![F]\!],$$

(c)

$$\frac{\partial f^{-1}}{\partial x_i} = -f^{-1}\frac{\partial f}{\partial x_i}, \quad f \in F,$$

(d)

$$\frac{\partial f^a}{\partial x_i} = b\frac{\partial f}{\partial x_i} \text{ for any } b \in \mathbb{Z}_p[\![F]\!] \text{ with } b(f-1) = f^a - 1, \quad f \in F.$$

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 $I = (i_1, \ldots, i_r)$ 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 $I = (i_1, \ldots, i_r)$ we denote by $|I| = r$ the **length** of I. If multi-indices $I_1 = (i_1, \ldots, i_r)$, $I_2 = (j_1, \ldots, j_s)$ are given, we denote by

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

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 $\mathbb{Z}_p\langle\!\langle X_1, \ldots, X_n\rangle\!\rangle$ of formal power series in n non commuting variables $X_1, \ldots, X_n$ over $\mathbb{Z}_p$, and an isomorphism is given by

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

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

$$M(f) = \psi(f) = 1 + \sum_I \varepsilon_I(f) X_I, \; \varepsilon_I(f) \in \mathbb{Z}_p,$$

where I runs over all multi indices of height n. For each multi-index I this gives us a map

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

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

(1.1.2) Proposition. *Let $f \in F$ and $I = (i_1, \ldots, i_r)$. Then*

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

We will introduce some filtrations on pro-p-groups.

(1.1.3) Definition. *Let G be a pro-p-group and let q be a power of p. Then the* **descending q-central series** *of G is the filtration $\{G^{(i,q)}\}_{i\geq 1}$ recursively defined by*

$$G^{(1,q)} = G, \quad G^{(i+1,q)} = (G^{(i,q)})^q[G^{(i,q)}, G],$$

where $[G^{(i,q)}, G]$ and $(G^{(i,q)})^q$ are the closed subgroups topologically generated by the commutators $(x, y) = x^{-1}y^{-1}xy$, $x \in G^{(i,q)}, y \in G$, and by the q-th powers of elements of $G^{(i,q)}$, respectively.
If $q = 0$, then we denote this series by $\{G_i\}_{i\geq 1}$, i.e.

$$G_1 = G, \quad G_{i+1} = [G_i, G].$$

It is called the **descending central series** *of G.*

We collect some properties of the maps ε_I, which are completely analogous to the discrete situation.

(1.1.4) Proposition. *Let $\alpha, \beta \in \mathbb{Z}_p[\![F]\!], f \in F_i, g \in F_j$ and let I be a multi-index. Then the following assertions hold:*

(a)
$$\varepsilon_I(\alpha\beta) = \sum_{I_1 I_2 = I} \varepsilon_{I_1}(\alpha)\varepsilon_{I_2}(\beta).$$

(b) If $|I| < i$, then $\varepsilon_I(f) = 0$.

(c) If $|I| \leq \max(i, j)$, then $\varepsilon_I(fg) = \varepsilon_I(f) + \varepsilon_I(g)$.

(d) If $|I| = i + j$, $I = I_1I_2 = I_2'I_1'$, where I_1, I_2, I_1', I_2' are multi-indices with $|I_1| = |I_1'| = i$, $|I_2| = |I_2'| = j$, then

$$\varepsilon_I((f, g)) = \varepsilon_{I_1}(f)\varepsilon_{I_2}(g) - \varepsilon_{I_1'}(f)\varepsilon_{I_2'}(g).$$

Proof. This follows the same way as in [F], 4.2.7, 4.4.1 □

We want to study the effect of ε_I on words from F in more detail. We need the following definition.

(1.1.5) Definition. *The* **basic commutators** *of weight one are $x_1, \ldots, x_n$ and their ordering is $x_1 > \ldots > x_n$. 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 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.*

(1.1.6) Example. *We obtain the following basic commutators of small weight:*

weight 1*:* x_i, $1 \leq i \leq n$.

weight 2*:* (x_i, x_j), $1 \leq i < j \leq n$.

weight 3*:* $((x_i, x_j), x_k)$, $1 \leq i < j \leq n$, $k \leq j$.

We have the following theorem, which follows directly from an analogous statement for discrete free groups, cf. [H], Thm. 11.2.4, by completion.

(1.1.7) Theorem. *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 describe the effect of ε_I on the basic commutators or more generally on the so-called bracket arrangements. We collect some definitions from [FS].

(1.1.8) Definition. *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.*

We will associate a tree $T(\beta)$ with a root to a bracket arrangement β.

(1.1.9) Definition. *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 I.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 $\mathcal{T}$.*

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. I.2.

(1.1.10) Definition. *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 $T(\beta, I) = \overset{x_i}{\cdot}$. 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*

Figure I.1: $T(\beta)$

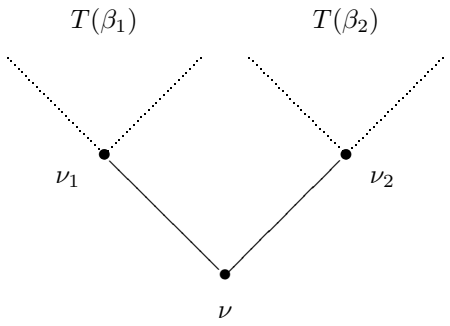
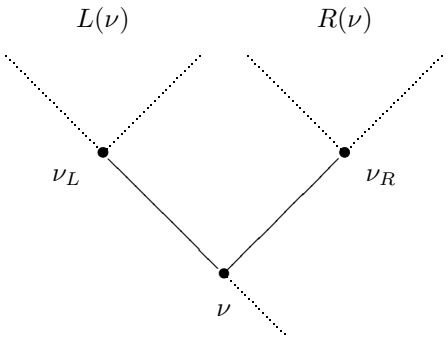


Figure I.2:



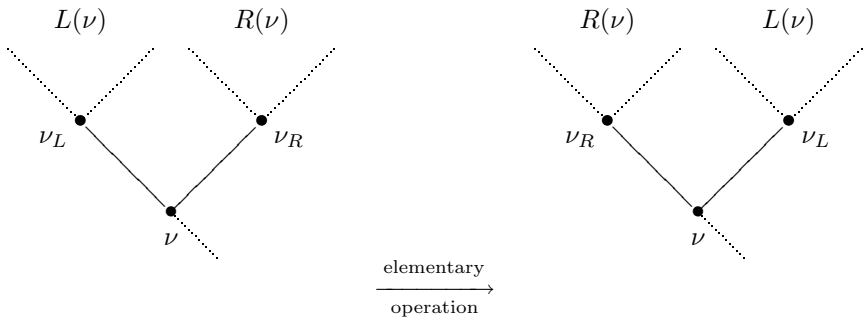
$U(\nu) = L(\nu) \cup R(\nu)$
$\nu_L =$ left-hand vertex
$\nu_R =$ right-hand vertex

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

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

(1.1.11) Definition. *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.I.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* $\mathrm{Op}(T)$.

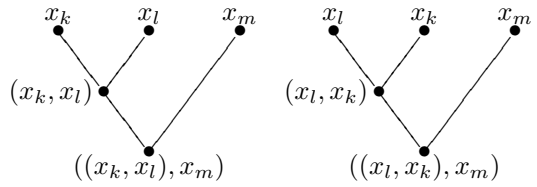
Figure I.3: elementary operation



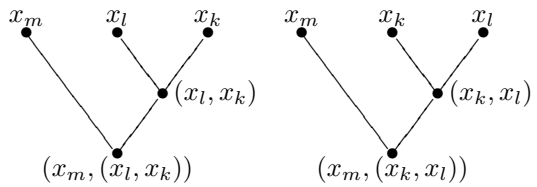
(1.1.12) Example. *(a) Let $1 \leq k, l \leq n$, $k \neq l$. There are two admissible operations on the labelled tree $T = T((*,*),(k,l)) \in \mathcal{T}_2$ whose results can be seen on the following picture. The corresponding signs are noted below the trees.*

$+1$ $\qquad$ -1

(b) 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.



$+1$ $\qquad$ -1



$+1$ $\qquad$ -1

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 [FS], lemma 5.5, we obtain the following result.

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

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

(1.1.14) Example. *(a) Let $\beta = (*,*)$, $I = (k,l)$ with $k \neq l$. We obtain*

$$\mathcal{L}((x_k, x_l)) = X_{kl} - X_{lk}$$

(b) 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. Recall that $\mathcal{M}_k^n$ denotes the set of multi-indices of length k. In later applications we will need a description of the map

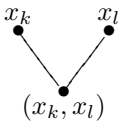
$$\eta_k : \mathcal{M}_k^n \to \mathcal{C}_k, \quad I \mapsto \sum_{\beta \in C_k} \varepsilon_I(\beta(I))\beta.$$

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

(1.1.15) Proposition. *The map η_k is given by*

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

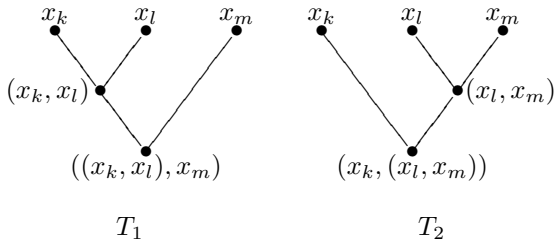
(1.1.16) Example. *(a) Let $I = (k,l)$ with $1 \leq k, l \leq n$. There is exactly one labelled tree $T \in \mathcal{T}_2$ with $\mathcal{I}(T) = I$:*



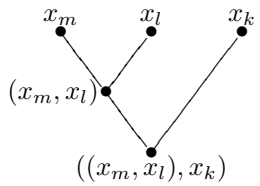
If $k < l$ this corresponds to a basic commutator, while for $k < l$ the tree has to be flipped to correspond to a basic commutator. Hence

$$\eta_2(I) = \begin{cases} (x_k, x_l) & \text{if } k < l, \\ -(x_l, x_k) & \text{if } k > l, \\ 0 & \text{if } k = l. \end{cases}$$

(b) 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 $\mathcal{I}(T_i) = I$, $i = 1, 2$:



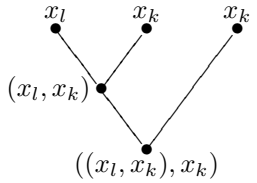
The labelled tree T_1 corresponds to a basic commutator, and no nontrivial admissible operation will produce a labelled tree from T_1 that corresponds to a basic commutator as well. The labelled tree T_2 does not correspond to a basic commutator, but the labelled tree



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

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

(c) Let $I = (k, l, k)$ with $1 \leq k, l \leq n$ and assume that $k > l$. As in the last example we have two trees T_1, T_2 with $\mathcal{I}(T_i) = I$, $i = 1, 2$. Both trees can be transformed into



using an admissible operation of sign -1. Hence

$$\eta_3(I) = -2((x_l, x_k), x_k).$$

The above examples show in particular that the naive guess that

$$\eta_k(I) = \pm c$$

where c is a basic commutator of length $|I|$, which one might make after taking a look at $k = 2$, is not true. This map depends heavily on the combinatorics of trees and becomes more and more complex with growing k. In particular it seems rather hopeless to obtain closed formulae.

We will now introduce a filtration that will turn out to be in very close connection to Massey products, and it is very important in our arithmetic applications as well.

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

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

is called the **Zassenhaus filtration** *of G.*

There is the following result on the Zassenhaus filtration, see [DDMS], Thm. 12.9.

(1.1.18) Theorem. (Jennings) *The Zassenhaus filtration can be recursively described as follows:*

$$G_{(n)} = G^p_{(\lceil n/p \rceil)} \prod_{i+j=n} (G_{(i)}, G_{(j)}),$$

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

We remark that the second step $G^{(2)}$ of the Zassenhaus Filtration and the second step $G^{(2,p)}$ of the descending p-central series coincide. For $p = 2$ also the third step $G_{(3)}$ of the Zassenhaus filtration and the third step $G^{(3,2)}$ of the descending 2-central series coincide.
The following result due to Lazard, see [DDMS], Thm. 11.2., is very useful for explicit calculations.

(1.1.19) Theorem. (Lazard) *For each n,*

$$G_{(n)} = \prod_{ip^j \geq n} G_i^{p^j}.$$

For free pro-p-groups F the last proposition allows us in particular to write down generating sets for the quotients $F_{(k)}/F_{(k+1)}$ using the description of the bases of F_k/F_{k+1} as given in (1.1.7). 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 $F_i^{p^j} \subset F_{(n)}$ then $F_{i+1}^{p^j} \subset F_{(n+1)}$. If $i \nmid n$ then $F_i^{p^j} \subset F_{(n)}$ implies $F_i^{p^j} \subset F_{(n+1)}$. In particular we have the following

(1.1.20) Corollary. *A generating system of $F_{(n)}/F_{(n+1)}$ can be represented by a set of the form*

$$C_{i_1}^{p^{j_1}} \dot\cup C_{i_2}^{p^{j_2}} \dot\cup \ldots \dot\cup C_{i_m}^{p^{j_m}}$$

or the empty set. Here $i_1 < i_2 < \ldots < i_m$ are divisors of n with $i_r p^{j^r} = n$ for $r = 1, \ldots, m$ (but not all of these divisors do necessarily occur.)

It is a rather combinatorial problem to write the i_k and j_k down explicitly in a more or less closed formula, so we will just extract the information that we need for our arithmetical applications, that is, we will write down generating sets for $F_{(2)}/F_{(3)}$ and $F_{(3)}/F_{(4)}$. But we point out, that given a concrete prime p and a concrete k it is very easy to calculate the i_k and j_k. This holds as well in the following example.

(1.1.21) Example. *(a) It holds that*

$$F_{(2)}/F_{(3)} = \begin{cases} F_2/F_2^pF_3 & \text{if} \quad p \neq 2, \\ F^2F_2/F^4F_2^2F_3 & \text{if} \quad p = 2. \end{cases}$$

In particular, for $p \neq 2$ the set C_2 of basic commutators of weight 2 represents a generating set of $F_{(2)}/F_{(3)}$ as a $\mathbb{Z}/p\mathbb{Z}$-module. For $p = 2$ such a generating set is represented by $C_1^2 \cup C_2$.

(b) It holds that

$$F_{(3)}/F_{(4)} = \begin{cases} F_3/F_3^pF_4 & \text{if} \quad p \neq 3, \\ F^3F_3/F^9F_2^3F_4 & \text{if} \quad p = 3. \end{cases}$$

In particular, for $p \neq 3$ the set C_3 of basic commutators of weight 3 represents a generating set of $F_{(3)}/F_{(4)}$ as a $\mathbb{Z}/p\mathbb{Z}$-module. For $p = 3$ such a generating set is represented by $C_1^3 \cup C_3$.

(c) A generating set for $F_{(4)}/F_{(5)}$ is given by C_4 if $p \neq 2$ and by $C_1^4 \cup C_2^2 \cup C_4$ for $p = 2$.

For the first two of the above generating sets we will show later that they are indeed bases.
Let $\varepsilon_{I,p} : F \to \mathbb{Z}/p\mathbb{Z}$ denote the reduction of ε_I modulo p. A similar result as (1.1.4) holds for the Zassenhaus filtration:

(1.1.22) Proposition. *Let $\alpha, \beta \in \mathbb{Z}_p[\![F]\!]$, $f \in F_{(i)}$, $g \in F_{(j)}$ and let I be a multi-index. Then the following assertions hold:*

(a)
$$\varepsilon_{I,p}(\alpha\beta) = \sum_{I_1I_2=I} \varepsilon_{I_1,p}(\alpha)\varepsilon_{I_2,p}(\beta).$$

(b) If $|I| < i$, then $\varepsilon_{I,p}(f) = 0$.

(c) If $|I| \leq \min(i, j)$, then $\varepsilon_{I,p}(fg) = \varepsilon_{I,p}(f) + \varepsilon_{I,p}(g)$.

(d) If $|I| = i + j$, $I = I_1I_2 = I_2'I_1'$, where I_1, I_2, I_1', I_2' are multi-indices with $|I_1| = |I_1'| = i$, $|I_2| = |I_2'| = j$, then

$$\varepsilon_{I,p}((f, g)) = \varepsilon_{I_1,p}(f)\varepsilon_{I_2,p}(g) - \varepsilon_{I_1',p}(f)\varepsilon_{I_2',p}(g).$$

Proof. The first statement follows from (1.1.4) by reducing modulo p. It is easily seen that (b) implies (c) and (d). A stronger statement than (b) will be given in (1.1.24) □

We will often need the following formula later which follows from (1.1.22).

(1.1.23) Lemma. *Let I be a multi-index and $1 \leq i \leq n$. Then*

$$\varepsilon_{I,p}(x_i^a) = \begin{cases} \binom{a}{|I|} & \text{if} \quad I = (i, \ldots, i), \\ 0 & \text{otherwise.} \end{cases}$$

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

(1.1.24) Lemma. *Let $f \in F$. Then:*

(a) $f \in F_k$ if and only if $\varepsilon_I(f) = 0$ for all multi-indices I with $|I| < k$.

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

Proof. (a) follows as in the discrete case, see [F], 4.4.5. (b) 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 generator system of $F_{(k)}$ modulo $F_{(k+1)}$ as given in (1.1.20). 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 $F_{(k)}$.

(1.1.25) Proposition. *Let I be multi-index of length k. Let $f \in F_{(k)}$ be represented modulo $F_{(k+1)}$ as a linear combination of elements of the generator system*

$$C_{i_1}^{p^{j_1}} \cup C_{i_2}^{p^{j_2}} \cup \ldots \cup C_{i_m}^{p^{j_m}}$$

of $F_{(k)}/F_{(k+1)}$ where $i_l p^{j_l} = k$, $l = 1, \ldots, m$. In order to calculate $\varepsilon_{I,p}(f)$ it is sufficient to know the maps η_{i_l} for $l = 1, \ldots, m$ which describe the effect of $\varepsilon_{I'}$ on basic commutators of weight I' where $|I'| = i_l$.

Proof. By (1.1.22) it is sufficient to calculate $\varepsilon_{I,p}$ on the elements of the generating system above. For the set C_k of basic commutators of weight k this is done by (1.1.15). 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 $I = I_1 \dots I_{p^r}$ of type w we associate a reduced decomposition $\tilde{I} = \tilde{I}_1 \dots \tilde{I}_{p^r-w}$ of type 0 by leaving out the empty multi-indices. We may then write

$$\varepsilon_{I,p}(c^{p^r}) = \sum_{w=0}^{p^r-1} \sum_{\substack{I=I_1\dots I_{p^r} \\ \text{of type } w}} \varepsilon_{\tilde{I}_1,p}(c) \cdot \ldots \cdot \varepsilon_{\tilde{I}_{p^r-w},p}(c)$$

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

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

hence $\varepsilon_{I,p}(c^{p^r})$ is determined by the knowledge of the map η_s from (1.1.15). □

A useful tool for making explicit calculations is the chain rule. In the discrete case there is a chain rule which involves the descending central series, see [FS], Thm.4.6. We will prove a chain rule which involves $\varepsilon_{I,p}$ and the Zassenhaus filtration. Its proof makes use of Jennings' theorem (1.1.18).

(1.1.26) Definition. *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.*

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

(1.1.27) Proposition. *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. We will use induction on k. For $k = 1$ it suffices to remark that the homomorphisms

$$f \mapsto \varepsilon^{F'}_{(i),p}(\phi(f)), \quad f \mapsto \sum_{j=1}^{k} \phi_i^j \varepsilon^F_{(j),p}(f)$$

from F to $\mathbb{Z}_p$ coincide on the base elements $x_1, \dots, x_n$ of F. Let $k > 1$. By Jennings' theorem (1.1.18) and (1.1.22) it is sufficient to consider the case where

f is of the form $f = (f_1, f_2)$ where $f_1 \in F_{k_1}$, $f_2 \in F_{k_2}$ and $k = k_1 + k_2$, and the case where $f = h^p$ where $h \in F_{(\lceil k/p \rceil)}$. Assume we are in the first case. Let I_1, J_1, I_1', J_1' denote multi-indices of length k_1 and I_2, J_2, I_2', J_2' multi-indices of length k_2. We use the summation convention, that repeated indices are summed over. Then we obtain by induction and (1.1.22)

$$\begin{aligned}
\varepsilon_{I,p}(\phi((f_1,f_2))) &= \varepsilon_{I,p}((\phi(f_1),\phi(f_2))) \\
&= \varepsilon_{I_1,p}(\phi(f_1))\varepsilon_{I_2,p}(\phi(f_2)) - \varepsilon_{I_2',p}(\phi(f_2))\varepsilon_{I_1'}(\phi(f_1)) \\
&= \phi_{I_1}^{J_1}\varepsilon_{J_1,p}(f_1)\phi_{I_2}^{J_2}\varepsilon_{J_2,p}(f_2) - \phi_{I_2'}^{J_2'}\varepsilon_{J_2',p}(f_2)\phi_{I_1'}^{1}J_1'\varepsilon_{J_1'}(f_1) \\
&= \phi_I^J(\varepsilon_{J_1,p}(f_1)\varepsilon_{J_2,p}(f_2) - \varepsilon_{J_2',p}(f_2)\varepsilon_{J_1',p}(f_1)) \\
&= \phi_I^J\varepsilon_{J,p}((f_1,f_2)).
\end{aligned}$$

Assume that $f = h^p$ with $h \in F_{(\lceil k/p \rceil)}$. By induction and (1.1.22) we obtain

$$\begin{aligned}
\varepsilon_{I,p}(\phi(h^p)) &= \sum_{I_1\ldots I_p=I} \varepsilon_{I_1,p}(\phi(h))\cdot\ldots\cdot\varepsilon_{I_p,p}(\phi(h)) \\
&= \sum_{\substack{I_1\ldots I_p=I \\ I_j\neq I \text{ for } 1\leq j\leq p}} \varepsilon_{I_1,p}(\phi(h))\cdot\ldots\cdot\varepsilon_{I_p,p}(\phi(h)) \\
&= \sum_{\substack{I_1\ldots I_p=I \\ I_j\neq I \text{ for } 1\leq j\leq p}} \phi_{I_1}^{J_1}\varepsilon_{J_1,p}(h)\cdot\ldots\cdot\phi_{I_p}^{J_p}\varepsilon_{J_p,p}(h) + p\phi_I^J\varepsilon_J(h) \\
&= \sum_{I_1\ldots I_p=I} \phi_{I_1}^{J_1}\varepsilon_{J_1,p}(h)\cdot\ldots\cdot\phi_{I_p}^{J_p}\varepsilon_{J_p,p}(h) \\
&= \phi_I^J\varepsilon_{J,p}(h^p)
\end{aligned}$$

which implies the claim. □

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

(1.1.28) Definition. *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*

(a) $c_{\alpha(i)} = a_i$ *for* $i = 1, \dots, l$ *and* $c_{\beta(j)} = b_j$ *for* $j = 1, \dots, m$.

(b) Each index $k = 1, \dots, n$ *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* $R(S)$ *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 [CFL], lemma 3.3, and carries over directly to our situation.

(1.1.29) Proposition. *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*

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

(1.1.30) Example. *(a)* $\varepsilon_{(1),p} \cdot \varepsilon_{(1,1),p} = 3\varepsilon_{(1,1,1),p} + 2\varepsilon_{(1,1),p}$.

(b) If $f \in F_{(3)}$*, and* $1 \le i, j, k \le n$*, then*

$$\varepsilon_{(i,j,k),p}(f) + \varepsilon_{(j,i,k),p}(f) + \varepsilon_{(j,k,i),p}(f) = 0.$$

§2 Massey products in the cohomology of pro-p-groups

Let G be a pro-p-group and let A be a G-module. Massey products are examples of so-called secondary cohomology operations. They exist if the cup product

$$H^i(G, A) \times H^j(G, B) \xrightarrow{\cup} H^{i+j}(G, A \otimes B),$$

vanishes. For a general definition of Massey products on the level of cochains we refer to [D], §1 and [Kr]. In this exposition we will be merely concerned with Massey products on the group $H^1(G, A)$ where A is a trivial discrete G-module, hence we will give a definition of Massey products only in this restricted sense. We denote by $C^*(G, A)$ the standard inhomogeneous cochain complex.

(1.2.1) Definition. *Let* $u_1, \dots, u_m$ *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* $\langle u_1, \dots, u_m \rangle$ *if the following conditions are fulfilled:*

(a) $a_{ii} = u_i$ *for all* $1 \leq i \leq m$.

(b) If $\tilde{a}_{ij}$ *is defined by*

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

then for $(i,j) \neq (1,m)$ *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** $\langle \boldsymbol{u_1, \ldots, u_m} \rangle$ **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* $\langle u_1 \rangle$ *is* u_1 *by definition.*

It is easily verified that the $\partial \tilde{a}_{ij} = 0$ for all $1 \leq i < j \leq m$, hence the above definition makes sense. We remark that there seems to be no consistent sign convention throughout the literature. We have chosen the signs such that

$$\langle u_1, u_2 \rangle = u_1 \cup u_2$$

for $u_1, u_2 \in H^1(G,A)$. We imagine the cochains a_{ij} in an upper triangular matrix:

$$a = \begin{pmatrix} a_{11} & & & & a_{1m-1} & * \\ & & & & & a_{2m} \\ & a_{ii} & \ldots & a_{ij} & & \\ & & & \vdots & & \\ & & & a_{jj} & & \\ & & & & & \\ & & & & & a_{mm} \end{pmatrix}.$$

The cochain $\tilde{a}_{ij}$ is the 'scalar product' of the row left of a_{ij} by the column beneath a_{ij}. Then $\tilde{a}_{ij}$ is required to be a coboundary in $C^2(G,A)$, and we choose a_{ij} in such a way that $\partial a_{ij} = \tilde{a}_{ij}$. The cochains (a_{kl}), $i \leq k \leq l \leq j$, form a defining set for the Massey product $\langle u_i, \ldots, u_j \rangle$ whose value is necessarily 0 in order for a_{ij} to be defined. On the other hand the condition $0 \in \langle u_i, \ldots, u_j \rangle$ is not sufficient for the existence of a defining set.

(1.2.2) Definition. *The* **indeterminacy** $\mathrm{In}\langle u_1, \ldots, u_m \rangle$ *is defined as*

$$\mathrm{In}\langle u_1, \ldots, u_m \rangle = \{a - b \mid a, b \in \langle u_1, \ldots, u_m \rangle\}.$$

The Massey product $\langle u_1, \ldots, u_m \rangle$ *is called* **uniquely defined** *if the indeterminacy* $\mathrm{In}\langle u_1, \ldots, u_m \rangle = 0$. *It is called* **strictly defined** *if for all* i, j *with* $1 \leq j - i \leq m - 2$ *it holds that* $\langle u_i, \ldots, u_j \rangle = 0$.

There are the following results on unique and strict definedness of Massey products.

(1.2.3) Proposition. *Let $u_1, \dots, u_m \in H^1(G, A)$. Assume that the Massey product $\langle u_1, \dots, u_m \rangle$ is defined and let $1 \leq k \leq m$.*

(a) If $u_k = 0$ then $0 \in \langle u_1, \dots, u_m \rangle$.

(b) Let $u_k'', u_k' \in H^1(G, A)$ with $u_k = u_k' + u_k''$. If $\langle u_1, \dots, u_k', \dots, u_m \rangle$ is strictly defined then $\langle u_1, \dots, u_k'', \dots, u_m \rangle$ is defined and it holds that

$$\langle u_1, \dots, u_k' + u_k'', \dots, u_m \rangle \subseteq \langle u_1, \dots, u_k', \dots, u_m \rangle + \langle u_1, \dots, u_k'', \dots, u_m \rangle.$$

(c) Assume that $\langle u_1, \dots, u_m \rangle$ is strictly defined. Then $\langle u_1, \dots, u_m \rangle$ is uniquely defined if and only if

$$\langle u_1, \dots, u_{l-1}, x_l, u_{l+2}, \dots, u_m \rangle = 0$$

holds for any k with $1 \leq l \leq m-1$ and any $x_l \in H^1(G, A)$.

Proof. This follows exactly the same way as in [F], lemma 6.2.4 and [FS], lemma 2.2 □

From now on we assume that $A = \mathbb{Z}/p\mathbb{Z}$. In addition to the above result, we have

(1.2.4) Proposition. *Let $u_1, \dots, u_m \in H^1(G, \mathbb{Z}/p\mathbb{Z})$, $\lambda \in \mathbb{Z}/p\mathbb{Z}$, and let $1 \leq k \leq m$. Assume that $\langle u_1, \dots, u_m \rangle$ is defined. Then $\langle u_1, \dots, \lambda u_k, \dots, u_m \rangle$ is defined and it holds that*

$$\lambda \langle u_1, \dots, u_m \rangle \subseteq \langle u_1, \dots, \lambda u_k, \dots, u_m \rangle.$$

Proof. This is proved in the same way as [F], lemma 6.2.4 (ii). □

For later purposes the following elementary lemma will turn out to be useful. For elements $u_1, \dots, u_m \in H^1(G, \mathbb{Z}/p\mathbb{Z})$ and a multi-index $I = (i_1, \dots, i_r) \in \mathcal{M}_r^m$ let $\langle u_I \rangle$ denote the Massey product $\langle u_{i_1}, \dots, u_{i_r} \rangle$.

(1.2.5) Lemma. *Let G be a finitely generated pro-p-group. 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 $J = (j_1, \dots, j_r) \in \mathcal{M}_r^n$ with $1 < r < m$. Let $u_1, \dots, u_m \in H^1(G, \mathbb{Z}/p\mathbb{Z})$. Then the Massey product $\langle u_1, \dots, u_m \rangle$ is strictly and uniquely defined. In particular this gives a multilinear map*

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

Proof. This follows inductively from Proposition (1.2.3) and (1.2.5). □

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

In topology the theorem of Porter-Turaev provides a connection between Massey products and Milnor invariants of links, see the appendix, Thm.(A.2) and Thm.(A.3). In the next chapter we will provide a number theoretical analogue. In order to do this we will prove an algebraic result that provides a connection between Massey products and the Fox differential calculus and which has to be seen as an analogue to one of the key steps in the proof of the theorem of Porter-Turaev. In the topological context a proof is given that uses some geometric arguments, see [F],§6.3. Such a proof is not possible in our context but it is possible to succeed using purely cohomological arguments in our situation. As a simple application of the theorem a close relation between Massey products and the Zassenhaus filtration is revealed.

Let G be a finitely generated pro-p-group. Let

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

be a minimal presentation of G. 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.
Let $x_1, \ldots, x_n$ be a basis of F. Let $\chi_1, \ldots, \chi_n$ be the dual basis to $\bar{x}_1, \ldots, \bar{x}_n$ of $H^1(F, \mathbb{Z}/p\mathbb{Z}) = H^1(G, \mathbb{Z}/p\mathbb{Z})$, i.e. $\chi_i(x_j) = \delta_{ij}$ for all $i, j \in \{1, \ldots, n\}$. In analogy to one of the key steps in the proof of the theorem of Porter-Turaev from topology, cf. [F],Thm. 6.3.4, we have the following

(1.2.6) Theorem. *Assume that $R \subseteq F_{(m)}$. Then there are well-defined k-fold Massey products*

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

for all $1 < k \leq m$. For all multi-indices $I \in \mathcal{M}^n$ with $1 < |I| \leq m$ we have

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

for all $f \in R$. In particular all k-fold Massey products on $H^1(G, \mathbb{Z}/p\mathbb{Z})$ with $1 < k < m$ vanish completely.

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

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

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:

(a) 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 $|I| = 1$).

(b) 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 (1.1.22) $\varepsilon_{(k),p}$ 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 $I = (i_1, \ldots, i_r)$, $1 < r \leq m$. 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

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

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 (1.2.5) 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 (1.1.22), 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 (1.1.22) 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. [NSW] (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. □

The next statement follows by an inspection of the foregoing proof.

(1.2.7) Remark. *The above theorem (1.2.6) remains valid if we replace p by a power q of p which is arbitrary if G^{ab} is torsion free, and which is $\leq p^f$ if G^{ab} has torsion, where p^f is the maximal p-power such that G^{ab}/p^f is a free $\mathbb{Z}/p^f\mathbb{Z}_p$-module. The assumption that $R \subseteq F_{(m)}$ has to be replaced by*

$$\varepsilon_{I,q}|_R = 0$$

for all $I \in \mathcal{M}$ with $1 < |I| < m$.

(1.2.8) Remark. *The above theorem (1.2.6) remains valid if we replace the assumption $R \subseteq F_{(m)}$ by the assumption $0 \in \langle\chi_I\rangle$ for all $I \in \mathcal{M}^n$ with $1 < |I| < m$.*

Proof. This follows inductively from (1.2.6). □

We have the following characterization of the Zassenhaus filtration by means of Massey products.

(1.2.9) Corollary. *It holds that $R \subseteq F_{(k)}$ if and only if all m-fold Massey products on $H^1(G, \mathbb{Z}/p\mathbb{Z})$ vanish for $1 < m < k$.*

The shuffle property (1.1.29) of the $\varepsilon_{I,p}$ induces a shuffle property for the Massey product.

(1.2.10) Corollary. *Assume that $R \subseteq F_{(m)}$. Let $I \in \mathcal{M}^n$ be a multi-index with $|I| = m$. Let I_1, I_2 be nonempty multi-indices such that $I = I_1 I_2 = (i_1, \ldots, i_m)$. Let $a_{i_1}, \ldots, a_{i_m} \in H^1(G, \mathbb{Z}/p\mathbb{Z})$. Then*

$$\sum_{s \in \hat{\mathcal{S}}(I_1, I_2)} \langle a_{\mathfrak{r}(s)} \rangle = 0.$$

Proof. To each multi-index $J = (j_1, \ldots, j_m)$ we associate multi-indices J_1, J_2 with $J = J_1 J_2$, $|J_1| = |I_1|$, $|J_2| = |I_2|$. We define a multilinear map

$$\begin{aligned} \phi : H^1(G, \mathbb{Z}/p\mathbb{Z})^m &\to H^2(G, \mathbb{Z}/p\mathbb{Z}), \\ \chi_J &\mapsto \sum_{s \in \hat{\mathcal{S}}(J_1, J_2)} \langle \chi_{\mathfrak{r}(s)} \rangle. \end{aligned}$$

It can be verified that

$$\phi(a_I) = \sum_{s \in \hat{\mathcal{S}}(I_1, I_2)} \langle a_{\mathfrak{r}(s)} \rangle.$$

But the map ϕ is the zero map because for each $f \in R$, it holds by (1.1.29) that

$$\mathrm{tr}_f\Big(\sum_{s \in \hat{\mathcal{S}}(J_1, J_2)} \langle \chi_{\mathfrak{r}(s)} \rangle \Big) = \sum_{s \in \hat{\mathcal{S}}(J_1, J_2)} \varepsilon_{\mathfrak{r}(s), p}(f) = 0,$$

hence for each J we have

$$\sum_{s \in \hat{\mathcal{S}}(J_1, J_2)} \langle \chi_{\mathfrak{r}(s)} \rangle = 0.$$

This implies the claim. □

(1.2.11) Example. *(a) For $m = 2$ the shuffle property is just the skew symmetry of the cup product.*

(b) Assume that $R \subseteq F_{(3)}$. Then the shuffle property can be summarized in the following two equations. For all $a, b, c \in H^1(G, \mathbb{Z}/p\mathbb{Z})$ it holds that

$$\langle a, b, c \rangle + \langle b, a, c \rangle + \langle b, c, a \rangle = 0 \quad \textit{and} \quad \langle a, b, c \rangle = \langle c, b, a \rangle.$$

If we are given a relation $r \in F_{(k)}$ which is given modulo $F_{(k+1)}$ as a linear combination by elements of a generating set of $F_{(k)}/F_{(k+1)}$ as given in (1.1.20), then (1.1.25) and our algebraic main result (1.2.6) from above allow us to calculate trace maps of k-fold Massey products provided we have knowledge of the maps η_l where l are certain divisors of k. Thus the determination of Massey products is reduced to a purely combinatorial problem which involves certain operations on labelled trees. Conversely, if all Massey products of order $< k$ vanish and the k-fold Massey product is completely known, we can write down the relations explicitly.

We make a few remarks about continuous cochain cohomology. If G^{ab} is torsion free the trace map is also defined for $\mathbb{Z}_p$-coefficients:

$$tr_\rho : H^2(G, \mathbb{Z}_p) \to \mathbb{Z}_p,$$

where we denote by $H^i(G, \mathbb{Z}_p)$ the continuous cochain cohomology. If the Massey product $\langle u_1, \dots, u_r\rangle \in H^2(G, \mathbb{Z}/p^e\mathbb{Z})$ is uniquely defined for any e there exists a uniquely defined Massey product $\langle u_1, \dots, u_r\rangle \in H^2(G, \mathbb{Z}_p)$. From the results above we obtain

(1.2.12) Corollary. *Let G^{ab} be torsion free. Assume that $R \subseteq F_m$. Then there are well-defined k-fold Massey products*

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

for all $1 < k \leq m$. For all multi-indices $I \in \mathcal{M}^n$ with $1 < |I| \leq m$ it holds that

$$\varepsilon_I(f) = (-1)^{|I|-1} \operatorname{tr}_f\langle \chi_I\rangle$$

for all $f \in R$. In particular all k-fold Massey products on $H^1(G, \mathbb{Z}_p)$ with $1 < k < m$ vanish completely.

(1.2.13) Corollary. *Let G^{ab} be torsion free. Then $R \subseteq F_k$ if and only if all m-fold Massey products on $H^1(G, \mathbb{Z}_p)$ vanish for $1 < m < k$.*

We finish this section with a few comments about the connection between Massey products and the Bockstein homomorphism. The **Bockstein homomorphism**

$$B : H^1(G, \mathbb{Z}/p\mathbb{Z}) \to H^2(G, \mathbb{Z}/p\mathbb{Z})$$

is defined as the connecting homomorphism in the long exact cohomology sequence associated to

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

Assume that $k > 1$ and that the relations R of G satisfy the condition $R \subseteq F_{(k)}$. Then we may define a map

$$\begin{array}{rcl} \langle\cdot\rangle^k : H^1(G, \mathbb{Z}/p\mathbb{Z}) & \to & H^2(G, \mathbb{Z}/p\mathbb{Z}) \\ a & \mapsto & \langle \underbrace{a, \dots, a}_{k \text{ factors}}\rangle \end{array}$$

which maps a to the k-fold Massey product $\langle a, \dots, a\rangle$. By the shuffle property (1.2.10) we obtain that

$$\binom{k}{l}\langle a\rangle^k = 0$$

for all $1 \leq l < k$. Hence, if k is not a power of p, the map $\langle\cdot\rangle^k$ is the zero map.

(1.2.14) Lemma. *The map $\langle\cdot\rangle^{p^m}$ is a homomorphism of abelian groups for each $m \geq 1$.*

Proof. Let $a, b \in H^1(G, \mathbb{Z}/p\mathbb{Z})$. We set $k = p^m$. By (1.1.22) we obtain that

$$\langle a+b\rangle^k = \langle a\rangle^k + \langle b\rangle^k + \sum_{\substack{i,j>0\\ i+j=k}} \sum_{s\in\hat{\mathcal{S}}(A_i,B_j)} \langle C_{\mathfrak{r}(s)}\rangle$$

where A_i denotes the multi-index $(1,\ldots,1)$ of length i, B_j denotes the multi-index $(2,\ldots,2$ of length j and $C_{\mathfrak{r}(s)}$ denotes the tuple in which the i-th place equals a or b according to whether the i-th place in the multi-index $\mathfrak{r}(s)$ is 1 or 2. Hence, by (1.2.10) we have

$$\langle a+b\rangle^k = \langle a\rangle^k + \langle b\rangle^k$$

Thus the proposition is proved. □

For $k = p$ the map $\langle\cdot\rangle^p$ is essentially given by the Bockstein homomorphism.

(1.2.15) Proposition. *Assume that $R \subseteq F_{(p)}$. Then*

$$-B : H^1(G, \mathbb{Z}/p\mathbb{Z}) \to H^2(G, \mathbb{Z}/p\mathbb{Z})$$

coincides with

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

Proof. It is sufficient to show that

$$\mathrm{tr}_{\rho_j}(\langle\chi_i\rangle^p) = \mathrm{tr}_{\rho_j} B(\chi_i)$$

for all $i = 1,\ldots,n$ and $j \in J$ where $\{\rho_j \mid j \in J\}$ is a minimal system of generators of R as a normal subgroup of F. A generating system of $F_{(p)}/F_{(p+1)}$ is given by $C_1^p \cup C_p$. We may thus write

$$\rho_j = \prod_{k=1}^{n} x_k^{pa_k^j} \prod_{c\in C_p} c^{e_c}\rho_j'$$

with $a_k^j, e_c \in \mathbb{Z}/p\mathbb{Z}$, $\rho_j' \in F_{(p+1)}$. Let I denote the multi-index $(i,\ldots,i)$ of length p. By (1.2.6) and the proof of (1.1.25) (or alternatively (1.1.23)) we obtain that

$$\mathrm{tr}_{\rho_j}(\langle\chi_i\rangle^p) = \varepsilon_I(\rho_j) = a_i^j.$$

This implies the result in combination with [NSW], 3.9.14. □

§3 Explicit calculations of the relation structure

In this section we will apply our results from the first section in order to explicitly calculate the values of $\varepsilon_{I,p}$ for $|I| = 2, 3$. By the results of the last section, this gives information on the cup product and on the triple Massey product if defined. The results for the cup product are of course well-known, we include them here for the sake of completeness.
We have already seen in (1.1.25) that in order to calculate $\varepsilon_{I,p}$ for $|I| = 2, 3$ we need to know the maps η_1, η_2, η_3.

(1.3.1) Proposition. *The maps η_1, η_2, η_3 are given by*

$$\eta_1 : \qquad (k) \mapsto x_k,$$

$$\eta_2 : \qquad (k,l) \mapsto \begin{cases} (x_k, x_l) & \text{if} \quad k < l, \\ -(x_l, x_k) & \text{if} \quad k > l, \\ 0 & \text{if} \quad k = l, \end{cases}$$

$$\eta_3 : \quad (k,l,m) \mapsto \begin{cases} -((x_l, x_k), x_m) & \text{if} \quad k > l,\ k > m, l \neq m, \\ ((x_k, x_l), x_m) + ((x_m, x_l), x_k) & \text{if} \quad l > k,\ l > m,\ k \neq m, \\ -((x_l, x_m), x_k) & \text{if} \quad m > l > k, \\ -((x_l, x_m), x_k) & \text{if} \quad m > k > l, \\ -((x_k, x_m), x_k) & \text{if} \quad k = l,\ k < m, \\ ((x_m, x_k), x_k) & \text{if} \quad k = l,\ k > m, \\ ((x_k, x_l), x_l) & \text{if} \quad l = m,\ k < l, \\ -((x_l, x_k), x_l) & \text{if} \quad l = m,\ k > l, \\ 2((x_k, x_l), x_k) & \text{if} \quad k = m,\ k < l, \\ -2((x_l, x_k), x_k) & \text{if} \quad k = m,\ k > l, \\ 0 & \text{if} \quad k = l = m, \end{cases}$$

for $1 \leq k, l, m \leq n$.

Proof. The map η_2 has already been given in (1.1.16). The map η_3 has been partially calculated in (1.1.16). We leave the remaining cases to the reader and remark that one can reduce the number of cases that have to be considered by the use of the shuffle property. □

Let G be a finitely generated pro-p-group with a minimal presentation

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1,$$

where F is the free group generated by $x_1, \ldots, x_n$. Let $\chi_1, \ldots, \chi_n$ be the dual basis to $\bar{x}_1, \ldots, \bar{x}_n$ of $H^1(F, \mathbb{Z}/p\mathbb{Z}) = H^1(G, \mathbb{Z}/p\mathbb{Z})$
We obtain the following result.

(1.3.2) Proposition. *Let $f \in F_{(2)}$. Then f may be uniquely written as*

$$f = \begin{cases} \displaystyle\prod_{1\le k<l\le n} (x_k, x_l)^{b_{kl}} f' & \text{if} \quad p \neq 2, \\ \displaystyle\prod_{k=1}^{n} x_k^{2a_k} \prod_{1\le k<l\le n} (x_k, x_l)^{b_{kl}} f' & \text{if} \quad p = 2, \end{cases}$$

where $a_k, b_{kl} \in \mathbb{Z}/p\mathbb{Z}$, $f' \in F_{(3)}$. For $1 \le k, l \le n$ it holds that

$$\varepsilon_{kl,p}(f) = \begin{cases} b_{kl}^i & \text{if} \quad k < l, \\ -b_{lk}^i & \text{if} \quad k > l, \\ 0 & \text{if} \quad k = l, p \neq 2, \\ a_k^i & \text{if} \quad k = l, p = 2. \end{cases}$$

If $\rho \in R$ then it holds in particular that

$$\mathrm{tr}_\rho(\chi_k \cup \chi_l) = -\varepsilon_{kl,p}(\rho).$$

Proof. The existence of such a representation is contained in (1.1.21). The uniqueness follows from the the second statement of that proposition. The calculation of $\varepsilon_{kl,p}$ has already been described in the proof of (1.1.25). We only remark that for $p = 2$ it holds that

$$\varepsilon_{kl,p}(x_\kappa^2) = \delta_{kl}\delta_{k\kappa}.$$

which is easily seen directly (or alternatively, it follows from the proof of (1.1.25) as well). The result follows from (1.3.1). □

The last proposition should be compared to [NSW], 3.9.13. The results are virtually the same, only that in [NSW] the descending p-central series is used. Our results indicate that the Zassenhaus filtration is the more natural filtration when dealing with Massey products. The result (1.2.6) should thus be seen as a natural generalization of [NSW], 3.9.13.
In our arithmetical applications we will be concerned with the case where the relations of G are inside $F_{(3)}$. Therefore we will now deal with this case as well.

(1.3.3) Proposition. *Let $f \in F_{(3)}$. Then f may be uniquely written as*

$$f = \begin{cases} \displaystyle\prod_{1\le k<l\le n; m\le l} ((x_k, x_l), x_m)^{e_{klm}} f' & \text{if} \quad p \neq 3, \\ \displaystyle\prod_{k=1}^{n} x_k^{3a_k} \prod_{1\le k<l\le n; m\le l} ((x_k, x_l), x_m)^{e_{klm}} f' & \text{if} \quad p = 3. \end{cases}$$

where a_k, $e_{klm} \in \mathbb{Z}/p\mathbb{Z}$, $f' \in F_{(4)}$. *For all* $1 \leq k, l, m \leq n$ *it holds that*

$$\varepsilon_{klm,p}(f) = \begin{cases} -e_{lkm} & \text{if } k > l,\ k > m,\ l \neq m, \\ e_{klm} + e_{mlk} & \text{if } l > k,\ l > m,\ k \neq m, \\ -e_{lmk} & \text{if } m > l > k, \\ -e_{lmk} & \text{if } m > k > l, \\ -e_{kmk} & \text{if } k = l,\ k < m, \\ e_{mkk} & \text{if } k = l,\ k > m, \\ e_{kll} & \text{if } l = m,\ k < l, \\ -e_{lkl} & \text{if } l = m,\ k > l, \\ 2e_{klk} & \text{if } k = m,\ k < l, \\ -2e_{lkk} & \text{if } k = m,\ k > l, \\ 0 & \text{if } k = l = m,\ p \neq 3, \\ a_k^i & \text{if } k = l = m,\ p = 3. \end{cases}$$

Assume that $R \subset F_{(3)}$, *or equivalently, that the cup product*

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \times H^1(G, \mathbb{Z}/p\mathbb{Z}) \overset{\cup}{\to} H^2(G, \mathbb{Z}/p\mathbb{Z})$$

vanishes. Then, for $\rho \in R$ *we have*

$$\mathrm{tr}_\rho \langle \chi_k, \chi_l, \chi_m \rangle = \varepsilon_{klm,p}(\rho).$$

Proof. The existence of such a representation is contained in (1.1.21). The uniqueness follows from the the second statement of that proposition. It suffices to remark that for $p = 3$ we have

$$\varepsilon_{klm,p}(x_\kappa^3) = \delta_{kl}\delta_{km}\delta_{k\kappa},$$

which follows from the proof of (1.1.25) (or, alternatively from (1.1.23)). The statement of the proposition follows from (1.3.1). □

Chapter II

Arithmetic part

§1 The maximal p-extension with restricted ramification

Throughout this section let K be a number field. We denote by $\mathcal{O}_K$ the ring of integers of K. For a prime $\mathfrak{l}$ of K, let $K_\mathfrak{l}$ denote the completion of K at $\mathfrak{l}$ and $U_\mathfrak{l}$ the unit group in $K_\mathfrak{l}^\times$. Let r_1 and r_2 denote the number of real and complex places of K, respectively. We fix a prime number p. We let S_p stand for the set of primes of K above p. Let S be a finite set of primes of K with $S \cap S_p = \varnothing$. We denote the Galois group of the maximal p-extension of K unramified outside S by $G = G_S(K)(p)$. Let

$$d(G) = h^1(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z}),$$
$$r(G) = h^2(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z})$$

be the generator and relation rank of G, respectively. Let

$$Б_S(K,p) = V_S(K,p)^*,$$

where

$$V_S(K,p) = \{a \in K^\times \mid a \in K_\mathfrak{l}^{\times p} \text{ for } \mathfrak{l} \in S \text{ and } a \in U_\mathfrak{l} K_\mathfrak{l}^{\times p} \text{ for } \mathfrak{l} \notin S\}/K^{\times p}$$

and * means the Pontryagin dual. We remark that there is an exact sequence

$$0 \longrightarrow \mathcal{O}_K^\times/p \longrightarrow V_\varnothing(K,p) \longrightarrow {}_pCl(K) \longrightarrow 0,$$

see [NSW](8.7.2), and that $Б_{S'}(K,p) \subseteq Б_S(K,p)$ if $S \subseteq S'$. We put

$$\delta = \begin{cases} 1 & \text{if} \quad \mu_p \subseteq K, \\ 0 & \text{if} \quad \mu_p \not\subseteq K, \end{cases}$$

and

$$\delta_\mathfrak{l} = \begin{cases} 1 & \text{if} \quad \mu_p \subseteq K_\mathfrak{l}, \\ 0 & \text{if} \quad \mu_p \not\subseteq K_\mathfrak{l}, \end{cases}$$

for a prime $\mathfrak{l}$ of K. Let C_K be the idèle class group of K. If L is an abelian extension of K we denote by

$$(\cdot, L/K) : C_K \to G(L/K)$$

the norm residue symbol of global class field theory.
The following primes cannot ramify in a p-extension, and are therefore redundant in S:

complex primes,

real primes if $p \neq 2$,

primes $\mathfrak{l} \nmid p$ with $N(\mathfrak{l}) \not\equiv 1 \mod p$.

Removing all these redundant primes from S we obtain a subset $S_{\min} \subseteq S$. The following result due to Koch is well-known, cf. [NSW](8.7.11).

(2.1.1) Theorem. *Let $r = r_1 + r_2$ be the number of archimedean primes of K and let $\theta = \theta(K,S) = 1$ if $\delta = 1$ and $S_{\min} = \varnothing$, and zero in all other cases. Then*

(i)

$$\begin{aligned} h^1(G) &= 1 + \sum_{\mathfrak{l} \in S_{\min}} \delta_{\mathfrak{l}} - \delta + \dim_{\mathbb{F}_p} Ш_S(K) - r, \\ h^2(G) &\leq \sum_{\mathfrak{l} \in S_{\min}} \delta_{\mathfrak{l}} - \delta + \dim_{\mathbb{F}_p} Ш_S(K) + \theta. \end{aligned}$$

(ii) The abelianization G^{ab} of G is finite.

Proof. For (i) we refer to [NSW](8.7.11). For the proof of (ii) we remark that $\mathbb{Z}_p$-extensions of number fields are unramified outside primes above p. Because $S \cap S_p = \varnothing$ and since there are no infinite unramified abelian extensions of K by the finiteness of the ideal class group, assertion (ii) follows. □

(2.1.2) Corollary. *Let $K = \mathbb{Q}$ or an imaginary quadratic number field. Assume that we are not in the case where $\delta = 1$, $S_{\min} = \varnothing$. Then*

(i) $h^1(G) = h^2(G) = \sum_{\mathfrak{l} \in S_{\min}} \delta_{\mathfrak{l}} - \delta + \dim_{\mathbb{F}_p} Ш_S(K)$,

(ii) $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) = 0$,

(iii) G is infinite if $h^1(G) \geq 4$.

Proof. Since $r = 1$ we obtain by (2.1.1) that $h^2(G) \leq h^1(G)$. Taking the long exact cohomology sequence associated to $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$ we obtain the exact sequence

$$0 \longrightarrow ({}_pG^{ab})^* \longrightarrow H^2(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow 0.$$

Because of (2.1.1)(ii), we obtain $\dim_{\mathbb{F}_p} {}_pG^{ab} = \dim_{\mathbb{F}_p} G^{ab}/p = h^1(G)$. This implies $h^1(G) \leq h^2(G)$. Therefore $h^1(G) = h^2(G)$, and as a by-product we obtain that $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Let

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

be a minimal presentation of G. Then $R \subseteq F_{(2)} = F^p[F,F]$ where $F_{(2)}$ denotes the second step of the Zassenhaus filtration of F, cf. (1.1.17). If G is finite, then the Golod-Shafarevich inequality implies

$$h^1(G) = h^2(G) > \frac{1}{4}h^1(G)^2,$$

hence $h^1(G) < 4$, which implies (iii). □

In the following we will consider the case where $K = \mathbb{Q}$. Let $S = \{l_1, \ldots, l_n, \infty\}$ be a finite set consisting of prime numbers $l_i \equiv 1 \mod p$, $1 \leq i \leq n$, and the infinite prime ∞ of $\mathbb{Q}$. Let $\mathfrak{l}_i$ be a fixed prime over l_i in $\mathbb{Q}_S(p)$. For $1 \leq i \leq n$ let σ_i be an element in $G = G_S(p)$ 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 $\mathbb{Q}_S(p)^{(2)}/\mathbb{Q}$ of the extension $\mathbb{Q}_S(p)/\mathbb{Q}$ is equal to $(\lambda_i, \mathbb{Q}_S(p)^{(2)}/\mathbb{Q})$, 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 $G_S(p)$ such that

(i) τ_i is a generator of the inertia group $T_{\mathfrak{l}_i}$ of $\mathfrak{l}_i$ in $\mathbb{Q}_S(p)/\mathbb{Q}$;

(ii) the restriction of τ_i to $\mathbb{Q}_S(p)^{(2)}/\mathbb{Q}$ equals $(\alpha_i, \mathbb{Q}_S(p)^{(2)}/\mathbb{Q})$, where α_i denotes the idèle whose l_i-component is a primitive root g_i modulo l_i and all other components are 1.

For $i \neq j$ let $\alpha_{i,j}$, $\beta_{i,j} \in \mathbb{Z}_p$, $\ell_{i,j} \in \mathbb{Z}/p\mathbb{Z}$, be defined by

$$l_i^{-1} = g_j^{\alpha_{i,j}}(l_j + 1)^{\beta_{i,j}}, \quad \ell_{i,j} = \alpha_{i,j} \mod p.$$

By class field theory, we have

$$\sigma_i \equiv \prod_{j \neq i} \tau_j^{\alpha_{i,j}} \mod (G_S(p), G_S(p)).$$

If $p \neq 2$ then $Ш_{\varnothing}(\mathbb{Q}, p) = 0$ because $\mathbb{Q}$ has trivial ideal class group. If $p = 2$ then $Ш_{\{\infty\}}(\mathbb{Q}, p) = 0$ because -1 is not a square in $\mathbb{R}$. By the above remarks, we obtain $Ш_S(\mathbb{Q}, p) = 0$ for all p. In particular, we may apply Theorem 11.10 of [K] to our situation and obtain the

(2.1.3) Theorem. (Fröhlich, Koch) *Let F be a free pro-p-group on generators $x_1, \ldots, x_n$. Then $G_S(p)$ has a minimal presentation*

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

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 $\mathcal{R} = \{\rho_i\}_{1 \leq i \leq n}$ with

$$\rho_i = x_i^{l_i - 1}(x_i^{-1}, y_i^{-1}),$$

where y_i is a preimage of σ_i, i.e. $\pi(y_i) = \sigma_i$. It holds that

$$\rho_i \equiv x_i^{l_i - 1} \prod_{j \neq i} (x_i, x_j)^{\ell_{i,j}} \mod F_{(3)}.$$

Proof. Except the minimality statement concerning $\mathcal{R}$ and the last assertion this is Theorem 11.10 of [K]. That $\mathcal{R}$ is a minimal system of generators follows from (2.1.2)(i). The last assertion follows from

$$\sigma_i \equiv \prod_{j \neq i} \tau_j^{\ell_{i,j}} \mod G_S(p)_{(2)},$$

which is a consequence of the above class field theoretic calculation. □

The above theorem should be compared to the theorem of Chen-Milnor in link theory, see the appendix, Thm.(A.1). The τ_i play the role of meridians, and the σ_i correspond to longitudes. Using this analogy, Morishita introduced Milnor invariants in this situation, see [M]. For the notation in the following definition we refer to the first chapter.

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

$$\mu_p(I) = \varepsilon_{I',p}(y_{i_r}),$$

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

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

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

There is also a shuffle property for Milnor invariants. As it is stated slightly incorrect in [M] we will restate it here.

(2.1.6) Remark. *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*

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

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

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

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

(It is the factor m that has been forgotten in [M], Thm. 3.1.8. In particular his result would imply that under the hypothesis that the second order Milnor invariants μ_2 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. From this point of view our situation is different from the one in link theory, where under the same assumption, concerning the vanishing of the second order Milnor invariants, the Milnor invariants $\mu(i,j,k)$ vanish if two of i,j,k are equal, see [F], §5.9.)

Using our algebraic main result (1.2.6) we can show that there is an intimate connection between Milnor numbers and Massey products. Let $l_i - 1 = p^{e_i}r_i$, $(r_i,p) = 1$ and $e = \min\{e_i\}$. Denote by $\{\chi_1,\ldots,\chi_n\}$ the dual basis of $H^1(F,\mathbb{Z}/p\mathbb{Z}) = H^1(G_S(p),\mathbb{Z}/p\mathbb{Z})$ to $\{x_1,\ldots,x_n\}$. The following theorem should be seen as a number theoretical analogue of the theorem of Porter-Turaev from link theory, see the appendix, Thm. (A.3).

(2.1.7) Theorem. *Let $1 < m \leq p^e$ and assume that $\mu_p(J) = 0$ for all multi-indices J with $1 < |J| < m$. Then we have a well-defined m-fold Massey product*

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

Let $I = (i_1,\ldots,i_m)$. Then

$$\begin{aligned}\mathrm{tr}_{\rho_{i_k}}\langle\chi_{i_1},\ldots,\chi_{i_m}\rangle \;=\; & (-1)^m(\delta_{i_m i_k}\mu_p(i_1,\ldots,i_m) - \delta_{i_1 i_k}\mu_p(i_2,\ldots,i_m,i_1) \\ & -\binom{l_{i_k}-1}{m}\delta_{I=(i_1,\ldots,i_1)}).\end{aligned}$$

The binomial coefficient $\binom{l_{i_m}-1}{m}$ is nonzero if and only if $m = p^e$, $e_{i_m} = e$.

Proof. The assumption implies that $\varepsilon_{J',p}(y_j) = 0$ for all $1 \leq j \leq r$ and all $1 \leq |J'| < m-1$. By (1.1.24)(b) we obtain that $y_j \in F_{(m-1)}$ for all $1 \leq j \leq r$. Therefore $(x_j^{-1}, y_j^{-1}) \in F_{(m)}$ and because $m \leq p^e$ we have $x_j^{l_i-1} \in F_{(m)}$. This implies that $R \subseteq F_{(m)}$ so that the assumptions of (1.2.6) are fulfilled. By (1.2.6)

we obtain

$$\begin{aligned}(-1)^{m-1}\,\mathrm{tr}_{\rho_{i_k}}\langle\chi_I\rangle &= \varepsilon_{I,p}(\rho_{i_k})\\ &= \varepsilon_{I,p}(x_{i_k}^{l_{i_k}-1}(x_{i_k}^{-1},y_{i_k}^{-1}))\\ &= \varepsilon_{I,p}(x_{i_k}^{l_{i_k}-1})+\varepsilon_I((x_{i_k}^{-1},y_{i_k}^{-1}))\\ &= \binom{l_{i_k}-1}{m}\delta_{I=(i_1,\ldots,i_1)}+\varepsilon_{(i_1),p}(x_{i_k}^{-1})\varepsilon_{(i_2,\ldots,i_m),p}(y_{i_k}^{-1})\\ &\quad -\varepsilon_{(i_m),p}(x_{i_k}^{-1})\varepsilon_{(i_1,\ldots,i_{m-1}),p}(y_{i_k}^{-1})\\ &= \binom{l_{i_k}-1}{m}\delta_{I=(i_1,\ldots,i_1)}+\delta_{i_1i_k}\mu_p(i_2,\ldots,i_m,i_1)\\ &\quad -\delta_{i_mi_k}\mu_p(i_1,\ldots,i_m),\end{aligned}$$

where we have made use of (1.1.22) and (1.1.23). An elementary calculation shows that

$$v_p(\binom{l_{i_m}-1}{m}) = e_{i_m}-v_p(m),$$

which implies the last claim. □

We may now use some results of Morishita on Milnor numbers in order to calculate Massey products. In [M], Thm. 3.13 it is shown that $\mu_p(i,i)=0$ and that $\mu_p(i,j)=\ell_{j,i}$ for $i\neq j$. In particular,

$$\zeta_p^{\mu_p(i,j)}=\zeta_p^{\ell_{j,i}}=\left(\frac{l_j}{l_i}\right)_p,\quad i\neq j,$$

where $\zeta_p=\tau_i(\sqrt[p]{l_i})/\sqrt[p]{l_i}$ is a primitive p-th root of unity and $(l_j/l_i)_p$ denotes the p-th power residue symbol in $\mathbb{Q}_{l_i}$. We recall, see [N], Kap.V.3., that $(l_j/l_i)_p$ is defined as the p-th root of unity which is determined by

$$\left(\frac{l_j}{l_i}\right)_p \equiv l_j^{\frac{l_i-1}{p}} \mod l_i\mathbb{Z}_{l_i}.$$

We immediately obtain the

(2.1.8) Corollary. *With the above notation we have*

$$\mathrm{tr}_{\rho_k}(\chi_i\cup\chi_j)=\begin{cases}\ell_{j,i} & \text{if } k=j,\ i\neq j,\\ -\ell_{i,j} & \text{if } k=i,\ i\neq j,\\ -\binom{l_i-1}{2} & \text{if } i=j=k,\\ 0 & \text{if } i=j\neq k,\\ 0 & \text{if } k,i,j \text{ pairwise distinct.}\end{cases}$$

Of course, we could have obtained that result from (2.1.3) and (1.3.2) as well. The advantage of working with (2.1.7) instead will become more apparent when

we deal with triple Massey products. We remark that for odd p the above corollary is contained already in a paper of Waldspurger [W], see the comment in [M].
From now on we assume that $p = 2$. We are particularly interested in the case where the cup product vanishes. By (2.1.8) a necessary condition is given by

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

for all i with $1 \leq i \leq n$. This condition is satisfied if and only if all l_i are congruent 1 modulo 4. Assume that $S = \{l_1, \ldots, l_n, \infty\}$, $n \geq 3$, where the l_i are prime numbers which are congruent 1 modulo 4. In this situation we have the symmetry relation

$$\ell_{j,i} = \mathrm{tr}_{\rho_j}(\chi_i \cup \chi_j) = \mathrm{tr}_{\rho_i}(\chi_j \cup \chi_i) = \ell_{i,j}$$

due to Gauss reciprocity. The cup product vanishes if and only if

$$\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \leq i, j \leq n, \ i \neq j$$

where $(\frac{\cdot}{\cdot})_2$ is the Legendre symbol. We assume this from now on. In this situation triple Massey products are well-defined and we want to calculate them. We remark that by (2.1.2)(iii) the group $G_S(2)$ is infinite.
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 [M], a connection is given between the Rédei symbols $[l_i, l_j, l_k]$ and the Milnor invariants $\mu_2(ijk)$ of $G_S(2)$ for pairwise distinct primes $l_i, l_j, l_k \in S$. We will generalize the result of [M] to the case where two of the l_i, l_j, l_k may coincide. This allows us to give a complete description of the triple Massey product

$$\langle \cdot, \cdot, \cdot \rangle : H^1(G_S(2)) \times H^1(G_S(2)) \times H^1(G_S(2)) \to H^2(G_S(2))$$

where $H^i(G_S(2))$ denotes $H^i(G_S(2), \mathbb{Z}/2\mathbb{Z})$ for $i = 1, 2$. Unfortunately the presentation in [M] 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 [M], Ex. 3.2.6 is indeed ramified at 2. This makes the calculation of the Milnor numbers in [M] incorrect. Fortunately, the construction can be rescued if we stay closer to the original work of [R]. For this reason we have decided to give a more detailed view of the aforementioned construction and the definition of the Rédei symbol.
We need the following notation.

(2.1.9) Definition. *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 [R], Satz 1.

(2.1.10) Proposition. *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*

$$\left(\frac{p_i}{p_j}\right)_2 = 1, \quad 1 \leq i \neq j \leq 3.$$

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 [R], 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 $x - y \equiv 1 \mod 4$.

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

$$\left(\frac{p_i}{p_j}\right)_2 = 1, \quad 1 \leq i, j \leq 3, \ p_i \neq p_j$$

Then the **Rédei symbol** *is defined as*

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

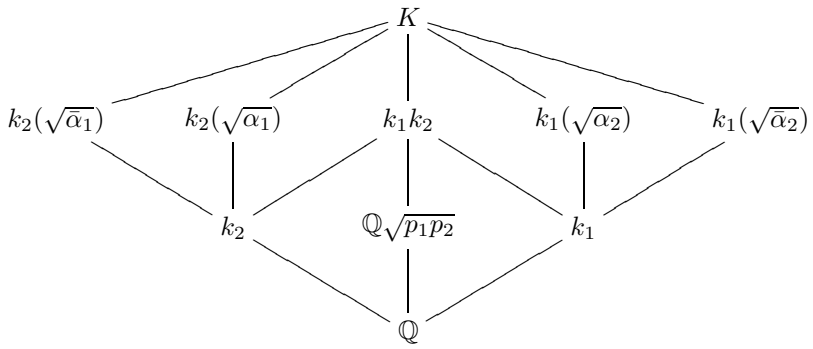
where α_2 *and* $\mathfrak{p}_3$ *are given as in (2.1.10).*

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

(2.1.12) Lemma. *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 [R], p.5, α_1 fulfils the conditions (i) and (ii) of (2.1.10) where the obvious replacements have to be made. Let $K := k_1k_2(\sqrt{\alpha_2})$.
We consider the case where $p_1 \neq p_2$. We then 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 [R], 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. Their relations are given by

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

It follows from the consideration in [R] 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 [M] 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 (2.1.10) 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 $G(K/\mathbb{Q})$ which will be useful for our further applications:

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

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-p-group generated by $x_1, \ldots, x_n$ as in (2.1.3). 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].

(2.1.13) Proposition. (Morishita) *If i, j, k are pairwise distinct then*

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

Proof. By [R], eq. (25) we have

$$\left(\frac{\alpha_2 | k_1}{\mathfrak{p}_3}\right) = \left(\frac{\alpha_2 | k_1 k_2}{\mathfrak{P}_3}\right)$$

where $\mathfrak{P}_3$ is a prime ideal of $k_1 k_2$ above $\mathfrak{p}_3$. By the assumptions on the Legendre symbols $p_3 = l_k$ is completely decomposed in k_1 and k_2, hence it is completely decomposed in $k_1 k_2$. Therefore the image of y_k under π is given by

$$\pi(y_k) = \begin{cases} t^2 = (a_1 a_2)^2 & \text{if} \quad [l_i, l_j, l_k] = -1, \\ 1 & \text{if} \quad [l_i, l_j, l_k] = 1. \end{cases}$$

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

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

For all generators it holds that $\varepsilon_{(i,j),2}$ as well as $\varepsilon_{(i),2}$ and $\varepsilon_{(j),2}$ vanish on them. By (1.1.22) 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 $\pi(y_k) = 1$ then $y_k \in \tilde{R}$, hence $\mu_2(i,j,k) = \varepsilon_{(i,j),2}(y_k) = 0$. If $\pi(y_k) = (a_1 a_2)^2$ then $y_k = (x_i x_j)^2 r$ with an element $r \in R$. We obtain

$$\begin{aligned} \varepsilon_{(i,j),2}(y_k) &= \varepsilon_{(i,j),2}((x_i x_j)^2) + \varepsilon_{(i,j),2}(r) + \varepsilon_{(i),2}((x_1 x_2)^2)\varepsilon_{(j),2}(r) \\ &= 1, \end{aligned}$$

because the Magnus expansion of $(x_1 x_2)^2$ is given by

$$(x_1 x_2)^2 \equiv 1 + X_1^2 + X_2^2 + X_1 X_2 + X_2 X_1 \mod \deg \geq 3.$$

This proves the proposition. □

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

(2.1.14) Proposition. *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 (1.1.29) and the proof of (2.1.7) we obtain

$$\begin{aligned}0 &= \varepsilon_{(j,i,j),2}(\rho_j) + \varepsilon_{(i,j,j),2}(\rho_j) + \varepsilon_{(i,j,j),2}(\rho_j)\\ &= \mu_2(i,j,j) + \mu_2(j,i,j)\end{aligned}$$

By (2.1.12) 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 $\mathfrak{P}_2|\mathfrak{q}_1$ 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

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

where $\mathfrak{P}_2|\mathfrak{q}_1$, 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 (we recall that y_j maps to $\sigma_j \in G_S(2)$) the restriction of σ_j to the maximal abelian subextension $\mathbb{Q}_S(2)^{(2)}/\mathbb{Q}$ of $\mathbb{Q}_S(2)/\mathbb{Q}$ is equal to $(\lambda_j, \mathbb{Q}_S(2)^{(2)}/\mathbb{Q})$, 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 $\rho(y_k) = t^2$. The statement of the proposition follows as in the proof of (2.1.13). □

Now we deal with the Milnor invariants $\mu_2(i,i,j)$. Suppose that $p_1 = p_2$. In this case 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 [R] 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 $\pi(y_i) = t$.

(2.1.15) Proposition. *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

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

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 (1.1.23) and (1.1.22) 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.

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

$$\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \leq i, j \leq n, \ i \neq j.$$

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

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

The triple Massey product

$$\langle \cdot, \cdot, \cdot \rangle : H^1(G_S(2)) \times H^1(G_S(2)) \times H^1(G_S(2)) \to H^2(G_S(2))$$

is determined by

$$(-1)^{\mathrm{tr}_{\rho_m}\langle \chi_i, \chi_j, \chi_k \rangle} = \begin{cases} [l_i, l_j, l_k] & \text{if } m = i \text{ and } m \neq k, \\ [l_i, l_j, l_k] & \text{if } m \neq i \text{ and } m = k, \\ 1 & \text{otherwise.} \end{cases}$$

In particular, this result allows a complete determination of the relations R of $G_S(2)$ modulo $F_{(4)}$.

Proof. This follows from (2.1.13), (2.1.14), (2.1.15), (2.1.7). □

We will give some examples. Explicit computations of Rédei symbols are quite complex, so we have used the computer algebra system KASH to compute them.

(2.1.17) Example. *(cf. [M], 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 [M] where it is chosen inappropriately). We obtain $[l_1, l_2, l_3] = -1$. Therefore all Massey products $\langle \chi_i, \chi_j, \chi_k \rangle$, $\{i,j,k\} = \{1,2,3\}$ are nontrivial. Our computer program yields that the Rédei symbol $[l_i, l_j, l_k]$ is -1 exactly for all permutations of the triples (i,j,k) where $(i,j,k) = (1,2,3)$, $(1,2,2)$, $(1,3,3)$, $(2,2,3)$, $(2,3,3)$. The corresponding triple Massey products are nontrivial, the other Massey products vanish. By (1.3.3) the relations are given by*

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

As in [M] we call $(5, 41, 61)$ a triple of Borromean primes.

(2.1.18) Example. *Set $l_1 = 5$, $l_2 = 41$, $l_3 = 61$, $l_4 = 241$, $l_5 = 569$, $l_6 = 829$. Using our computer program we obtain that the Massey products $\langle \chi_i, \chi_j, \chi_k \rangle$ with i,j,k pairwise distinct are nontrivial for $\{i,j,k\} = \{1,2,3\}$, $\{1,2,6\}$, $\{2,3,4\}$, $\{2,3,6\}$, $\{3,4,5\}$, $\{4,5,6\}$.*

(2.1.19) Example. *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 the relations are given by*

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

We suggest to call $(13, 61, 937)$ *a proper Borromean triple modulo* 2.

We remark that by looking at the abelianizations in the above examples one can already conclude that the relations of $G_S(2)$ are inside $F_{(3)} - F_{(4)}$ or $F_{(4)} - F_{(5)}$. The above calculations ensure that they are inside $F_{(3)} - F_{(4)}$.

(2.1.20) Example. *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. Hence the triple Massey product vanishes completely. This implies that the relations of* $G_S(2)$ *are inside* $F_{(4)}$. *Hence in this example it holds that*

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

The next example gives a little impression of the heuristic of Rédei symbols.

(2.1.21) Example. *There are* 41 *triples* (l_1, l_2, l_3) *of primes* $l_i \equiv 1 \mod 4$ *with* $l_1 < l_2 < l_3$ *and* $l_1 l_2 l_3 < 100000$ *for which the pairwise Legendre symbols vanish. Among these there are* 25 *triples for which the Rédei symbol* $[l_1, l_2, l_3]$ *is* -1. *There are* 777 *triples* (l_1, l_2, l_3) *of primes* $l_i \equiv 1 \mod 4$ *with* $\gcd(l_1, l_2, l_3) = 1$ *and* $l_1 l_2 l_3 < 100000$ *for which the pairwise Legendre symbols vanish. Among these there are* 423 *triples for which the Rédei symbol* $[l_1, l_2, l_3]$ *is* -1.

We finish this section with a few remarks about $G_S(2)$ if the conditions $2 \notin S$, $\infty \in S$ do not necessarily hold.
If $\infty \notin S$ the connection between triple Massey products and Rédei symbols will exist only in special cases as Rédei's construction of the dihedral extension of degree 8 usually produces extensions that are ramified at the infinite prime therefore not being quotients of $G_S(2)$. If $2 \in S$, $\infty \in S$ it follows by [K2], Thm. 6.3. that the cup product

$$H^1(G_S(2), \mathbb{Z}/2\mathbb{Z}) \times H^1(G_S(2), \mathbb{Z}/2\mathbb{Z}) \stackrel{\cup}{\to} H^2(G_S(2), \mathbb{Z}/2\mathbb{Z})$$

does never completely vanish.

§2 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. For an imaginary quadratic number field this is the same as $K_\varnothing$, the maximal unramified 2-extension of K.
We make use of the well-known fact that one can descend from $G_S(2)$ to $G(K_{S_\infty}/\mathbb{Q})$ which is reflected in the following lemma, see [K2], Prop. 7.1. As in the last section, let $\mathfrak{l}_i$ be a fixed prime over l_i in $\mathbb{Q}_S(2)$. We denote the inertia group of $\mathfrak{l}_i$ in $\mathbb{Q}_S(2)/\mathbb{Q}$ by $T_{\mathfrak{l}_i}$.

(2.2.1) Lemma. *Let N_S be the normal subgroup of $G_S(2)$ generated by the groups $T_{\mathfrak{l}_i} \cap G(\mathbb{Q}_S(2)/K)$ with $1 \leq i \leq n$. 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

$$D = \pm l_1 \cdot \ldots \cdot l_n$$

where the l_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

$$\mathrm{Ram}_f(K/\mathbb{Q}) = \begin{cases} \{l_1, \ldots, l_n\} & \text{if} \quad D \equiv 1 \mod 4, \\ \{2, l_1, \ldots, l_n\} & \text{otherwise.} \end{cases}$$

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_i 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.
The groups $T_{\mathfrak{l}_i} \cap G(\mathbb{Q}_S(2)/K)$ are generated by τ_i^2. Using the minimal presentation

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

of $G_S(2)$ from Thm.(2.1.3) 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 group generated by $x_1, \ldots, x_n$ and R_a is generated as a normal subgroup by R and by the preimages x_i^2 of τ_i^2, $1 \leq i \leq n$. The following theorem, see [K2], Thm. 7.1, is an easy consequence.

(2.2.2) Theorem. (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-p-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

$$\begin{aligned} x_i^2, &\quad 1 \leq i \leq n, \\ \rho_i = (x_i, y_i), &\quad 1 \leq i \leq n. \end{aligned}$$

It holds that

$$\rho_i \equiv \prod_{\substack{1\le j\le n\\ j\neq i}} (x_i, x_j)^{\ell_{i,j}} \mod F_{(3)}$$

where $\ell_{i,j}$ has been defined in the last section. We recall that

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

In particular we see that the relations R_a are always inside $F_{(2)} - F_{(3)}$, so the cup product

$$H^1(G(K_{S_\infty}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z}) \times H^1(G(K_{S_\infty}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z}) \overset{\cup}{\to} H^2(G(K_{S_\infty}/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$$

does never completely vanish.
For further purposes we need the following result:

(2.2.3) Proposition. *Assume that*

$$\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \le i, j \le n, \ i \neq j.$$

Let $1 \le i, j, k, m \le n$. Then

$$\varepsilon_{(i,j,k),2}(\rho_m) = \delta_{im}\mu_2(jki) + \delta_{km}\mu_2(ijk).$$

If $1 \le i, j, k \le r$ and $1 \le m \le n$ then

$$(-1)^{\varepsilon_{(i,j,k),2}(\rho_m)} = \begin{cases} [l_i, l_j, l_k] & \text{if} \quad m = i \text{ or } m = k, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Note that the assumption implies that $y_m \in F_{(2)}$. The proof of the first statement involves basically the same calculation as in the proof of (2.1.7):

$$\begin{aligned} \varepsilon_{(i,j,k),2}(\rho_m) &= \varepsilon_{(i,j,k),2}(x_m, y_m) \\ &= \varepsilon_{(i),2}(x_m)\varepsilon_{(j,k),2}(y_m) + \varepsilon_{(k),2}(x_m)\varepsilon_{(i,j),2}(y_m) \\ &= \delta_{im}\mu_2(i,j,k) + \delta_{km}\mu_2(i,j,k). \end{aligned}$$

The second statement follows from (2.1.5), (2.1.16). □

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

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

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

$$x_i^2, \ \rho_i, \ x_i^{-1}\rho_i x_i, \quad i = 1, \ldots, n.$$

An elementary calculation shows that R_a can be generated as a normal subgroup of H already by x_i^2, ρ_i, $1 \leq i \leq n$. If we pass to the factor group $\mathfrak{H}$ of H with respect to the normal subgroup N generated by $x_1^2, \ldots, x_n^2$, 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

$$w_i = x_i x_n N, \quad i = 1, \ldots, n-1,$$

and generating relations $\rho_i N$, $i = 1, \ldots, n$. The relations $\rho_i N$ have to be expressed in terms of the generators w_i. A short calculation gives

$$(t_i, t_j) = w_i^2 (w_i, w_j) w_j^{-2}$$

where we have put $w_n = 1$. We quote the following lemma, see [K2], Lemma 7.2.:

(2.2.4) Lemma. *For $k \geq 2$ we have*

$$NF^{(k,2)} = NH^{(k,2)}.$$

In summary, there is the following theorem, see [K2], Thm. 7.3.

(2.2.5) Theorem. (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-p-group $\mathfrak{H}$ with generators $w_1, \ldots, w_{n-1}$ and defining relations

$$\begin{aligned} r_i = \rho_i N &= w_i^{2\ell_{i,n}} \prod_{\substack{1 \leq j \leq n-1 \\ j \neq i}} (w_i^2 w_j^2 (w_i, w_j))^{\ell_{i,j}} r_i', \quad 1 \leq i \leq n-1, \\ r_n = \rho_n N &= \prod_{i=1}^{n-1} (w_i^2)^{\ell_{n,i}} r_n', \end{aligned}$$

where $r_i' \in \mathfrak{H}^{(3,2)} = \mathfrak{H}_{(3)}$ for all $1 \leq i \leq n$.

We set $H^i(G(K_{S_\infty}/K)) = H^i(G(K_{S_\infty}/K), \mathbb{Z}/2\mathbb{Z})$. It is obvious from the theorem that the cup product

$$H^1(G(K_{S_\infty}/K)) \times H^1(G(K_{S_\infty}/K)) \stackrel{\cup}{\to} H^2(G(K_{S_\infty}/K))$$

vanishes if and only if all $\ell_{k,l}$ vanish. Denote by $\{\chi_1, \ldots, \chi_{n-1}\}$ the dual basis of $H^1(\mathfrak{H}, \mathbb{Z}/2\mathbb{Z}) = H^1(G(K_{S_\infty}/K), \mathbb{Z}/2\mathbb{Z})$ to $\{w_1, \ldots, w_{n-1}\}$. Although we don't

need them we give the following formulae for the cup product whose easy proof we leave to the reader. For $1 \leq k, l \leq n-1$ and $1 \leq m < n$ it holds that

$$\mathrm{tr}_{r_m}(\chi_k \cup \chi_l) = \begin{cases} 0 & \text{if} \quad k \neq m,\ l \neq m, \\ \ell_{m,l} & \text{if} \quad k = m,\ l \neq m, \\ \ell_{m,k} & \text{if} \quad k \neq m,\ l = m, \\ \ell_{m,n} + \ldots + \ell_{m,m+1} + \ell_{m,m-1} & \\ \quad + \ldots + \ell_{m,1} & \text{if} \quad k = l = m, \\ \ell_{m,n-1} + \ldots + \ell_{m,m+1} + \ell_{m,m-1} & \\ \quad + \ldots + \ell_{m,1} & \text{if} \quad k = l \neq m. \end{cases}$$

and

$$\mathrm{tr}_{r_n}(\chi_k \cup \chi_l) = \begin{cases} 0 & \text{if} \quad k \neq l, \\ \ell_{n,k} & \text{if} \quad k = l. \end{cases}$$

From now on we assume that the cup product vanishes completely, i.e.

$$\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \leq i, j \leq n,\ i \neq j.$$

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 $l_1, \ldots, l_{n-1}$ 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 $\ell_{i,j} + \ell_{j,i} = 1$.

(2.2.6) Theorem. *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 $l_1, \ldots, l_{n-1}$ are congruent 1 modulo 4 and l_n is congruent 3 modulo 4.

and assume that $\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \leq i, j \leq n,\ i \neq j$. Then the cup product

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

vanishes completely. For the triple Massey product

$$\langle \cdot, \cdot, \cdot \rangle : H^1(G(K_{S_\infty}/K)) \times H^1(G(K_{S_\infty}/K)) \times H^1(G(K_{S_\infty}/K)) \to H^2(G(K_{S_\infty}/K))$$

the following formula holds for pairwise distinct i, j, k with $1 \leq i, j, k \leq n-1$:

$$(-1)^{\mathrm{tr}_{r_m}\langle \chi_i, \chi_j, \chi_k \rangle} = \begin{cases} [l_i, l_j, l_k] & \text{if} \quad m = i \text{ or } m = k, \\ 1 & \text{otherwise.} \end{cases}$$

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 (1.1.27) 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 (1.1.22). Let $I = (i,j,k)$. Because the cup product and hence all ℓ_{kl} vanish we have that $\rho_m \in F_{(3)}$. By (2.2.4) we may write $\rho_m N = \tilde{\rho}_m N$ with $\tilde{\rho}_m \in H_{(3)}$. Hence we have

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

This implies the result by (2.2.3). □

(2.2.7) Example. *Let $K = \mathbb{Q}(\sqrt{5 \cdot 41 \cdot 61 \cdot 241})$. By the above proposition and (2.1.18) the triple Massey product $\langle \chi_i, \chi_j, \chi_k \rangle$ for $\{i,j,k\} = \{1,2,3\}$ is nontrivial. We remark that by the Golod-Shafarevich inequality the group $G(K_{S_\infty}/K)$ is infinite. Further real quadratic number fields with these properties are given by*

$$\mathbb{Q}(\sqrt{13 \cdot 17 \cdot 53 \cdot 433}),\ \mathbb{Q}(\sqrt{17 \cdot 89 \cdot 373 \cdot 257}),\ \mathbb{Q}(\sqrt{5 \cdot 29 \cdot 181 \cdot 241}).$$

Imaginary quadratic fields with these properties are given by

$$\mathbb{Q}(\sqrt{-5 \cdot 41 \cdot 61 \cdot 131}),\ \mathbb{Q}(\sqrt{-5 \cdot 29 \cdot 181 \cdot 59}),\ \mathbb{Q}(\sqrt{-13 \cdot 17 \cdot 53 \cdot 43}),$$
$$\mathbb{Q}(\sqrt{-17 \cdot 89 \cdot 373 \cdot 179}).$$

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:

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

and $H^2(G(K_\varnothing/K))$ can be described by the exact sequence

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

The pairings

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

are therefore pairings

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

§3 The p-class field tower of a quadratic number field

In this section we study the p-class field tower of quadratic number fields for odd prime numbers p. We will see that the appearance of triple Massey products in this situation is much more natural than in the case of the 2-class field tower. However, an explicit determination of them seems to be more complicated.
Let 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. There is the following well-known result, see [S], lemma 4.1.

(2.3.1) Proposition. *We have*

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

In particular, the cup product

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

is trivial.

Proof. We set $G = G(K_\varnothing/K)$ and let σ be a generator of $G(K/\mathbb{Q})$. Taking the long exact cohomology sequence to $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}_p/Z_p \to 0$, we obtain an isomorphism

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \cong {}_p(H^1(G, \mathbb{Q}_p/\mathbb{Z}_p)).$$

By [Wi], Thm. 1.1. it follows that

$${}_p(H^1(G, \mathbb{Q}_p/\mathbb{Z}_p)) \cong (H^1(G, \mathcal{O}_{K_\varnothing^\times})/p)^* \cong (\mathrm{Cl}(K)/p)^*.$$

Because the norm map $N_{K/\mathbb{Q}} : \mathrm{Cl}(K) \to \mathrm{Cl}(K)$ factors through $\mathrm{Cl}(\mathbb{Q})$ which is trivial, σ acts on $\mathrm{Cl}(K)/p$ as -1. The above isomorphisms are σ-invariant, hence $H^1(G(K_\varnothing/K))^+ = 0$.
By dualizing the long exact cohomology sequence to $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}_p/Z_p \to 0$ we obtain an exact sequence

$$0 \longrightarrow H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^*/p \longrightarrow H^2(G, \mathbb{Z}/p\mathbb{Z})^* \longrightarrow_p (H^1(G, \mathbb{Q}_p/\mathbb{Z}_p)^*) \longrightarrow 0.$$

An application of [Wi], Thm. 1.1. yields the exact sequence

$$0 \longrightarrow \hat{H}^0(G, \mathcal{O}_{K_\varnothing}^\times)/p \longrightarrow H^2(G, \mathbb{Z}/p\mathbb{Z})^* \longrightarrow {}_p\,\mathrm{Cl}(K) \longrightarrow 0.$$

We have a surjection

$$\mathcal{O}_K^\times \twoheadrightarrow \hat{H}^0(G, \mathcal{O}_{K_\varnothing}^\times)$$

and hence an exact sequence

$$\mathcal{O}_K^\times/\mathcal{O}_K^{\times p} \longrightarrow H^2(G, \mathbb{Z}/p\mathbb{Z})^* \longrightarrow {}_p\,\mathrm{Cl}(K) \longrightarrow 0.$$

The norm map $N_{K/\mathbb{Q}} : \mathcal{O}_K^\times/\mathcal{O}_K^{\times p} \to \mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$ factors through $\mathbb{Z}^\times/\mathbb{Z}^{\times p} = 0$, hence σ acts on $\mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$ as -1. Since all morphisms above are σ-invariant, we conclude that $H^2(G, \mathbb{Z}/p\mathbb{Z})^+ = 0$. The second assertion follows because the cup product is σ-equivariant. □

By this result we immediately obtain the following corollary.

(2.3.2) Corollary. *There are well-defined triple Massey products*

$$H^1(G(K_\varnothing/K)) \times H^1(G(K_\varnothing/K)) \times H^1(G(K_\varnothing/K)) \stackrel{\langle\cdot,\cdot,\cdot\rangle}{\longrightarrow} H^2(G(K_\varnothing/K)).$$

Assume we are given a minimal presentation

$$1 \longrightarrow R \longrightarrow F \longrightarrow G(K_\varnothing/K) \longrightarrow 1$$

of $G(K_\varnothing/K)$ by a free pro-p-group F and a subgroup R which is generated as a normal subgroup of F by $\{r_i | i \in I\}$. Then for each r_i, $i \in I$, we have a pairing

$$(\mathrm{Cl}(K)/p)^* \times (\mathrm{Cl}(K)/p)^* \times (\mathrm{Cl}(K)/p)^* \overset{\langle \cdot,\cdot,\cdot \rangle}{\to} H^2(G, \mathbb{Z}/p\mathbb{Z}) \overset{\mathrm{tr}_{r_i}}{\to} \mathbb{Z}/p\mathbb{Z}$$

It is a crucial question which interpretations these pairings have.
We will sketch how they are related to certain invariants of the Galois group of the maximal p-extension of K unramified outside a certain set of primes. Assume we are given a set of primes $S = \{\mathfrak{l}_1, \ldots, \mathfrak{l}_n\}$ of K which does not contain primes of K above p, such that $\text{Ↄ}_S(K) = 0$ and such that no redundant primes are contained in S, that is $S = S_{\min}$. Denote by K_S the maximal p-extension of K unramified outside S, and let $G_S = G(K_S/K)$. For the sake of the simplicity of our presentation, we restrict ourselves to the case where K is imaginary quadratic and different from $\mathbb{Q}(\sqrt{-3})$, but we remark that similar considerations also hold for the real quadratic case. Let I_K denote the idèle group of K, and let U be the subgroup of I_K consisting of those idèles which have units at each component. We set $h = \dim_{\mathbb{F}_p} \mathrm{Cl}(K)/p$ and fix a system $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ of idèles of K whose image under the map

$$I_K \to I_K/U I_K^p K^\times = \mathrm{Cl}(K)/p$$

forms a basis of $\mathrm{Cl}(K)/p$. For $\mathfrak{l} \in S$ we denote by $K_\mathfrak{l}$ the completion of K at $\mathfrak{l}$ and by $U_\mathfrak{l}$ the unit group of $K_\mathfrak{l}$. Furthermore, let $\lambda_\mathfrak{l}$ be a uniformizer of $K_\mathfrak{l}$ and $\alpha_\mathfrak{l}$ be a generator of the cyclic group $U_\mathfrak{l}/U_\mathfrak{l}^p$. Let $\mathfrak{L}$ be an extension of $\mathfrak{l}$ to K_S. For $1 \le i \le n$ let σ_i be an element of G_S 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 $K_S^{(2)}/K$ of K_S/K is equal to $(\lambda_i, K_S^{(2)}/K)$, where λ_i denotes the idèle whose $\mathfrak{l}_i$-component equals $\lambda_{\mathfrak{l}_i}$ and all other components are 1.

For $1 \le i \le n$ let τ_i denote an element of G_S such that

(i) τ_i is an element of the inertia group $T_{\mathfrak{L}_i}$ of $\mathfrak{L}_i$ in K_S/K;

(ii) the restriction of τ_i to $K_S^{(2)}/K$ equals $(\alpha_i, K_S^{(2)}/K)$, where α_i denotes the idèle whose $\mathfrak{l}_i$-component equals $\alpha_{\mathfrak{l}_i}$ and all other components are 1.

For $1 \le i \le h$, let ω_i be an extension of $(\mathfrak{a}_i, K_S^{(2)})$. It is shown in [K] that the automorphisms $\omega_1, \ldots, \omega_h, \tau_1, \ldots, \tau_n$ form a system of generators of G_S. This system is not minimal, however. By (2.1.1) it is possible to omit h elements from the system, and it is described in [K] how to choose them among the $\tau_1, \ldots, \tau_n$: There is a system of equations

$$\prod_{i=1}^{n} \tau_1^{b_{1\nu}} \cdot \ldots \cdot \tau_n^{b_{n\nu}} \equiv \omega_\nu^{q_\nu} \mod (G_S, G_S), \quad \nu = 1, \ldots, h$$

with $b_{k\nu} \in \mathbb{Z}_p$ for $k = 1, \ldots, n$, $\nu = 1, \ldots, h$, where q_ν denotes the smallest positive integer such that $\mathfrak{a}_\nu^{q_\nu} \in UK^\times$. We assume that the redundant elements are given by $\tau_{n-h+1}, \ldots, \tau_n$. There is the following theorem.

(2.3.3) Theorem. (Koch) *Let F be the free pro-p-group on generators $x_1, \ldots, x_n$. Then $G_S(p)$ has a minimal presentation*

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

where π is given by $x_i \mapsto \omega_i$, for $i = 1, \ldots, h$, $x_i \mapsto \tau_{i-h}$ for $i = h+1, \ldots, n$. A minimal generating system of R as a normal subgroup of F is given by $\mathcal{R} = \{\rho_i\}_{1 \le i \le n}$ with

$$\rho_i = x_i^{\mathrm{N}(\mathfrak{l}_i)-1}(x_i^{-1}, y_i^{-1}),$$

where y_i is any preimage of σ_i, i.e. $\pi(y_i) = \sigma_i$.

Proof. Except for the minimality statement concerning the relations this is [K], Thm. 11.10. That $\mathcal{R}$ is a minimal system of relations follows from (2.1.1). □

Let H denote the quotient group of F by the normal subgroup N generated by $x_{h+1}, \ldots, x_n$. The following result is an immediate consequence of the above theorem.

(2.3.4) Corollary. *The group $G(K_\varnothing/K)$ has a minimal presentation*

$$1 \longrightarrow \tilde{R} \longrightarrow H \xrightarrow{\pi} G(K_\varnothing/K) \longrightarrow 1$$

where π is given by $w_i = x_i N \mapsto \omega_i$, $i = 1, \ldots, h$. A minimal generating set of $\tilde{R}$ as a normal subgroup of H is given by $\tilde{\mathcal{R}} = \{r_i\}_{1 \le i \le h}$ with

$$r_i = \rho_{n-h+i} N = x_{n-h+i} N^{\mathrm{N}(\mathfrak{l}_{n-h+i})-1}(x_{n-h+i}^{-1} N^{-1}, y_{n-h+i}^{-1} N).$$

By the remark after (1.1.27) we obtain that

$$\varepsilon_{I,p}^H(r_m) = \varepsilon_{I,p}^H(\rho_{n-h+m} N) = \varepsilon_{I,p}^F(\rho_{n-h+m})$$

for all multi-indices $I \in \mathcal{M}^h$ of height h and all $1 \le m \le h$. By (2.3.1) this gives us the following extra information on G_S:

$$\varepsilon_{(i,j),p}^F(\rho_{n-h+m}) = 0$$

for all $1 \le i, j, m \le h$. A short calculation shows that this means that

$$\varepsilon_{(i),p}^F(x_{n-h+m})\varepsilon_{(j),p}^F(y_{n-h+m}) = \varepsilon_{(j),p}^F(x_{n-h+m})\varepsilon_{(i),p}^F(y_{n-h+m})$$

for all $1 \le i, j, m \le h$. This may in turn be used to calculate the trace of the triple Massey product on $H^1(G(K_\varnothing/K))$. Denote by $\{\chi_1, \ldots, \chi_h\}$ the dual basis of $H^1(G(K_\varnothing/K)) = (\mathrm{Cl}(K)/p)^*$ to $\{w_1, \ldots, w_h\}$. A lengthy calculation using (1.2.6), (1.1.22) and the above identity gives the following expression for

the trace of the triple Massey product on $H^1(G(K_\varnothing/K))$ completely in terms of G_S:

$$\begin{aligned}\mathrm{tr}_{r_m}\langle\chi_i,\chi_j,\chi_k\rangle &= \varepsilon^F_{(i),p}(x_{\tilde m})\varepsilon^F_{(j,k),p}(y_{\tilde m}) - \varepsilon^F_{(k),p}(x_{\tilde m})\varepsilon^F_{(i,j),p}(y_{\tilde m})\\ &\quad -\varepsilon^F_{(i),p}(y_{\tilde m})\varepsilon^F_{(j,k),p}(x_{\tilde m}) + \varepsilon^F_{(k),p}(y_{\tilde m})\varepsilon^F_{(i,j),p}(x_{\tilde m})\\ &\quad +\binom{\mathrm{N}(\mathfrak{l}_{\tilde m})-1}{3}\varepsilon^F_{(i),p}(x_{\tilde m})\varepsilon^F_{(j),p}(x_{\tilde m})\varepsilon^F_{(k),p}(x_{\tilde m})\end{aligned}$$

for $1 \le i,j,k,m \le h$ where we have put $\tilde m = n-h+m$. The last term vanishes for $p \neq 3$. The natural objects to study are the $\varepsilon^F_{I,p}(y_i)$ for index sets $I \in \mathcal{M}^n$ and $1 \le i \le n$ which should be seen as Milnor invariants as in §1, and the $\varepsilon^F_{I,p}(x_i)$ for index sets $I \in \mathcal{M}^n$ and $n-h+1 \le i \le n$ which are absent in the case of $G_S(\mathbb{Q})$. However, we are far from understanding them.

Appendix A

Link theory

In this appendix we present some results from link theory which are analogous to our results in algebraic number theory. This presentation follows closely along the lines of [P].
We denote by $C(n)$ the space consisting of n disjoint oriented circles. An ***n*-link** in the sphere S^3 is an embedding

$$L : C(n) \hookrightarrow S^3.$$

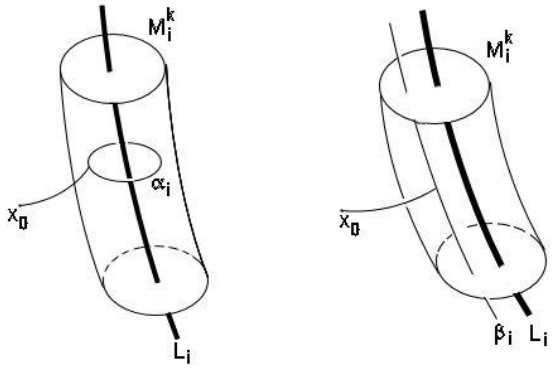
We will use the symbol L to denote either the embedding or its image in S^3. Two links L, L' are called **isotopic** if there is a continuous 1-parameter family of links h_t with $h_0 = L$ and $h_1 = L'$.
The **group of a link *L*** is by definition the fundamental group of the link complement:

$$\pi = \pi_1(S^3 - L).$$

The lower central series of π is defined as usual by $\pi_1 = \pi$, $\pi_{k+1} = [\pi_k, \pi]$ where $[\pi_k, \pi]$ denotes the subgroup of π generated by elements of the form $aba^{-1}b^{-1}$, $a \in \pi_k$, $b \in \pi$. The quotients π/π_k are called the **Chen groups** of the link. Let $L_1, \ldots, L_n$ denote the components of the link.
We choose pairwise disjoint connected neighborhoods $M_1^0, \ldots, M_n^0$ of $L_1, \ldots, L_n$. For each $i = 1, \ldots, n$ we choose a sequence $M_i^0 \supseteq M_i^1 \supseteq \ldots \supseteq M_i^k$ of connected open neighborhoods of L_i such that M_i^j can be deformed into L_i within M_i^{j-1} for each $j = 1, \ldots, k$. This means that there is a homotopy $r_t : M_i^j \to M_i^{j-1}$ such that r_0 is the inclusion map and $r_1(M_i^j) \subseteq L_i$. We let the base point x_0 be a point in $S^3 - \bigcup_{i=1}^n M_i^0$. For each i we choose a path $p_i(t)$, $0 \leq t \leq 1$, from x_0 to L_i. An ***i*-th meridian** α_i of L with respect to the path p_i is defined as follows: First we traverse the path p_i to a point in $M_i^k - L_i$, then we traverse a closed loop in $M_i^k - L_i$ which has linking number $+1$ with L_i and is homotopic to a constant in M_i^q, and finally we return to x_0 along p_i. (For several equivalent definitions of linking numbers, see [Ro].) This procedure defines a unique element α_i of π/π_k. An ***i*-th longitude** β_i of L with respect to the path p_i is an element of π/π_k obtained by traversing p_i from x_0 to a point in $M_i^k - L_i$, then traversing

a closed loop in $M_i^k - L_i$ which is homotopic to L_i within M_i^k and has linking number 0 with L_i, and finally returning to x_0 along p_i. This defines a unique element $\beta_i \in \pi/\pi_k$. If p_i is replaced by some other path then the pair (α_i, β_i) is replaced by a conjugate pair. There is the following result on Chen groups.

Figure A.1: meridian and longitude



(A.1) Theorem. (Chen, Milnor) *Let L be an n-link and F the free group on generators $x_1, \ldots, x_n$. The Chen group π/π_k of an n-link L has the presentation*

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\kappa} \pi/\pi_k \longrightarrow 1,$$

where κ is given by $x_i \mapsto \alpha_i$, $i = 1, \ldots, n$ and $\alpha_1, \ldots, \alpha_n$ are meridians of L. The group R is generated as a normal subgroup of F by F_k and $[x_i, w_i]$ where the w_i are elements of F with $\kappa(w_i) = \beta_i$ for $i = 1, \ldots, n$ and $\beta_1, \ldots, \beta_n$ are longitudes of L.

By virtue of this theorem we are now in a position to define the Milnor invariants of a link. Let $\mathbb{Z}\langle\langle X_1, \ldots, X_n \rangle\rangle$ be the power series ring over $\mathbb{Z}$ in n non-commuting variables. The **Magnus expansion** is the homomorphism

$$m : \mathbb{Z}[F] \to \mathbb{Z}\langle\langle X_1, \ldots, X_n \rangle\rangle$$

which is given on generators by

$$m(x_i) = 1 + X_i, \quad m(x_i^{-1}) = 1 - X_i + X_i^2 - X_i^3 + \ldots, \quad i = 1, \ldots, n.$$

If we are given a sequence $(l_1, \ldots, l_m)$ of integers with $1 \leq l_i \leq n$ and $m < k$, we set $\mu(l_1, \ldots, l_m)$ equal to the coefficient of $X_{l_1} \cdot \ldots \cdot X_{l_{m-1}}$ in the Magnus expansion of w_m. We put $\Delta(l_1, \ldots, l_m)$ equal to the greatest common divisor of the numbers $\mu(j_1, \ldots, j_s)$ where $(j_1, \ldots, j_s)$ ranges over all cyclic permutations of proper subsequences of $(l_1, \ldots, l_m)$. The **Milnor invariant $\bar{\mu}(l_1, \ldots, l_m)$**

of the link is the residue class of $\mu(l_1,\dots,l_m)$ modulo $\Delta(l_1,\dots,l_m)$. It has been shown by Milnor, see [Mi], that $\bar{\mu}(l_1,\dots,l_m)$ is an isotopy invariant of L and a homotopy invariant of L if the l_i are distinct.
Massey products of elements in H^1 are defined as follows. Let $\{X_i\}_{i=1,\dots,m}$ be a collection of subspaces of a space X. Given elements u_i in $H^1(X_i,R)$ for $i=1,\dots,m$, where R is a commutative ring with unit, a **defining system** for the Massey product $\langle u_1,\dots,u_m\rangle$ in the system $\{X_i\}_{i=1}^m$ with coefficients in R is a collection $m_{i,j}$, $1\le i\le j\le m$, $(i,j)\neq(1,m)$, satisfying:

(i) $m_{i,j}\in C^1(X_i\cap X_{i+1}\cap\dots\cap X_j,R)$,

(ii) $m_{i,i}$ is a cocycle representative of u_i, for $i=1,\dots,m$.

(iii) $\delta(m_{i,j})=\sum_{k=i}^{j-1} m_{i,k}m_{k+1,j}$ for $i<j$ where $m_{i,k}m_{k+1,j}$ denotes the cup product in $C^*(X_i\cap\dots\cap X_j,R)$ of the restrictions of $m_{i,k}$ and $m_{k+1,j}$ to $X_i\cap\dots\cap X_j$.

Here $C^*(Y,R)$ denotes the complex of singular cochains of Y with coefficients in R. It follows that $\sum_{k=1}^{m-1} m_{1,k}m_{k+1,m}$ is a cocycle in $C^2(X_1\cap\dots\cap X_m,R)$. We say that $\langle u_1,\dots,u_m\rangle$ **is defined** if there is a defining system for it, in which case $\langle u_1,\dots,u_m\rangle$ is the subset $H^2(X_1\cap\dots\cap X_m,R)$ consisting of all elements representable by cocycles of the form $\sum_{k=1}^{m-1} m_{1,k}m_{k+1,m}$ with $\{m_{i,j}\}$ a defining system for $\langle u_1,\dots,u_m\rangle$.
Assume we are given an n-link L in S^3. We set u_i equal to the element in $H^1(S^3-L)$ which corresponds by Alexander duality to the generator of $H_1(L_i)$ determined by the orientation of L_i. For $1\le i,j\le n$ set $\gamma_{i,j}$ equal to the element in $H^2(S^3-(L_i\cup L_j))$ which corresponds by Lefschetz duality to the element in $H_1(S^3,L_i\cup L_j)$ determined by a path from L_i to L_j. There is the following result on the relationship between the $\bar{\mu}$-invariants of a link and Massey products in the link complement.

(A.2) Theorem. (Porter, Turaev) *Let L be an n-link in S^3. For any sequence $(l_1,\dots,l_m)$ of integers with $1\le l_j\le n$, the Massey product $\langle u_{l_1},\dots,u_{l_m}\rangle$ in the system $\{S^3-L_{l_i}\}_{i=1,\dots,m}$ with coefficients $\mathbb{Z}/\Delta(l_1,\dots,l_p)\mathbb{Z}$ is defined and contains the single element $(-1)^m\bar{\mu}(l_1,\dots,l_m)\gamma_{l_1,l_m}$.*

We may consider Massey products in S^3-L as well, where the elements in a defining system for a product in S^3-L are only required to be cochains in S^3-L. The Massey product $\langle u_{l_1},\dots,u_{l_m}\rangle$ in the system $\{S^3-L_{l_i}\}_{i=1,\dots,m}$ is always a subset of the Massey product $\langle u_{l_1},\dots,u_{l_m}\rangle$ in $S^3-\cup_{i=1}^m L_i$. However, in general the last set may contain more than one element. There is the following variant of the theorem of Porter-Turaev.

(A.3) Theorem. (Porter, Turaev) *Let L be an n-link in S^3. Let $(l_1,\dots,l_m)$ be a sequence of integers with $1\le l_j\le n$. Assume that $\mu(k_1,\dots,k_s)=0$ for all $1<s<m$ and all sequences $(k_1,\dots,k_s)$ of integers with $1\le k_j\le n$. Then the Massey product $\langle u_1,\dots,u_{l_m}\rangle$ in S^3-L with coefficient ring $\mathbb{Z}$ is defined and contains the single element $(-1)^m\mu(l_1,\dots,l_m)\gamma_{l_1,l_m}$.*

Bibliography

[CFL] 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

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

[DDMS] 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)

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

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

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

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

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

[K] Koch, H.: *Galoissche Theorie der p-Erweiterungen.* Deutscher Verlag der Wiss., 1970 (English translation Berlin 2002)

[K2] Koch, H.: *On p-extensions with given ramification.* Appendix 1 in [Ha]

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

[KV] Koch, H., Venkov, B.: *Über den p-Klassenkörperturm eines imaginärquadratischen Zahlkörpers.* Astérisque 24-25 (1975), 57-67

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

[Mi] Milnor, J.: *Isotopy of links.* Proc. Symp. in Honor of S. Lefschetz, 280-306, Princeton 1957

[N] Neukirch, J.: *Algebraische Zahlentheorie.* Springer 1992

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

[P] Porter, R.: *Milnor's $\bar{\mu}$-invariants and Massey products.* Trans. Am. Math. Soc. 257 (1980), 39-71

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

[Ro] Rolfsen, D.: *Knots and links.* Publish or Perish, Berkeley 1976

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

[Sh] Sharifi, R.: *Massey products and ideal class groups.* preprint

[T] Turaev, V.G.: *Milnor invariants and Massey products.* J. Sov. Math. 12 (1979), 128-137

[W] Waldspurger, J.-L.: *Entrelacements sur Spec*($\mathbb{Z}$), Bull. Sci. Math. 100 (1976), 113-139

[Wi] Wingberg, K.: *On the Fontaine-Mazur conjecture for CM-fields.* Comp. Math. 131 (2002), 341-354