Inaugural-Dissertation

zur Erlangung der Doktorwürde der
Naturwissenschaftlich-Mathematischen Gesamtfakultät der
Ruprecht-Karls-Universität Heidelberg

vorgelegt von
Diplom-Mathematiker Jochen Gärtner
aus Heilbronn

Tag der mündlichen Prüfung: 22. November 2011

Mild pro-p-groups with trivial cup-product

Gutachter: Prof. Dr. Kay Wingberg

Prof. Dr. Alexander Schmidt

Abstract

Using results of J. Labute on strongly free sequences in free Lie algebra (cf. [Lab06]), A. Schmidt proved a sufficient conditions for a finitely presented pro-p-group G to be mild and hence in particular of cohomological dimension $cd\, G = 2$ (cf. [Sch06], [Sch10]). This criterion admits an elegant formulation in terms of the cup-product $H^1(G, \mathbb{Z}/p\mathbb{Z}) \times H^1(G, \mathbb{Z}/p\mathbb{Z}) \overset{\cup}{\to} H^2(G, \mathbb{Z}/p\mathbb{Z})$. In particular, one requires it to be surjective. In this thesis, we study the complementary case of finitely presented pro-p-groups G having trivial cup-product. Under this assumption there exist higher Massey products which are closely related to the Zassenhaus filtration of G. We give an explicit description of the structure of the graded Lie algebras associated to (generalized) Zassenhaus filtrations of free pro-p-groups and establish analogues of Labute's results for pro-p-groups which are mild with respect to these filtrations. We formulate and prove a generalization of Schmidt's criterion for arbitrary higher Massey products. Further investigations are pursued in the special case of one-relator pro-p-groups. We construct a class of mild pro-2-groups having trivial cup-product, which occur as Galois groups $G_S(2)$ of the maximal 2-extensions of $\mathbb{Q}$ unramified outside certain finite sets of places S. To this end, we generalize the description of the triple Massey product via Rédei symbols given by M. Morishita and D. Vogel (cf. [Mor02], [Vog04]) to the case of wild ramification. Finally this product is determined explicitly for Galois groups of the form $G_S^T(2)$ (i.e. in addition to restricted ramification the corresponding extensions are completely decomposed above the set of primes T) and an example of a fab pro-p-group of cohomological dimension 2 having only 3 generators is constructed.

Zusammenfassung

Aufbauend auf Ergebnisse von J. Labute über stark freie Sequenzen in freien Lie-Algebren (s. [Lab06]), entwickelte A. Schmidt eine hinreichende Bedingung, unter welcher eine endlich präsentierte pro-p-Gruppe G mild, also insbesondere von kohomologischer Dimension $cd\, G = 2$, ist (s. [Sch06],[Sch10]). Dieses Kriterium lässt auf elegante Weise durch das gruppenkohomologische Cup-Produkt $H^1(G, \mathbb{Z}/p\mathbb{Z}) \times H^1(G, \mathbb{Z}/p\mathbb{Z}) \overset{\cup}{\to} H^2(G, \mathbb{Z}/p\mathbb{Z})$ ausdrücken und fordert insbesondere die Surjektivität desselbigen. In der vorliegenden Arbeit betrachten wir den komplementären Fall endlich präsentierter pro-p-Gruppen G mit verschwindendem Cup-Produkt. Unter dieser Voraussetzung existieren höhere Massey-Produkte, die im engen Zusammenhang mit der Zassenhaus-Filtrierung von G stehen. Für (verallgemeinerte) Zassenhaus-Filtrierungen auf freien pro-p-Gruppen geben wir eine explizite Beschreibung der Struktur der assoziierten graduierten Lie-Algebren an und übertragen Labutes Resultate auf Gruppen, die bezüglich dieser Filtrierungen mild sind. Wir formulieren und beweisen eine Verallgemeinerung von Schmidts Kriterium für beliebige höhere Massey-Produkte. Eine weitere Vertiefung dieser Resultate wird im Falle endlich erzeugter pro-p-Gruppen mit $\dim_{\mathbb{F}_p} H^2(G) = 1$ erreicht. Wir konstruieren eine Klasse milder pro-2-Gruppen mit trivialem Cup-Produkt, welche als Galoisgruppen $G_S(2)$ der maximalen außerhalb bestimmter endlicher Stellenmengen S unverzweigter 2-Erweiterungen von $\mathbb{Q}$ auftreten. Hierzu verallgemeinern wir die von D. Vogel und M. Morishita (s. [Mor02], [Vog04]) bewiesene Beschreibung des dreifachen Massey-Produkts mittels Rédei-Symbolen auf den Fall wilder Verzweigung. Schließlich wird eine explizite Darstellung dieses Produkts für Galoisgruppen der Form $G_S^T(2)$ (d.h. neben der auf S beschränkten Verzweigung wird zusätzliche volle Zerlegung über der Stellenmenge T gefordert) gegeben und wir konstruieren so eine Fab-pro-p-Gruppe der kohomologischen Dimension 2 mit lediglich 3 Erzeugern.

Contents

Introduction

Mild pro-p-groups and p-extensions with restricted ramification

The introduction of Galois cohomological techniques is doubtlessly one of the major landmarks of 20th century algebraic number theory. For example, *class field theory* for a local or global field k is nowadays usually formulated via cohomological duality properties of the absolute Galois group G_k of k together with a description of the *dualizing module* in terms of arithmetic data. In this context, the *reciprocity map,* which classically has been formulated as a mapping of generalized ideal class groups, occurs as a special case of a perfect pairing of certain cohomology groups induced by the cup-product. The question whether for a given profinite extension of a local or global field k such duality properties hold is of group theoretical nature and hence makes sense for arbitrary, i.e. not necessarily arithmetically defined, profinite groups. One central task related to this *abstract class field theory* of a given profinite group is to determine its *cohomological dimension*. The duality theorems in group cohomology, which are mainly due to J. Tate, can of course be considered as analogs of classical duality theorems such as *Poincaré duality*. As for the dimension of a manifold, it is the cohomological dimension that indicates the dimension of the (possibly perfect) cup-product pairing.

The central objects studied in this thesis are *mild* pro-p-groups. The concept of mild groups has first been developed by J. Labute in [Lab85] in the case of discrete groups and since then been studied extensively by J. Labute, D. Anick et al.*) They have become of great importance for algebraic number theory and arithmetic geometry since in [Lab06] J. Labute applied mild pro-p-groups to study tamely ramified p-extensions of the rationals. This has recently led to much more far-reaching results due to A. Schmidt (e.g. see [Sch10]). Mild pro-p-groups constitute examples of finitely presented pro-p-groups which are of cohomological dimension ≤ 2. This is the main reason for their importance not only from a group theoretical but also from an arithmetic point of view. Their definition is based on the existence of *strongly free* presentations via free groups. Although the notion of a strongly free presentation might appear rather technical at first sight, it can be motivated in a plausible way by the following well-known fact: Let G be a pro-p-group and

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

*) The term "mild" has been introduced by D. Anick in [Ani87].

be a *minimal presentation*, i.e. F is a free pro-p-group and the inflation map $inf : H^1(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(F, \mathbb{Z}/p\mathbb{Z})$ is an isomorphism. The complete group ring $\mathbb{F}_p[\![G]\!]$ operates (from the left) on the $\mathbb{F}_p$-vector space $R/R^p[R,R]$ via conjugation and the following equivalence holds: The cohomological dimension $cd\ G$ of G satisfies $cd\ G \leq 2$ if and only if $R/R^p[R,R]$ is a free $\mathbb{F}_p[\![G]\!]$-module of rank $m := \dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z})$. Now assume that G is finitely presented and $r_1, \ldots, r_m$ is a system of defining relations, i.e. the r_i generate R as a closed normal subgroup of F. Consider the *Zassenhaus filtration* $F = F_{(1)} \supseteq F_{(2)} \supseteq \ldots$ of F. The associated graded object

$$\operatorname{gr} F = \bigoplus_{i=1}^{\infty} F_{(i)}/F_{(i+1)}$$

carries the structure of a $\mathbb{F}_p$-Lie algebra, more precisely it is a graded *restricted Lie algebra* over $\mathbb{F}_p$. If the sequence of initial forms $\rho_i \in \operatorname{gr} F$ of the r_i satisfies a certain condition of being "free in maximum possible way", one can derive that $R/R^p[R,R]$ is free as $\mathbb{F}_p[\![G]\!]$-module and hence in particular $cd\ G \leq 2$ holds. Such a sequence $\rho_1, \ldots, \rho_m$ is called *strongly free* and in this case we say that G admits a *strongly free presentation*. It is one advantage of this approach that no complete knowledge of the generating relations of G is required. This can be crucial for arithmetic situations, where for example a description of appropriately chosen relations modulo the third step of the Zassenhaus filtration is possible via class field theory. Furthermore, since $\operatorname{gr} F$ is a locally finite graded $\mathbb{F}_p$-vector space, one can use computations of Poincaré series to derive sufficient criteria for a given sequence to be strongly free. One should note that one can define mild pro-p-groups in an analogous way with respect to different types of filtrations. In fact, in [Lab06] J. Labute studies strongly free sequences with respect to (generalized) descending p-central series. Basically this amounts to the same strategy, however the structure of $\operatorname{gr} F$ as $\mathbb{F}_p$-Lie algebra is slightly different in these cases. As will be made more precise below, with a view towards relating mild pro-p-groups to *higher Massey products* we have to consider Zassenhaus filtrations instead.

These sufficient (though in general not necessary) criteria for which a given pro-p-group is of cohomological dimension ≤ 2 apply to many arithmetically defined groups. In particular, one is interested in studying the maximal pro-p-quotient

$$G_{S \cup S_\infty}(p) = \pi_1^{et}(X_{k,S})(p)$$

of the étale fundamental group of the arithmetic curve $X_{k,S} := Spec(\mathcal{O}_k) \setminus S$ where k is a number field, $\mathcal{O}_k$ denotes its ring of integers and S is a finite set of finite primes. In other words, $G_{S \cup S_\infty}(p)$ is the Galois group of the maximal p-extension $k_{S \cup S_\infty}(p)$ of k unramified outside S and the set of infinite primes S_∞.*) If S contains the set S_p of primes of k lying above p and k is totally imaginary if $p = 2$, it is well-known that $cd\ G_S(p) \leq 2$ (cf. [NSW08], Ch.

*) Of course, the assumption that S is a finite set is a priori not necessary. However, we focus on this case, since on the one hand $G_{S \cup S_\infty}(p)$ is finitely generated then. On the other hand, "large" sets of primes having Dirichlet density $\delta(S) = 1$ are well understood.

X).*) Furthermore, it is often a duality group (cf. [Win89]) and there is an arithmetic version of *Riemann's existence theorem* stating that the Galois group $\mathrm{Gal}(k_S(p)|k_{S_p}(p))$ admits a free product decomposition by local inertia groups. Under some further assumptions, similar results have been obtained for the *mixed case*, i.e. if $\varnothing \subsetneq S \cap S_p \subsetneq S_p$ (e.g. see [Win86] and [Mai05]). On the contrary, in the *tame* case, i.e. if $S_p \cap S = \varnothing$, until recently there have been no results about the cohomological dimension of $G_{S\cup S_\infty}(p)$ except if $p = 2$ and k has a real prime ramifying in $k_{S\cup S_\infty}(2)$ (in which case obviously $cd\, G_{S\cup S_\infty}(p) = \infty$). Among the comparatively few facts that have been known are the following (henceforth S denotes an arbitrary finite set of primes of k disjoint from S_p, i.e. S may also contain infinite primes): $G_S(p)$ is a finitely presented *fab* pro-p-group (i.e. the abelianization H^{ab} is finite for any open subgroup $H \subseteq G_S(p)$) and by the *Golod-Šafarevič theorem* it can be infinite. Furthermore, by results of I.R. Šafarevič and H. Koch (cf. [Koc02], Ch.11.4), under certain conditions a minimal presentation of these groups can be given explicitly with the relations generated by *local relations*, which can be determined explicitly modulo the third step of the p-central series. Using the latter presentations, in his 2006 article [Lab06], J. Labute came up with the first examples of finite sets S of primes of $\mathbb{Q}$ such that $S \cap S_p = \varnothing$ for an odd prime p and $cd\, G_S(p) = 2$ by showing that under certain conditions these groups are mild, cf. [Lab06]. For instance, this holds if the *linking diagram* associated to S is a *non-singular circuit*, cf. [Lab06], Th.1.6. Moreover, an elegant application of the Čebotarev density theorem shows that for any given set S one can always find a finite set S_0 disjoint from $S \cup S_p$ such that $G_{S\cup S_0}(p)$ is mild.**)

Under the additional condition that the natural homomorphism

$$H^2(G_S(p), \mathbb{F}_p) \longrightarrow H^2_{et}(X_{\mathbb{Q},S}, \mathbb{F}_p)$$

is surjective (which for instance is always satisfied in the examples given in [Lab06]), A. Schmidt showed that $cd\, G_S(p) \leq 2$ implies the following geometric formulation, see [Sch06]: The scheme X_S is a $K(\pi, 1)$ *for* p, i.e. for any discrete p-primary module M of $G_S(p)$, the Galois cohomology $H^i(G_S(p), M)$ coincides with the étale cohomology $H^i_{et}(X_S, M)(p)$ (of the locally constant étale sheaf M). Using arithmetic arguments, Schmidt weakened Labute's condition on the set S in order to obtain $cd\, G_S(p) \leq 2$ and proved that in these cases $G_S(p)$ is a duality group of *strict cohomological dimension* $scd\, G_S(p) = 3$ and the dualizing module can be described in terms of idèle classes (cf. [Sch06]). Furthermore, he showed that for any prime $l \in S$ the extension $\mathbb{Q}_S(p)$ realizes the maximal p-extension of $\mathbb{Q}_l$ ***) and that an arithmetic form of Riemann's existence theorem holds. There has been much effort in transferring these results to more general situations, such as to the mixed case, to number fields different

*) In fact, for $p = 2$ this is also true for an arbitrary number field k if S contains no real prime, cf. [Sch02], Th.1.

**) It is not hard to show that this can always be achieved by adding at most 2 primes, see [FG09].

***) This is the tame case analogue of Kuz'min's theorem, cf. [NSW08], Th.10.8.4.

from $\mathbb{Q}$ and to more general classes of arithmetically defined pro-p-groups, e.g. see [Sch06], [Vog06], [Vog07], [Win07].

In [Sch10], Th.1.1, A. Schmidt obtained the following remarkable result on the existence of $K(\pi,1)'s$ over an arbitrary number field k:

Theorem (Schmidt). *Let p be an odd prime different from* $\mathrm{char}(k)$*. Let S be a finite set of primes and $\mathcal{M}$ an arbitrary set of primes with Dirichlet density $\delta(\mathcal{M}) = 0$. Then there exists a finite set of primes S_0 disjoint from $S \cup \mathcal{M}$ such that $Spec(\mathcal{O}_k) \setminus (S \cup S_0)$ is a $K(\pi,1)$ for p.*

The precise statement of Schmidt's theorem is actually even stronger: Firstly the theorem deals with the more general groups $G_S^T(p)$, i.e. the Galois group of the maximal pro-p-extension of k unramified outside S and completely decomposed at the primes in T. This generalization is also crucial for avoiding restrictions on the p-th roots of unity and the p-part of the ideal class group of k. Moreover analogous results to the case $k = \mathbb{Q}$ hold, i.e. for the primes in $S \cup S_0$ the complete maximal pro-p-extensions of the associated local fields are realized, an arithmetic version of Riemann's existence theorem holds and under additional assumptions duality properties are obtained. One important ingredient in the proof is the following [Sch10], Th.6.2:

Theorem (Schmidt). *Let p be an odd prime number and G be a finitely presented pro-p-group such that $H^2(G) \neq 0$.*[*)] *Assume that $H^1(G)$ admits a decomposition $H^1(G) = U \oplus V$ as $\mathbb{F}_p$-vector space, such that the following holds:*

(i) *The cup-product $V \otimes V \xrightarrow{\cup} H^2(G)$ is trivial.*

(ii) *The cup-product $U \otimes V \xrightarrow{\cup} H^2(G)$ is surjective.*

Then cd $G = 2$.

This result is a cohomological reformulation of [Sch06], Th.5.5, where, using Labute's results on strongly free sequences in Lie algebras, it is shown that such pro-p-groups are mild. The same statement is true for pro-2-groups, which has been proven by J. Labute and J. Mináč [LM11] and later independently by P. Forré [For10]. Obviously the assumptions of the above criterion imply the surjectivity of the cup-product $H^1(G) \otimes H^1(G) \xrightarrow{\cup} H^2(G)$. Equivalently, if $G = F/R$ is a minimal presentation of G and $r_1, \ldots, r_m \in R \cap F_{(2)}$ is a minimal system of defining relations, then the r_i are linearly independent modulo $F_{(3)}$. If this is not the case, e.g. if $R \subseteq F_{(3)}$, then G can still be mild, but the cup-product doesn't contain enough information. If the cup-product vanishes, there exist well-defined *higher Massey products*. It has been shown independently by M. Morishita [Mor04] and D. Vogel [Vog04], that in analogy to a well-known result on the cup-product (cf. [NSW08], Th.3.9.13), the defining relations can be determined modulo higher filtration steps of the Zassenhaus filtration via these products. In this thesis we investigate the notion of mild pro-p-groups *with respect to (generalized) Zassenhaus filtrations* and prove a generalization

[*)] For a pro-p-group G we set $H^i(G) := H^i(G, \mathbb{Z}/p\mathbb{Z}),\ i \geq 0$.

of Schmidt's theorem to arbitrary Massey products (and arbitrary p). Furthermore, we give arithmetic examples of these groups in terms of Galois groups of the form $G_S^T(2)$ over the rationals.

Structure of this thesis and main results

As we have already remarked, there is a close link between Massey products and the Zassenhaus filtration of finitely presented pro-p-groups. In the first chapter, we investigate the structure of the associated Lie algebras of certain *p-restricted filtrations of* free pro-p-groups and study the notion of mild pro-p-groups with respect to these filtrations.

If $(G_i)_{i\in\mathbb{N}}$ is a p-restricted filtration of the (pro-p-group) G, i.e.

$$[G_i, G_j] \subseteq G_{i+j}, \quad G_i^p \subseteq G_{pi},$$

the associated graded object $\operatorname{gr} G = \bigoplus_{i=1}^{\infty} G_i/G_{i+1}$ is a graded *restricted Lie algebra* over $\mathbb{F}_p$. A special class of these filtrations is given by the *Zassenhaus (x,τ)-filtrations* $(F_{(\tau,i)})_{i\in\mathbb{N}}$ of a finitely generated free pro-p-group F on generators $x = \{x_1, \ldots, x_d\}$ with weights $\tau = (\tau_1, \ldots, \tau_d)$, which are induced by natural filtrations of the complete group ring $\mathbb{F}_p[\![F]\!]$. Concerning the structure of $\operatorname{gr} F$, we prove the following

Theorem (1.3.8)**.** *Let F be the free pro-p-group on the set $x = \{x_1, \ldots, x_d\}$ and let $\tau_1, \ldots, \tau_d \in \mathbb{N}$. Then $\operatorname{gr}^\tau F = F_{(\tau,i)}/F_{(\tau,i+1)}$ is a free restricted Lie algebra over $\mathbb{F}_p$ on the images of the x_i in $\operatorname{gr} F$.*

This result might seem classical, but according to the author's knowledge it cannot be found in the standard literature. For the proof we can make use of techniques similar to those used in [Laz65], where the lower p-central series is considered instead of the Zassenhaus filtration. In this case the associated graded Lie algebra is a free Lie algebra over the polynomial ring $\mathbb{F}_p[\pi]$. However, this only holds in the case $p > 2$. If $p = 2$, one has to deal with *mixed Lie algebras* instead (cf. [Laz65], Ch.II, §3). Apart from the fact that the Zassenhaus filtration is the "natural" filtration when studying higher Massey products, it is another advantage that the above theorem holds for arbitrary p.

We investigate the notion of *strongly free sequences* of homogeneous polynomials in the non-commutative polynomial ring $\mathbb{F}_p\langle X_1, \ldots, X_n\rangle$. We give equivalent characterizations and recall criteria due to J. Labute (for polynomials of Lie type) and D. Anick ([Ani82]). Anick's criterion is a powerful tool which applies to arbitrary polynomials. It is based on the notion of a *combinatorially free* sequence of monomials. We introduce a special *multiplicative monomial order*, which will later be crucial in the proof of the Massey product criterion, cf. (2.3.2). The last section is devoted to the study of finitely presented pro-p-groups which are mild with respect to the Zassenhaus (x,τ)-filtration. The main result is the following

Theorem (1.5.10)**.** *Let F be the free pro-p-group on $x = \{x_1, \ldots, x_d\}$ endowed with the (x, τ)-filtration for some $\tau = (\tau_1, \ldots, \tau_d)$. Let G be a mild pro-p-group such that $G = F/R = \langle x_1, \ldots, x_d \mid r_1, \ldots, r_m \rangle$ is a strongly free presentation with respect to the Zassenhaus (x, τ)-filtration where $R \subseteq F_{(\tau,2)}$ denotes the closed normal subgroup generated by r_i, $i = 1, \ldots, m$. Set $\sigma_i := \deg^\tau r_i$, $i = 1, \ldots, m$. Then the following holds:*

(i) *We have $\operatorname{cd} G = 2$ and the relation rank $h^2(G)$ of G is equal to m.*

(ii) *The $\mathbb{F}_p[\![G]\!]$-module $R/R^p[R, R]$ is free over the images of $r_1, \ldots, r_m$.*

(iii) *We have $\operatorname{gr}^\tau(G) = \operatorname{gr}^\tau(F)/(\rho_1, \ldots, \rho_m)$ where $(\rho_1, \ldots, \rho_m)$ denotes the ideal of the restricted Lie algebra $\operatorname{gr}^\tau(F)$ generated by the initial forms ρ_i of r_i.*

(iv) *The universal enveloping algebra $U_{\operatorname{gr}^\tau(G)}$ of $\operatorname{gr}^\tau(G)$ is the graded algebra associated to the filtration on $\mathbb{F}_p[\![G]\!]$ induced by the (x, τ)-filtration on $\mathbb{F}_p[\![F]\!]$ and its Poincaré series satisfies*

$$U_{\operatorname{gr}^\tau(G)}(t) = \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d}) + (t^{\sigma_1} + \ldots + t^{\sigma_m})}.$$

This generalizes previous results due to J. Labute ([Lab06], Th.5.1) and P. Forré ([For10], Th.3.7); here we don't have to assume that the initial forms ρ_i are Lie polynomials and we obtain an explicit description of the restricted Lie algebra $\operatorname{gr} G$.

In the second chapter we state and prove a criterion analogous to Schmidt's cup-product criterion involving higher Massey products. In the first section we do this for finitely presented pro-p-groups with relations of degree 3, since in this case we can apply Labute's technique based on the *elimination theorem* for free Lie algebras. For relations of higher degree, the structure of the basic commutators becomes unhandy. However, using Massey products we can apply Anick's criterion with respect to the monomial order introduced in the first chapter. After recalling the definition of higher Massey products and its basic properties, we cite a theorem due to D. Vogel relating these products to the Zassenhaus filtration. In order to state the main result, we suggest the following notation: For a finitely presented pro-p-group G we define the *Zassenhaus invariant* $\mathfrak{z}(G)$ as the supremum of all natural numbers $n \in \mathbb{N}$ such that in a minimal presentation $G = F/R$ we have $R \subseteq F_{(n)}$.

Theorem (2.3.2)**.** *Let G be a finitely presented pro-p-group with Zassenhaus invariant $\mathfrak{z}(G) = n < \infty$. Assume that $H^1(G)$ admits a decomposition $H^1(G) = U \oplus V$ as $\mathbb{F}_p$-vector space such that for some natural number e with $1 \leq e \leq n-1$ the n-fold Massey product $\langle \cdot, \ldots, \cdot \rangle : H^1(G)^n \longrightarrow H^2(G)$ satisfies the following conditions:*

(a) *We have $\langle \xi_1, \ldots, \xi_n \rangle = 0$ for all tuples $(\xi_1, \ldots, \xi_n) \in H^1(G)^n$ such that $\#\{i \mid \xi_i \in V\} \geq n - e + 1$.*

(b) $\langle \cdot, \ldots, \cdot \rangle$ *maps*

$$U^{\otimes e} \otimes V^{\otimes n-e}$$

surjectively onto $H^2(G)$.

Then G is mild with respect to the Zassenhaus filtration. In particular, G is of cohomological dimension cd $G = 2$.

Important examples of finitely presented pro-p-groups are constituted by *one-relator pro-p-groups*, which for instance occur as the maximal pro-p-quotient of the absolute Galois group of a local field containing the p-th roots of unity. If the cup-product pairing $H^1(G) \times H^1(G) \to H^2(G)$ of the one-relator pro-p-group G is non-degenerate, then G is a duality group of dimension 2.*) More generally, it has been known by a result by J. Labute [Lab67a], that $G = F/(r)$ is of cohomological dimension 2 if the generating relation r is not "too close" to being a p-th power. Using the results on bases of free restricted Lie algebras, we obtain the following more general statement:

Theorem (2.4.6)**.** *Let G be a one-relator pro-p-group such that the Zassenhaus invariant $\mathfrak{z}(G)$ is prime to p. Then G is mild with respect to the Zassenhaus filtration.*

Finally we discuss an open question due to Serre and show that if $G = F/(r)$ is a one-relator pro-p-group with $\mathfrak{z}(G) = p$ and *cd* $G > 2$, then r is congruent to a p-th power modulo $F_{(p+1)}$.

Having developed a criterion for a pro-p-group with trivial cup-product to be mild, the question arises whether such groups occur as arithmetic groups. Let $S = \{l_1, \ldots, l_n, \infty\}$ where the l_i are prime numbers $\equiv 1 \mod 4$ and ∞ denotes the infinite prime of $\mathbb{Q}$. If all Legendre symbols $\left(\frac{l_i}{l_j}\right)_2$ for $i \neq j$ are trivial, the Zassenhaus invariant of the Galois group $G_S(2)$ of the maximal 2-extension of $\mathbb{Q}$ unramified outside S is at least 3. A description of the generating relations modulo the fourth step of the Zassenhaus filtration has been given in [Mor02] and [Vog05]. However, in these cases $G_S(2)$ is never mild, since the real prime becomes complex in $\mathbb{Q}_S(2)$ and hence *cd* $G_S(2) = \infty$.**) Hence, if one wants to obtain arithmetic examples of mild pro-2-groups over $\mathbb{Q}$, the infinite prime has to be removed from S. On the other hand, in order to have a trivial *Kummer group* $V_S(\mathbb{Q})$ (which by [Koc02] is an obstruction for the relations of $G_S(2)$ being generated by *local* relations), one has to add the prime 2 or primes $\equiv 3 \mod 4$ to the set S. If S contains more than one prime $\equiv 3 \mod 4$, then $G_S(2)$ has Zassenhaus invariant $\mathfrak{z}(G_S(2)) = 2$. If S contains only one prime $\equiv 3 \mod 4$, then the relations of $G_S(2)$ satisfy certain symmetries and yield sequences which are not strongly free. Consequently, we have to consider 2-extensions with *wild* ramification (i.e. $2 \in S$) but without ramification at the infinite prime (i.e. $\infty \notin S$).

*) These *Poincaré groups* of dimension 2 are called *Demuškin groups*.

**) In fact, the same holds for any extension of the of the form $G_S(2)$ over an arbitrary number field k if S contains a real prime of k, cf. [Sch02], Th.4.

Vogel and Morishita calculate the triple Massey product of $G_S(2)$ in the tame case using a number theoretical symbol introduced be L. Rédei (cf. [Réd38]). This symbol can be seen as a higher analogue of the Legendre symbol and is defined in terms of the ramification behavior of primes in certain dihedral extensions of $\mathbb{Q}$. We transfer these results to the wild case and give a complete description of the triple Massey product of $G_S(2)$ for $2 \in S, \infty \notin S$. This requires a careful investigation of the question in which cases the dihedral extensions determining the Rédei symbols are totally real. Explicit examples can be calculated using the computational algebra system [MAGMA]. It turns out that one obtains a large supply of mild pro-2-groups having trivial cup-product. As a general result, we prove the following:

Theorem (3.4.12)**.** *Let $S = \{l_0, l_1, \ldots, l_n\}$ for some $n \geq 1$ and prime numbers $l_0 = 2,\ l_i \equiv 9 \mod 16,\ i = 1, \ldots, n$, such that the Legendre symbols satisfy*

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

Then $G_S(2)$ is a mild pro-2-group with generator rank $n+1$, relation rank n and trivial cup-product

$$H^1(G_S(2)) \times H^1(G_S(2)) \overset{\cup}{\to} H^2(G_S(2)).$$

As we have already remarked, in the *tame case* the groups $G_S(p)$ are fab pro-p-groups. Since fab groups are duality groups if their cohomological dimension is equal to 2, we are interested in finding examples of mild fab groups with trivial cup-product. The groups given in the above theorem are clearly not fab, since $\mathbb{Q}_S(2)$ contains the maximal real subfield of the cyclotomic $\mathbb{Z}_2$-extension. However, fab groups occur as Galois groups of the form $G_S^T(2)$ (here we have to assume the Leopoldt conjecture for certain totally real extensions of $\mathbb{Q}$ and the prime 2). We compute the triple Massey product of these groups in the case $\#T = 1$ and using computations with [MAGMA] we construct a fab pro-2 duality group with trivial cup-product:

Example (3.5.4)**.** Let $S = \{2, 17, 7489, 15809\}, T = \{5\}$. Then the group $G_S^T(2)$ is mild and admits a minimal presentation $G = F/R$ where F is the free pro-2-group on $x_1, \ldots, x_3$ and R is generated by r_1, r_2, r_3 as a normal subgroup of F, such that

$$\begin{aligned} r_1 &\equiv [[x_1, x_3], x_1]\,[[x_1, x_3], x_3]\,[[x_2, x_3], x_1] \mod F_{(4)} \\ r_2 &\equiv [[x_1, x_3], x_2] \mod F_{(4)}, \\ r_3 &\equiv [[x_1, x_3], x_1]\,[[x_1, x_3], x_2]\,[[x_2, x_3], x_1] \mod F_{(4)}. \end{aligned}$$

Furthermore, $G_S^T(2)$ is a fab duality group of dimension 2.

One should remark that the existence of fab pro-p-groups is a rather mysterious phenomenon: On the one hand, many finitely presented pro-p-Galois groups can be shown to be fab using arithmetic arguments, since this reduces to the question whether the associated extension contains a $\mathbb{Z}_p$-extension. On

the other hand, so far we do not have an explicit description of a single infinite fab group in terms of generators and relations, i.e. we cannot give an "algebraic" proof of the fab-property (see also [Lab08]). However, such an algebraic criterion could itself provide new insight into arithmetic questions related to $\mathbb{Z}_p$-extensions.

Acknowledgements

First and foremost, I would like to thank my advisor Kay Wingberg most warmly for introducing me to this interesting subject and for his invaluable guidance and support. I would like to express my sincere gratitude for his constant encouragement and the numerous discussions and suggestions that led to considerable improvements of this thesis. I very much appreciate the excellent working conditions.

Many other people deserve my gratitude for their support: I'd like to thank Denis Vogel for lending a sympathetic ear for countless questions and his great MAGMA support. Many thanks go to Alexander Schmidt and John Labute for valuable comments and corrections.

Moreover, I am indebted to Jakob Stix, Johannes Bartels, Kilian Kilger, and Peter Barth for many fruitful discussions. I thank Patrick Forré for proofreading a preliminary version of this thesis and his hospitality during several visits in Regensburg.

Further thanks go to all members of the Heidelberg Mathematical Institute for creating an inspiring working environment as well as for the stimulating non-mathematical discussions during the coffee breaks.

I feel deeply grateful towards my parents for their constant backing and encouragement. Finally, I'd like to thank Julia for her unshakable support and for being around whenever I needed her.

1 Restricted Lie algebras and strongly free sequences

1.1 p-restricted filtrations of pro-p-groups

Let p denote an arbitrary prime number. The following definition is due to M. Lazard, cf. [Laz65].

(1.1.1) Definition. *Let G be a pro-p-group. A decreasing sequence $\omega = (G_n)_{n\in\mathbb{N}}$ of subgroups $G = G_1 \supseteq G_2 \supseteq \dots$ is called* **p-restricted filtration** *of G if*

$$[G_i, G_j] \subseteq G_{i+j}, \quad G_i^p \subseteq G_{pi}$$

for all $i, j \in \mathbb{N}$. The pair (G, ω) will be called **p-filtered group**. *We say that ω is* **separated** *if in addition*

$$\bigcap_{n\in\mathbb{N}} G_n = \{1\}$$

holds.

Let G be a pro-p-group and $\omega = (G_n)_{n\in\mathbb{N}}$ a p-restricted filtration of G. Note that the condition $[G_n, G] \subseteq G_{n+1}$ implies that the G_n are normal subgroups of G. By abuse of notation we denote the function

$$\omega : \ G \longrightarrow \mathbb{N} \cup \{+\infty\},$$

$$x \longmapsto \omega(x) = \sup_{n:\ x\in G_n} n$$

also by ω. For $x, y \in G$ it satisfies the following properties:

(1) $\omega(xy^{-1}) \geq \min(\omega(x), \omega(y))$,

(2) $\omega([x, y]) \geq \omega(x) + \omega(y)$,

(3) $\omega(x^p) \geq p\omega(x)$.

Note that (2) implies $\omega(1) = \infty$. Furthermore, ω is separated if and only if $\omega(x) = \infty$ implies $x = 1$. On the other hand, if $\tilde{\omega} : G \longrightarrow \mathbb{N} \cup \{+\infty\}$ is an arbitrary function satisfying the properties (1)-(3), we can associate to ω a p-restricted filtration of G by setting

$$\tilde{G}_n = \{x \in G \mid \tilde{\omega}(x) \geq n\}.$$

These transformations are inverse to each other, hence the datum (G, ω) where $\omega = (G_n)_{n\in\mathbb{N}}$ is a p-restricted filtration of G is equivalent to specifying a function satisfying the properties (1)-(3) and we will make use of both descriptions concurrently.

(1.1.2) Definition.

(i) *Let (G, ω_G), (H, ω_H) be p-filtered groups. A* **homomorphism of p-filtered groups**

$$f : (G, \omega_G) \longrightarrow (H, \omega_H)$$

is a homomorphism $f : G \longrightarrow H$, such that $\omega_H(f(x)) \geq \omega_G(x)$ for all $x \in G$. Furthermore, we say that f is an **isometry** *if it is injective and $\omega_H(f(x)) = \omega_G(x)$ for all $x \in G$.*

(ii) *Let G be a pro-p-group and $\omega, \tilde{\omega}$ be p-restricted filtrations of G. We say that ω is* **finer** *than $\tilde{\omega}$ if $\omega(x) \leq \tilde{\omega}(x)$ for all $x \in G$, or equivalently, if the identity on G yields a homomorphism of p-filtered groups $(G, \omega) \longrightarrow (G, \tilde{\omega})$.*

(1.1.3) Remarks.

(i) So far we didn't need the assumption that G is a profinite (or even pro-p-) group. The notion of a p-restricted filtration can be defined for any (discrete) group.

(ii) In our applications, the subgroups $G_n \subseteq G$ will be closed (and even open) subgroups of G, but note that in definition (1.1.1) there are no topological conditions involved.

(iii) A more general definition of p-restricted filtrations on G is possible by considering functions ω satisfying the properties (1)-(3) as above but taking values in $\mathbb{R}^{\times}_{>0}$ (cf. [Laz65]). In this context, filtrations as defined in (1.1.1) are called **discrete**.

A well-known example of a p-restricted filtration for a pro-p-group G is the **Zassenhaus filtration**. It is defined via a natural filtration on the complete group algebra $\mathbb{F}_p[\![G]\!]$. In order to deal with a more general class of filtrations later, we start with the following general definition:

(1.1.4) Definition. *Let Ω be a ring with unit. A* **filtration** *ν of Ω is a function $\nu : \Omega \longrightarrow \mathbb{N}_0 \cup \{+\infty\}$ such that for $x, y \in \Omega$ the following holds:*

(1) $\nu(x - y) \geq \min(\nu(x), \nu(y))$,

(2) $\nu(xy) \geq \nu(x) + \nu(y)$,

(3) $\nu(1) = 0$.

If ν is a filtration of Ω, we define two-sided ideals Ω_n by setting

$$\Omega_n = \{x \in \Omega \mid \nu(x) \geq n\}.$$

We have $\Omega_n\Omega_m \subseteq \Omega_{n+m}$ for all $n, m \in \mathbb{N}_0$.

(1.1.5) Lemma. *Let Ω be a ring of characteristic $p > 0$ and ν a filtration of Ω. Furthermore, assume that the pro-p-group $G \subseteq \Omega^\times$ is a subgroup of the multiplicative group of Ω such that $\nu(g-1) > 0$ for all $g \in G$. Then by setting*

$$\omega(g) = \nu(g-1),$$

the pair (G, ω) is a p-filtered group. We say that ω is the **p-restricted filtration of G induced by ν**.

Proof. This follows by straightforward computation using the identity

$$gh - 1 = (g-1)(h-1) + (g-1) + (h-1),\ g, h \in G.$$

□

We now consider the case where Ω is the complete group algebra $\mathbb{F}_p[\![G]\!]$. We quickly recall the following

(1.1.6) Definition. *Let G be a pro-p-group and $\mathcal{O}$ denote a complete commutative local ring. The* **complete group algebra of G over $\mathcal{O}$** *is defined as the projective limit*

$$\mathcal{O}[\![G]\!] := \varprojlim_U \mathcal{O}[G/U]$$

where U runs through the open normal subgroups of G. By $I(G) \subseteq \mathcal{O}[\![G]\!]$ we denote the **augmentation ideal** *of G, i.e. the kernel of the canonical* **augmentation map**

$$\mathcal{O}[\![G]\!] \twoheadrightarrow \mathcal{O}.$$

Note that $I(G)$ is the closed left (right) ideal generated by $g - 1,\ g \in G$.

(1.1.7) Definition. *Let G be a pro-p-group. Let $I^n(G)$ denote the n-th power of the augmentation ideal of the complete group algebra $\mathbb{F}_p[\![G]\!]$ and ν the filtration of $\mathbb{F}_p[\![G]\!]$ given by the descending chain of ideals $(I^n(G))_{n\in\mathbb{N}_0}$, i.e.*

$$\nu(x) = \sup_{n:\ x \in I^n(G)} n.$$

The filtration $\omega = (G_{(n)})_{n\in\mathbb{N}}$ of G induced by ν is called the **Zassenhaus filtration of G**, *i.e.*

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

If G is finitely generated, then $G_{(n)}$ is an open subgroup of G for any $n \in \mathbb{N}$.

(1.1.8) Proposition. *If G is a finitely generated pro-p-group, the subgroups $G_{(n)}$ are open and form a neighbourhood basis for $1 \in G$. In particular, the Zassenhaus filtration is separated.*

Proof. See [Koc02], Th.7.11. The proof uses the fact that the powers $I^n(G)$ form a neighbourhood basis for $0 \in \mathbb{F}_p[\![G]\!]$. We will also obtain a more general statement for free pro-p-groups in (1.3.4). □

By the following theorem of Jennings, one can give a handy recursive description of the groups $G_{(n)}$. For a proof using the theory of restricted Lie algebras (which we will define in section (1.2)), we refer to [DdSMS99], Th.12.9.

(1.1.9) Theorem. *The subgroups $G_{(n)}$ can be described recursively by the formula*

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

where $\lceil n/p \rceil$ denotes the least integer $\geq n/p$.[*)]

As an immediate consequence of Jennings' theorem, we see that the Zassenhaus filtration is the finest p-restricted filtration of G by closed subgroups $G_{(n)}$.

Another class of filtrations frequently occuring in the theory of pro-p-groups is given by the **descending q-central series** $(G^{(n,q)})_{n\in\mathbb{N}}$. If G is a pro-p-group and q is a power of p, the subgroups $G^{(n,q)} \subseteq G$ are recursively defined by

$$G^{(1,q)} = G,\ G^{(n+1,q)} = (G^{(n,q)})^q [G^{(n,q)}, G],\ n \geq 1.$$

For $q = p$ we set $G^{(n)} = G^{(n,p)}$. Furthermore we denote by $(G_n)_{n\in\mathbb{N}}$ the usual **descending central series** of G defined by

$$G_1 = G,\ G_{n+1} = [G_n, G],\ n \geq 1.$$

Clearly, the descending p-central series is a subfiltration of the Zassenhaus filtration. By (1.1.9), we obtain more precisely the following

(1.1.10) Corollary. *For $n \geq 1$ we have*

$$G^{(n)} \subseteq G_{(n)}.$$

Equality holds if

(i) $n \leq 2$ *or*

(ii) $p = 2,\ n = 3$.

Finally we'd like to state a theorem due to Lazard giving an explicit description of the Zassenhaus filtration in terms of the descending central series. For a proof see [DdSMS99], Th.11.2.

(1.1.11) Theorem. *For $n \geq 1$, we have*

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

[*)] By definition, the groups $G^p_{(i)}$ and $[G_{(i)}, G_{(j)}]$ are the *closed* subgroups generated by p-th powers $x^p,\ x \in G^p_{(i)}$ and commutators $[x, y],\ x \in G_{(i)}, y \in G_{(j)}$ respectively.

Although the descending p-central series has many nice properties, for some purposes the Zassenhaus filtration may appear to be more natural and convient. For instance, it occurs in the proof (and formulation) of the (generalized) Golod-Šafarevič inequality (cf. [NSW08], Th.3.9.7 and the following remarks) and in the study of Massey products, which we will introduce in the next chapter. Therefore - with a view towards our applications - we will focus on these filtrations and the corresponding restricted Lie algebras when introducing the notion of **mild** pro-p-groups. Analogous definitions exist for the descending p-central series and the corresponding (mixed) Lie algebras, cf. [Lab06] or [LM11].

Now we come back to arbitrary p-restricted filtrations. As usual, we define the associated graded objects:

(1.1.12) Definition. *Let G be a pro-p-group and $\omega = (G_n)_{n\in\mathbb{N}}$ a p-restricted filtration of G.*

(i) *For any $i \geq 1$ we set*
$$\mathrm{gr}_i^\omega(G) = G_i/G_{i+1}.$$
In a natural way, these quotients are $\mathbb{F}_p$-vector spaces. Furthermore, we set
$$\mathrm{gr}^\omega(G) = \bigoplus_{i\geq 1} \mathrm{gr}_i^\omega(G)$$

(ii) *The maps $G \times G \longrightarrow G,\ (x,y) \longmapsto [x,y]$ and $G \longrightarrow G,\ x \longmapsto x^p$ induce well-defined maps*
$$\begin{aligned} [\cdot,\cdot] : \mathrm{gr}_i^\omega(G) \times \mathrm{gr}_j^\omega(G) &\longrightarrow \mathrm{gr}_{i+j}^\omega(G), \\ {}^{[p]} : \mathrm{gr}_i^\omega(G) &\longrightarrow \mathrm{gr}_{pi}^\omega(G). \end{aligned}$$
Furthermore, we extend these maps lineraly to $[\cdot,\cdot] : \mathrm{gr}^\omega(G) \times \mathrm{gr}^\omega(G) \longrightarrow \mathrm{gr}^\omega(G)$ and ${}^{[p]} : \mathrm{gr}^\omega(G) \longrightarrow \mathrm{gr}^\omega(G)$ respectively.

(iii) *If ω is the Zassenhaus filtration, we set $\mathrm{gr}_i(G) = \mathrm{gr}_i^\omega(G)$ and $\mathrm{gr}(G) = \mathrm{gr}^\omega(G)$.*

(1.1.13) Remarks.

(i) It is easily checked that $[\cdot,\cdot] : \mathrm{gr}^\omega(G) \times \mathrm{gr}^\omega(G) \longrightarrow \mathrm{gr}^\omega(G)$ is $\mathbb{F}_p$-bilinear and endowes $\mathrm{gr}^\omega(G)$ with a Lie algebra structure over $\mathbb{F}_p$. As we will see in the next section, together with the map ${}^{[p]}$ (which is not $\mathbb{F}_p$-linear in general), $\mathrm{gr}^\omega(G)$ is a **restricted Lie algebra** over $\mathbb{F}_p$.

(ii) In the situation of (1.1.5), the filtration ν of Ω also gives rise to a graded $\mathbb{F}_p$-vector space $\mathrm{gr}^\nu\,\Omega$ (or more precisely a graded restricted Lie algebra over $\mathbb{F}_p$) and the injective map $G \hookrightarrow \Omega,\ g \longmapsto g-1$ induces an inclusion
$$\mathrm{gr}^\omega\, G \hookrightarrow \mathrm{gr}^\nu\,\Omega,$$
cf. [Laz65], App.2.

1.2 Restricted Lie algebras

If $(G_n)_{n\in\mathbb{N}}$ is a p-restricted filtration of a pro-p-group G, we are interested in the associated graded object

$$\mathrm{gr}(G) = \bigoplus_{n\geq 1} G_n/G_{n+1},$$

which is a **restricted Lie algebra** over $\mathbb{F}_p$ in the sense of Jacobson, cf. [Jac62].

Unless stated otherwise, if L is a Lie algebra (over an arbitrary commutative ring), we denote by $[\cdot,\cdot] : L \times L \longrightarrow L$ its Lie bracket and for $x \in L$ by $\mathrm{ad}(x) : L \longrightarrow L,\ y \longmapsto [x,y]$ the adjoint endomorphism. Throughout this section, let k denote a field of characteristic $p > 0$.*)

(1.2.1) Definition. *A* **restricted Lie algebra** *over k is a Lie algebra L over k together with a mapping*

$$(\cdot)^{[p]} :\ L \longrightarrow L,$$

$$a \longmapsto a^{[p]}$$

satisfying the following properties:

(i) $(\alpha a)^{[p]} = \alpha^p a^{[p]},\ \alpha \in k,\ a \in L,$

(ii) $(a+b)^{[p]} = a^{[p]} + b^{[p]} + \sum_{i=1}^{p-1} s_i(a,b)/i,\ a,b \in L$ *where $s_i(a,b)$ denotes the coefficient of λ^{i-1} in the formal expression* $\mathrm{ad}(\lambda a + b)^{p-1}(a)$,

(iii) $\mathrm{ad}(a^{[p]}) = \mathrm{ad}(a)^p,\ a \in L.$

An **ideal** $\mathfrak{r}$ of a restricted Lie algebra L is an ideal of the underlying Lie algebra of L which is also closed under $(\cdot)^{[p]}$. In a natural way the quotient $L/\mathfrak{r}$ is again a restricted Lie algebra over k. A **homomorphism of restricted Lie algebras** is a homomorphism of Lie algebras that commutes with the additional $(\cdot)^{[p]}$-maps. In order to avoid confusion, we make the following notational convention: By $\mathcal{F}_{res}$ we denote the **forgetful functor**

$$\mathcal{F}_{res} :\ \{\text{restricted Lie algebras over } k\} \longrightarrow \{\text{Lie algebras over } k\}.$$

(1.2.2) Example. If A is an associative k-algebra, then A can be considered as restricted Lie algebra over k setting

$$[a,b] = ab - ba, \quad a^{[p]} = a^p$$

for $a, b \in A$.**)

*) In our later applications, we will only have to deal with the case $k = \mathbb{F}_p$.

**) This standard example makes clear why condition (ii) in (1.2.1), which might look rather technical at first sight, is the natural one.

More precisely, the construction made in the example yields a covariant functor

$$\mathcal{L}_{res}: \{\text{algebras over } k\} \longrightarrow \{\text{restricted Lie algebras over } k\}.$$

Furthermore, by $\mathcal{L}$ we denote the natural functor

$$\mathcal{L}: \{\text{algebras over } k\} \longrightarrow \{\text{Lie algebras over } k\},$$

sending a k-algebra A to the Lie algebra $\mathcal{L}(A)$ having A as underlying k-vector space and Lie bracket $[a,b] = ab - ba$. Obviously $\mathcal{L} = \mathcal{F}_{res} \circ \mathcal{L}_{res}$. Similar to $\mathcal{L}$, the functor $\mathcal{L}_{res}$ also has a left adjoint functor

$$\mathcal{U}_{res}: \{\text{restricted Lie algebras over } k\} \longrightarrow \{\text{algebras over } k\},$$

given by the so-called **(restricted) universal enveloping algebra**:

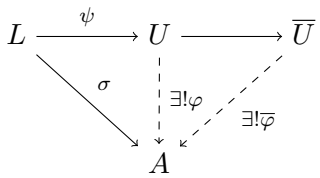
(1.2.3) Definition. *Let L be a restricted Lie algebra over k. An (associative) algebra $\mathcal{U}_{res}(L)$ over k together with a homomorphism of restricted Lie algebras $\psi_L : L \longrightarrow \mathcal{L}_{res}(\mathcal{U}_{res}(L))$ is called* **universal enveloping algebra** *of L, if for every algebra A over k the map*

$$\begin{aligned} \mathrm{Hom}(\mathcal{U}_{res}(L), A) &\xrightarrow{\sim} \mathrm{Hom}(L, \mathcal{L}_{res}(A)) \\ \phi &\longmapsto \phi \circ \psi_L, \end{aligned}$$

where $\mathrm{Hom}(\mathcal{U}_{res}(L), \cdot)$ and $\mathrm{Hom}(L, \cdot)$ denote morphisms in the categories of algebras and restricted Lie algebras over k respectively, is an isomorphism.

(1.2.4) Proposition. *For every restricted Lie algebra L over k, there exists a universal enveloping algebra $\mathcal{U}_{res}(L)$, which is unique up to isomorphism.*

Proof. See also [Jac62], Ch.V, Th.12. The uniqueness follows immediately from the universal property. To construct $\mathcal{U}_{res}(L)$, denote by U the universal enveloping algebra of the Lie algebra $\mathcal{F}_{res}(L)$ and let ψ be the canonical morphism $\psi : \mathcal{F}_{res}(L) \longrightarrow \mathcal{L}(U)$. Let $I \subseteq U$ be the two-sided ideal generated by $\psi(a)^p - \psi(a^{[p]})$, $a \in \mathcal{F}_{res}(L)$ and $\overline{U} = U/I$. Now let A be a k-algebra and $\sigma : L \longrightarrow \mathcal{L}_{res}(A)$ a homomorphism of restricted Lie algebras. By the universal property of U, σ factors over U via a unique homomorphism $\phi : U \to A$. We have $I \subseteq \ker \varphi$ and therefore we get the commutative diagram



of Lie algebras where we have identified L with $\mathcal{F}_{res}(L)$ etc. Noting that the map $L \xrightarrow{\psi} U \longrightarrow \overline{U}$ is even a homomorphism of *restricted* Lie algebras, $\overline{U}$ satisfies the desired universal property. □

The above proof shows that we have the commutative diagram

$$\begin{array}{ccc} \mathcal{F}_{res}(L) & \xrightarrow{\psi_L} & \mathcal{L}(\mathcal{U}_{res}(L)) \\ & \searrow & \uparrow \\ & & \mathcal{L}(U) \end{array}$$

of Lie algebra homomorphisms. Note that since k is a field, $\mathcal{F}_{res}(L)$ is free as k-module and by the **Poincaré-Birkhoff-Witt theorem** it follows that the natural map from $\mathcal{F}_{res}(L)$ to its universal enveloping algebra U is injective. For the universal enveloping algebras of restricted Lie algebras we have the following analogue, stating that the map ψ_L in the above diagram is also an injection. For a proof see [Jac62], Ch.V, Th.12.

(1.2.5) Proposition. *Let L be a restricted Lie algebra over k. Then L is embedded into its universal enveloping algebra, i.e. the homomorphism of restricted Lie algebras*

$$\psi_L : \ L \hookrightarrow \mathcal{L}_{res}(\mathcal{U}_{res}(L))$$

is injective.

Furthermore, we will need the following fact: If L' is a quotient of the restricted Lie algebra L, then $\mathcal{U}_{res}(L')$ is a quotient of $\mathcal{U}_{res}(L)$ in a natural way. This is exactly the statement of the following

(1.2.6) Proposition. *Let L be a restricted Lie algebra over k and let $\mathfrak{r} \subseteq L$ be an ideal. Let $\mathfrak{R}$ denote the left ideal of $\mathcal{U}_{res}(L)$ generated by the image of $\mathfrak{r}$ under the embedding $\psi_L : L \hookrightarrow \mathcal{L}_{res}(\mathcal{U}_{res}(L))$. Then $\mathfrak{R}$ is a two-sided ideal and the canonical surjection $L \twoheadrightarrow L/\mathfrak{r}$ induces an exact sequence*

$$0 \longrightarrow \mathfrak{R} \longrightarrow \mathcal{U}_{res}(L) \longrightarrow \mathcal{U}_{res}(L/\mathfrak{r}) \longrightarrow 0.$$

Proof. For the analogous statement for (ordinary) Lie algebras, see [Bou75], Ch.I, §1.3, Th.1. Since the universal enveloping algebra of a restricted Lie algebra satisfy the analogous universal property as for an (ordinary) Lie algebra, the proof carries over. □

After having established the basic properties of universal enveloping algebras for restricted Lie algebras, in the following it will always be clear from the context which category is considered. Therefore, we make the following notational convention: We omit the functors $\mathcal{F}_{res}, \mathcal{L}, \mathcal{L}_{res}$ and for the sake of brevity we set

$$U_L := \mathcal{U}_{res}(L)$$

for any restricted Lie algebra L over k.

We are particularly interested in the structure of *free* restricted Lie algebras which are defined via the usual universal property. We can construct them as

follows: Let X be a set and $k\langle X\rangle$ be the free associative algebra on X over k with free generating set X. Let L be the restricted subalgebra of $\mathcal{L}_{res}(k\langle X\rangle)$ generated by X. Then L is the **free restricted Lie algebra** with free generating set X over k, denoted by $L_{res}(X)$.

(1.2.7) Proposition. *Let $L_{res}(X)$ be the free restricted Lie algebra on X over k and $\psi : L_{res}(X) \hookrightarrow k\langle X\rangle$ the embedding into the free associative algebra on X over k. Then $k\langle X\rangle$ is the restricted universal enveloping algebra of $L_{res}(X)$ via ψ.*

Proof. This is an immediate consequence from the construction of the universal enveloping algebra $U_{L_{res}(X)}$ as given in the proof of (1.2.4). □

In the following, we consider $L_{res}(X)$ as a restricted Lie subalgebra of $\mathcal{L}_{res}(k\langle X\rangle)$. Moreover, by $L(X)$ we denote the free Lie algebra on X over k, which is a Lie subalgebra of $\mathcal{L}(k\langle X\rangle)$, i.e. we have inclusions

$$L(X) \subseteq L_{res}(X) \subseteq k\langle X\rangle$$

and via these inclusions $k\langle X\rangle$ is the universal enveloping algebra for both $L(X)$ and $L_{res}(X)$. We say that $f \in k\langle X\rangle$ is **of Lie type** or **of restricted Lie type**, if $f \in L(X)$ or $f \in L_{res}(X)$ respectively. Elements of restricted Lie type are characterized by the following

(1.2.8) Theorem. *Let X be a non-empty set. By δ we denote the homomorphism of k-algebras defined by*

$$\delta : \ k\langle X\rangle \longrightarrow k\langle X\rangle \otimes_k k\langle X\rangle,$$

$$x \longmapsto x \otimes 1 + 1 \otimes x, \ x \in X.$$

For $f \in k\langle X\rangle$ the following statements are equivalent:

(i) *f is of restricted Lie type.*

(ii) $\delta(f) = f \otimes 1 + 1 \otimes f$.

Furthermore, let Ad *be the homomorphism of k-algebras given by*

$$\mathrm{Ad} : \ k\langle X\rangle \longrightarrow \mathrm{End}(k\langle X\rangle),$$

$$x \longmapsto \mathrm{ad}(x) = (y \mapsto xy - yx), \ x \in X.$$

If $\#X \geq 2$, then (i) *and* (ii) *are equivalent to*

(iii) *The constant term of f is zero and* $\mathrm{ad}(f) = \mathrm{Ad}(f)$.

For a proof see [Reu93], Th.1.4 and the remarks at the end of section 2.5.2.

For the sake of simplicity and with a view towards our applications, we will now assume that $X = \{X_1, \ldots, X_d\}$ is finite. In a natural way, $k\langle X\rangle = \bigoplus_{n\geq 0} k\langle X\rangle_n$ is a graded k-algebra via the usual degree function. In order to give explicit k-bases for the subspaces $L(X)_n \subset L(X)$ and $L_{res}(X)_n \subset L_{res}(X)$ of homogeneous elements of degree n, we recall the notion of the set of **Hall commutators**.

(1.2.9) Definition. *The set $C_n \subseteq L(X)$ of* **Hall commutators of weight n** *together with a total order $<$ is inductively defined as follows:*

(i) *$C_1 = \{X_1, \ldots, X_d\}$ with the ordering $X_1 > \ldots > X_d$.*

(ii) *C_n is the set of all commutators $[c_1, c_2]$ where $c_1 \in C_{n_1}$, $c_2 \in C_{n_2}$ such that $n_1 + n_2 = n$, $c_1 > c_2$ and if $n_1 \neq 1$, $c_1 = [c_3, c_4]$ we have $c_2 \geq c_4$. The set C_n is ordered 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 $c_2 < c_2'$. Finally for $c \in C_n$ we set $d < c$ for any $d \in C_i$, $i < n$.*

We set $\mathcal{C} = \bigcup_{n\in\mathbb{N}} C_n$.

(1.2.10) Example. For weights ≤ 3 the Hall commutators are given by

$$\begin{aligned} C_1 &= \{X_i \mid 1 \leq i \leq d\} && (\#C_1 = d),\\ C_2 &= \{[X_i, X_j] \mid 1 \leq i < j \leq d\} && (\#C_2 = \tbinom{d}{2}),\\ C_3 &= \{[[X_i, X_j], X_k] \mid 1 \leq i < j \leq d, k \leq j\} && (\#C_3 = 2\tbinom{d+1}{3}). \end{aligned}$$

Obviously the Hall commutators of weight k are homogeneous polynomials (of Lie type) of degree k (with respect to the natural grading). Their importance lies in the following

(1.2.11) Theorem. *Let $L(X)$ and $L_{res}(X)$ be endowed with the natural grading.*

(i) *The sets C_n are k-vector space bases of $L(X)_n$. In particular, $\mathcal{C} = \bigcup_{n\in\mathbb{N}} \mathcal{C}_n$ is a k-basis of $L(X)$.*

(ii) *The sets*

$$\overline{C}_n = \dot{\bigcup}_{ip^j=n} (C_i)^{p^j}$$

are k-bases of $L_{res}(X)_n$. In particular, $\overline{\mathcal{C}} = \bigcup_{n\in\mathbb{N}} \overline{C}_n$ is a k-basis of $L_{res}(X)$.

Proof. The fact that $\mathcal{C}$ is a k-basis of $L(X)$ is well-known, cf. [Bou75], Ch.II, §2.11, Th.1 or [Reu93], Th.4.9 (i). The bases for the subspaces $L(X)_n$ are easily obtained by comparing degrees. Now we show (ii): Let $L \subseteq k\langle X\rangle$ denote the k-span of $\overline{\mathcal{C}}$. Taking into account that the sets C_n generate $L(X)$ and using the identity (iii) in (1.2.1), it follows that L is closed under taking commutators and p-th powers, i.e. L is a restricted Lie subalgebra of $\mathcal{L}_{res}(k\langle X\rangle)$ containing

X and therefore $L_{res}(X) \subseteq L$. On the other hand, we clearly have $L \subseteq L_{res}(X)$ and hence equality holds. It remains to show that $\overline{\mathcal{C}}$ is linearly independent. This follows as a direct consequence of the *Poincaré-Birkhoff-Witt theorem*, cf. [Bou75], Ch.I, §2.7, Cor.3, stating that the set of all elements of the form

$$c_{i_1} c_{i_2} \cdots c_{i_k}$$

where $c_{i_j} \in \mathcal{C},\ c_{i_1} \leq \ldots \leq c_{i_k}$ is a k-basis of the enveloping algebra $k\langle X\rangle$. In particular, the union $\overline{C}_n = \dot{\bigcup}_{ip^j=n}(C_i)^{p^j}$ is indeed disjoint. Now again the statement for $L_{res}(X)_n$ follows immediately. □

Using weights we define a general class of gradings:

(1.2.12) Definition. *Let $\tau = (\tau_1, \ldots, \tau_d)$ be a sequence of integers $\tau_i > 0$. For a monomial $X_{i_1} \cdots X_{i_d}$ we set*

$$\deg_\tau(X_{i_1} \cdots X_{i_k}) = \tau_{i_1} + \ldots + \tau_{i_k}.$$

We define the **(X, τ)-grading** *on $k\langle X\rangle$ by*

$$k\langle X\rangle = \bigoplus_{n\geq 0} k\langle X\rangle_n^\tau$$

where $k\langle X\rangle_n^\tau$ denotes the k-subspace generated by all monomials f satisfying $\deg_\tau(f) = n$. By (1.2.11)*, both $L(X)$ and $L_{res}(X)$ possess k-bases of (x,τ)-homogeneous polynomials, hence the grading on $k\langle X\rangle$ induces gradings on $L(X)$ and $L_{res}(X)$*

$$L(X) = \bigoplus_{n\geq 0} L(X)_n^\tau, \quad L_{res}(X) = \bigoplus_{n\geq 0} L_{res}(X)_n^\tau.$$

This makes $L(X)$ a **graded Lie algebra***, i.e. $[L(X)_i^\tau, L(X)_j^\tau] \subseteq L(X)_{i+j}^\tau$ and $L_{res}(X)$ a* **graded restricted Lie algebra***, i.e. $[L_{res}(X)_i^\tau, L_{res}(X)_j^\tau] \subseteq L_{res}(X)_{i+j}^\tau$ and $(L_{res}(X)_i^\tau)^p \subseteq L_{res}(X)_{pi}^\tau$. We call the above grading the* **(X, τ)-grading** *of $L(X)$ and $L_{res}(X)$ respectively. The (X,τ)-grading where $\tau_i = 1$ for all $i = 1, \ldots, d$ will also be called* **natural grading**.

(1.2.13) Remark. Noting that the Hall commutators are homogeneous with respect to the (X,τ)-grading for any τ, we deduce that the set

$$\overline{C}_n^\tau = \{c \in \overline{\mathcal{C}} \mid c \in L_{res}(X)_n^\tau\} \subseteq \overline{\mathcal{C}}$$

is a $\mathbb{F}_p$-basis for $L_{res}(X)_n$ for all $n \in \mathbb{N}$.

Now we come back to p-restricted filtrations of pro-p-groups. As already remarked, they are closely linked to restricted Lie algebras by the following

(1.2.14) Proposition.

(i) *Let (G,ω) be a p-filtered group. Via the maps*

$$[\cdot,\cdot] : \mathrm{gr}^\omega(G) \times \mathrm{gr}^\omega(G) \longrightarrow \mathrm{gr}^\omega(G), \quad {}^{[p]} : \mathrm{gr}^\omega(G) \longrightarrow \mathrm{gr}^\omega(G),$$

defined as in (1.1.12)*, $\mathrm{gr}^\omega(G)$ is a restricted Lie algebra over $\mathbb{F}_p$.*

(ii) *Let $f : G \longrightarrow H$ be a homomorphism of p-filtered groups (G, ω_G), (H, ω_H). Then f induces a canonical homomorphism of restricted Lie algebras*

$$\mathrm{gr}(f) : \mathrm{gr}^{\omega_G}(G) \longrightarrow \mathrm{gr}^{\omega_H}(H).$$

Proof. This is straightforward. See [Laz65], App.2, Th.2.3 and Cor.2.4. □

1.3 Zassenhaus (x, τ)-filtrations of free pro-p-groups

If F is a finitely generated free pro-p-group, the complete group algebra $\mathbb{F}_p[\![F]\!]$ can be described in terms of formal power series over $\mathbb{F}_p$. This identification allows us to define a more general class of p-restricted filtrations. For $X = \{X_1, \ldots, X_d\}$, by $\mathbb{F}_p\langle\langle X\rangle\rangle = \mathbb{F}_p\langle\langle X_1, \ldots, X_d\rangle\rangle$ we denote the **Magnus algebra** on X over $\mathbb{F}_p$, i.e. the algebra of formal power series in the non-commuting indeterminates $X_1, \ldots, X_d$ over $\mathbb{F}_p$. It is endowed by the natural **degree** valuation

$$\deg\Big(\sum_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} X_{i_1} \cdots X_{i_k}\Big) = \inf_{\substack{i_1,\ldots,i_k \\ a_{i_1,\ldots,i_k} \neq 0}} (k),$$

making it a compact topological $\mathbb{F}_p$-algebra.

(1.3.1) Proposition. *Let F be the free pro-p-group over $x = \{x_1, \ldots, x_d\}$. Furthermore, set $X = \{X_1, \ldots, X_d\}$. Then we have a topological isomorphism*

$$\mathbb{F}_p[\![F]\!] \xrightarrow{\sim} \mathbb{F}_p\langle\langle X\rangle\rangle,$$

$$x_i \longmapsto 1 + X_i,$$

mapping the augmentation ideal $I(F)$ onto the (two-sided) ideal

$$I(X) = \langle X_1, \ldots, X_d\rangle = \bigoplus_{i=1}^{d} \mathbb{F}_p\langle\langle X\rangle\rangle \cdot X_i.$$

Proof. Clearly, assigning to $x_i \in \mathbb{F}_p[\![F]\!]$ the element $1 + X_i \in \mathbb{F}_p\langle\langle X\rangle\rangle$ extends to a homomorphism $\psi : \mathbb{F}_p[\![F]\!] \longrightarrow \mathbb{F}_p\langle\langle X\rangle\rangle$ with inverse given by $X_i \longmapsto x_i - 1$, mapping $I(F)$ onto $I(X)$. Therefore, both ψ and its inverse are continuous, since the powers of $I(F)$ and $I(X)$ form full systems of neighbourhoods of the zero elements in $\mathbb{F}_p[\![F]\!]$ and $\mathbb{F}_p\langle\langle X\rangle\rangle$ respectively (cf. also [Laz54], Ch.I, Th.6.11). □

We keep the notation of the above proposition, i.e. F denotes the free pro-p-group on $x = \{x_1, \ldots, x_d\}$ and $X = \{X_1, \ldots, X_d\}$. Furthermore, we set $\overline{A} = \mathbb{F}_p\langle\langle X\rangle\rangle$. By assigning different weights to the variables X_i, we define a more general class of valuations on $\overline{A}$ inducing various p-restricted filtrations on F.

(1.3.2) Definition. *Let $\tau = (\tau_1, \ldots, \tau_d)$ be a sequence of integers $\tau_i > 0$. We define the filtration ν_τ of $\overline{A}$ by*

$$\nu_\tau\Big(\sum_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} X_{i_1}\cdots X_{i_k}\Big) = \inf_{\substack{i_1,\ldots,i_k \\ a_{i_1,\ldots,i_k}\neq 0}} (\tau_{i_1}+\ldots+\tau_{i_k})$$

and set $\overline{A}_{\tau,n} = \{h \in \overline{A} \mid \nu_\tau(h) \geq n\},\ n \geq 0$. The p-restricted filtration $\omega_\tau = (F_{(\tau,n)})_{n\geq 1}$ of F induced by ν_τ, i.e. the filtration given by the normal open subgroups

$$F_{(\tau,n)} = \{f \in F | f-1 \in \overline{A}_{\tau,n}\},\ n \geq 1$$

where we make the identification $\mathbb{F}_p[\![F]\!] \cong \overline{A}$ as in (1.3.1)*, is called* **Zassenhaus (x,τ)-filtration** *of F.*[*)] *We write $\mathrm{gr}_i^\tau(F)$ and $\mathrm{gr}^\tau(F)$ for the associated graded objects.*

Note that if $\tau_i = 1$ for all i, then $F_{(\tau,n)} = F_{(n)}$ is just the usual Zassenhaus filtration. Since

$$\bigcap_{n\in\mathbb{N}} \overline{A}_{\tau,n} = \{0\},$$

the filtration ω^τ is separated.

(1.3.3) Lemma. *With the notations of* (1.3.2)*, let the graded $\mathbb{F}_p$-algebra $\mathrm{gr}^\tau \overline{A}$ be defined as*

$$\mathrm{gr}^\tau \overline{A} = \bigoplus_{n\geq 0} \mathrm{gr}_n^\tau \overline{A} \text{ where } \mathrm{gr}_n^\tau = \overline{A}_{\tau,n}/\overline{A}_{\tau,n+1},\ n \geq 0.$$

By $\xi_i \in \mathrm{gr}_{\tau_i}^\tau \overline{A}$ we denote the initial forms of $X_i,\ i = 1,\ldots,d$. Then there is an isomorphism of graded $\mathbb{F}_p$-algebras

$$\mathrm{gr}^\tau \overline{A} \xrightarrow{\sim} \mathbb{F}_p\langle X\rangle$$

$$\xi_i \longmapsto X_i,$$

where $\mathbb{F}_p\langle X\rangle$ is endowed with the **(X,τ)-grading**, *associating to X_i the degree τ_i.*

Proof. This is obvious. □

(1.3.4) Proposition. *Making the identifications $\mathbb{F}_p[\![F]\!] \cong \overline{A},\ \mathrm{gr}^\tau \overline{A} \cong \mathbb{F}_p\langle X\rangle$, the map $F \hookrightarrow \overline{A}$ induces an embedding*

$$\mathrm{gr}^\tau(F) \hookrightarrow \mathbb{F}_p\langle X\rangle$$

of graded restricted Lie algebras. In particular, the $\mathbb{F}_p$-vector spaces $\mathrm{gr}_i^\tau(F)$ are of finite dimension. It follows that the subgroups $F_{\tau,i}$ are of finite index and hence open in F and form a neighbourhood basis at $1 \in F$.

[*)] It is not hard to see that these subgroups are closed. The fact that they are of finite index will be shown in (1.3.4).

Proof. By (1.1.13) (ii), we get a canonical embedding of $\mathrm{gr}^\tau(F)$ into the graded $\mathbb{F}_p$-algebra $\mathrm{gr}^\tau \overline{A} \cong \mathbb{F}_p\langle X\rangle$. By (1.2.14), $\mathrm{gr}(F)$ is a restricted Lie algebra over $\mathbb{F}_p$ in a natural way and one checks immediately that the above embedding is a homomorphism of restricted Lie algebras. □

As the central result of this section, we will show that under the above embedding $\mathrm{gr}^\tau(F)$ identifies with the free restricted Lie algebra $L_{res}(X)$ over X. This amounts to proving that $\mathrm{gr}^\tau(F)$ is generated by the initial forms of $x_1, \ldots, x_d$. This fact might seem obvious at first sight, but its proof requires some preliminary work. We start by giving a simple equivalent characterization of the Zassenhaus (X, τ)-filtration. Throughout the rest of this section F denotes the free pro-p-group over $x = \{x_1, \ldots, x_d\}$ endowed with the Zassenhaus (x, τ)-filtration for some fixed $\tau = (\tau_1, \ldots, \tau_d)$.

(1.3.5) Lemma. *The Zassenhaus (x, τ)-filtration ω_τ of F is the finest among all p-restricted filtrations ω satisfying the following two properties:*

(i) $\omega(x_i) \geq \tau_i,\ i = 1, \ldots, d.$

(ii) *The subgroups $\{y \in F \mid \omega(y) \geq n\}$ are closed.*

Proof. We keep the notation as in (1.3.2). It is not hard to see that the filtration ν_τ is the finest filtration of $\overline{A}$ in the sense of (1.1.4) satisfying $\nu_\tau(X_i) \geq \tau_i,\ i = 1, \ldots d$. Now suppose that ω is an arbitrary p-restricted filtration of G satisfying the conditions (i) and (ii). We have to show that ω_τ is finer than ω. To this end we define ν to be the finest filtration of $\overline{A}$ satisfying $\nu(f-1) \geq \omega(f)$ for all $f \in F$, i.e. ν is given by

$$\nu(a) = \inf_{\nu'}(\nu'(a)),\ a \in \overline{A}$$

where ν' runs over all filtrations of $\overline{A}$ satisfying $\nu(f-1) \geq \omega(f),\ f \in F$. By (1.1.5), ν induces itself a filtration $\tilde{\omega}$ on F. We have

$$\tilde{\omega}(f) = \nu(f-1) \geq \omega(f),\ f \in F$$

i.e. ω is finer than $\tilde{\omega}$ and we have a homomorphism of restricted Lie algebras

$$\mathrm{gr}(f) : \mathrm{gr}^\omega F \longrightarrow \mathrm{gr}^{\tilde{\omega}} F$$

induced by the identity on F. We claim that $\omega = \tilde{\omega}$. In fact, by (1.1.13), we have the inclusion (of restricted Lie algebras) $\mathrm{gr}^{\tilde{\omega}} F \hookrightarrow \mathrm{gr}^\nu \overline{A}$. Considering the induced homomorphisms on the universal enveloping algebras we obtain the commutative diagram

$$\begin{array}{ccccc}
\mathrm{gr}^\omega F & \xrightarrow{\mathrm{gr}(f)} & \mathrm{gr}^{\tilde{\omega}} F & & \\
\downarrow & & \downarrow & & \\
U_{\mathrm{gr}^\omega F} & \longrightarrow & U_{\mathrm{gr}^{\tilde{\omega}} F} & \longrightarrow & U_{\mathrm{gr}^\nu \overline{A}} \\
 & \searrow & & \nearrow_{\psi} &
\end{array}$$

where the vertical arrows are injective by (1.2.5). By [Laz65], App.2, Th.2.6, the composition ψ of the lower horizontal maps is an isomorphism.*) It follows that $\mathrm{gr}(f)$ is injective which implies that $\tilde{\omega}$ is finer than ω and hence $\omega = \tilde{\omega}$. Now it is not hard anymore to complete the proof: Since $\nu(X_i) \geq \omega(x_i) \geq \tau_i$ for all $i = 1, \ldots, d$, it follows that ν_τ is finer than ν and hence the same holds for the induced filtrations on F, i.e. ω_τ is finer than $\tilde{\omega} = \omega$. □

For the next two statements we closely follow the proofs of [Laz65], Ch.II, Lemma 3.3.1 and Prop.3.3.2 respectively, where analogous results are treated in the case of so-called (x, τ, p)-filtrations, which generalize the descending p-central series.

(1.3.6) Lemma. *Fix some natural number $n \in \mathbb{N}$. Let G be the closed subgroup of F generated by the following elements:*

(i) *The subset of all generators x_i where $\omega^\tau(x_i) = \tau_i > n$.*

(ii) *The p-th powers y^p such that $p\omega^\tau(y) > n$.*

(iii) *The commutators $[y, z]$ where $\omega^\tau(y) + \omega^\tau(z) > n$.*

Then $G = F_{(\tau, n+1)}$.

Proof. Clearly, we have the inclusion $G \subseteq F_{(\tau,n+1)}$. Now we define a family $(F_i)_{i \in \mathbb{N}}$ of subgroups of F by setting

$$F_i = \begin{cases} F_{(\tau,i)}, & \text{if } i \leq n, \\ F_{(\tau,i)} \cap G, & \text{if } i > n. \end{cases}$$

Using the definition of G one checks immediately that $[F_i, F_j] \subseteq F_{i+j}$ and $F_i^p \subseteq F_{pi}$, i.e. these subgroups define a p-restricted filtration of F which we denote by ω. Furthermore, the F_i are closed and we have $\omega(x_i) \geq \tau_i$ for all $i = 1, \ldots, d$. Now (1.3.5) applies and it follows that ω^τ is finer than ω and therefore $F_i = F_{(\tau,i)}$ for all $i \in \mathbb{N}$. In particular, $F_{n+1} = F_{(\tau,n+1)} \cap G = F_{(\tau,n+1)}$ and hence $F_{(\tau,n+1)} \subseteq G$. □

Now we give the proof of the announced fact on generators of $\mathrm{gr}^\tau F$:

(1.3.7) Proposition. *Let $\xi_i \in \mathrm{gr}^\tau_{\tau_i}(F)$, $i = 1, \ldots, d$, denote the initial form of x_i. Then $\mathrm{gr}^\tau(F)$ is generated by $\xi_1, \ldots, \xi_d$ as restricted Lie algebra over $\mathbb{F}_p$.*

Proof. Again we stick closely to the proof of the analogous statement for (x, τ, p)-filtrations given in [Laz65], Ch.II, Prop.3.3.2. Let $I \subseteq \mathbb{N}$ denote the set of values of ω^τ. In other words, I is the smallest subset of $\mathbb{N}$ containing $\tau_1, \ldots, \tau_d$ and being closed under addition and p-th powers. We write $I = \{i_1, i_2, \ldots\}$

*) Theorem 2.6 in [Laz65], App.2 is actually stated in a slightly different way. It involves the ordinary group ring $\mathbb{F}_p[G]$ of some arbitrary (not necessarily free pro-p) p-filtered group (G, ω) instead of $\mathbb{F}_p[\![G]\!]$. By considering finite groups first and then passing to the limit, by condition (ii) the statement remains true when considering complete group rings and filtrations given by *closed* subgroups.

where $i_1 < i_2 < \ldots$. Let L denote the restricted Lie subalgebra of $\mathrm{gr}^\tau F$ generated by $\xi_1, \ldots, \xi_d$ and for $i \in \mathbb{N}$ let L_i denote its homogeneous component of degree i. By definition of I we have $L_i = 0$ for all $i \notin I$. By induction on n we prove that

$$L_i = \mathrm{gr}_i^\tau F \text{ for all } i \leq i_n.$$

First let $n = 1$. Since i_1 is the smallest element in I, we have that $F = F_{(\tau,1)} = F_{(\tau,2)} = \ldots = F_{(\tau,i_1)}$ and hence

$$\mathrm{gr}_i^\tau F = L_i = 0 \text{ for all } i < i_1.$$

Furthermore, since F is topologically generated by $x_1, \ldots, x_d$ and $F_{(\tau,i+1)}$ is an open subgroup of F, $\mathrm{gr}_{i_1}^\tau(F)$ is generated by the initial forms ξ_i of the generators satisfying $\tau_i = i_1$, i.e. $\mathrm{gr}_{i_1}^\tau(F) = L_{i_1}$, which completes the initial step of the induction. Now assume that the hypothesis holds for some $n \in \mathbb{N}$. We have that $F_{(\tau,i_n+1)} = F_{(\tau,i_n+2)} = \ldots = F_{(\tau,i_{n+1})}$ and therefore

$$\mathrm{gr}_i^\tau F = L_i = 0 \text{ for all } i_n < i < i_{n+1}.$$

Now we can apply (1.3.6): Noting that $F_{(\tau,i_{n+1}+1)}$ is an open subgroup of $F_{(\tau,i_{n+1})}$, it follows that the quotient $F_{(\tau,i_{n+1})}/F_{(\tau,i_{n+1}+1)}$ is generated by generators x_i such that $\tau_i = i_{n+1}$ and by commutators $[y,z]$ and p-th powers y^p where $\omega^\tau(y), \omega^\tau(z) \leq i_n$. By the induction hypothesis, this implies that $\mathrm{gr}_{i_{n+1}}^\tau(F)$ is contained in L and hence $\mathrm{gr}_{i_{n+1}}^\tau(F) = L_{i_{n+1}}$. □

We are finally able to deduce the identification $\mathrm{gr}^\tau(F) \cong L_{res}(X)$:

(1.3.8) Theorem. *We have an isomorphism of graded restricted Lie algebras*

$$\mathrm{gr}^\tau(F) \xrightarrow{\sim} L_{res}(X)$$

$$\xi_i \longmapsto X_i,$$

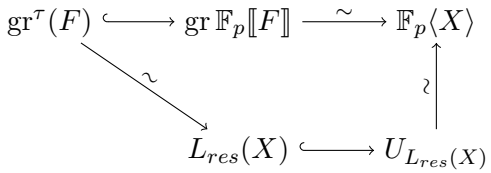
where $\xi_i \in \mathrm{gr}_{\tau_i}^\tau(F)$ denotes the initial form of x_i, $i = 1, \ldots, d$ and $L_{res}(X)$ is endowed with the (X,τ)-graduation defined in (1.2.12).

Proof. By (1.3.4) we have the injective homomorphism of restricted Lie algebras

$$\mathrm{gr}^\tau(F) \hookrightarrow \mathbb{F}_p\langle X \rangle,$$

sending ξ_i to X_i. (1.3.7) shows that this yields an isomorphism of $\mathrm{gr}^\tau(F)$ onto the restricted Lie subalgebra of $\mathbb{F}_p\langle X\rangle$ generated by X_i, $i = 1, \ldots, d$, which is the free restricted Lie algebra $L_{res}(X)$. By definition of the (X,τ)-grading on $L_{res}(X)$ this isomorphism also respects the gradings. □

We can sum up the identifications we have made in the following commutative diagram of restricted Lie algebras:



(1.3.9) Remark. The notion of Zassenhaus (x, τ)-filtrations extends to arbitrary (not necessarily free) finitely generated pro-p-groups: Let G be a pro-p-group with minimal set of generators $y = \{y_1, \ldots, y_d\}$ and

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G \longrightarrow 1,$$

$$x_i \longmapsto y_i$$

be a minimal presentation of G where F denotes the free pro-p-group on $x = \{x_1, \ldots, x_d\}$. Then the Zassenhaus (x, τ)-filtration on F induces a p-restricted filtration on G by setting

$$G_{(\tau,n)} = \pi(F_{\tau,n}).$$

We denote this filtration also by ω^τ. It is the finest p-restricted filtration of G such that $\pi : (F, \omega^\tau) \longrightarrow (G, \omega^\tau)$ is a homomorphism of p-restricted groups. By $\mathrm{gr}^\tau(G)$ we denote the associated graded restricted Lie algebra. We have seen in (1.3.8) that if G is freely generated by the y_i, $\mathrm{gr}^\tau(G)$ is the free restricted Lie algebra on the initial forms of the y_i if G is free. The converse also holds: If $\mathrm{gr}^\tau(G)$ is free on the initial forms of the y_i, it follows that the induced homomorphism of restricted Lie algebras

$$\mathrm{gr}^\tau(F) \longrightarrow \mathrm{gr}^\tau(G)$$

is injective, which implies that $\pi : F \longrightarrow G$ is an isomorphism. In fact, suppose that $1 \neq f \in R$, then, since ω^τ is separated, $f \in F_{(\tau,n)} \setminus F_{(\tau,n+1)}$ for some n, which contradicts the injectivity of $\mathrm{gr}^\tau_n(F) \longrightarrow \mathrm{gr}^\tau_n(G)$.

As an application of (1.3.8) we are able to give explicit bases for the quotients $F_{(\tau,i)}/F_{(\tau,i+1)}$. In analogy to the set of Hall commutators in the free Lie algebra $L(X)$ we introduce the notion of **basic commutators** in the free pro-p-group F, cf. [Vog04]:*)

(1.3.10) Definition. *Let F be the free pro-p-group on the set $x = \{x_1, \ldots, x_d\}$. The set $B_n \subseteq L(X)$ of* **basic commutators of weight n** *together with a total order $<$ is inductively defined as follows:*

(i) $B_1 = \{x_1, \ldots, x_d\}$ *with the ordering* $x_1 > \ldots > x_d$.

*)The definition of basic commutators in the free pro-p-group F is exactly the same as for Hall commutators in free Lie algebras. We only have to replace Lie brackets by taking commutators in F.

(ii) *B_n is the set of all commutators $[b_1, b_2]$ where $b_1 \in B_{n_1},\ b_2 \in B_{n_2}$ such that $n_1 + n_2 = n$, $b_1 > b_2$ and if $n_1 \neq 1,\ b_1 = [b_3, b_4]$ we have $b_2 \geq b_4$. The set B_n is ordered lexicographically, i.e. $[b_1, b_2] < [b_1', b_2']$ if and only if $b_1 < b_1'$ or $b_1 = b_1'$ and $b_2 < b_2'$. Finally for $b \in B_n$ we set $c < b$ for any $c \in B_i,\ i < n$.*

Furthermore, we set

$$\overline{B}_n = \dot{\bigcup}_{ip^j=n} (B_i)^{p^j}$$

and $\mathcal{B} = \bigcup_{n\in\mathbb{N}} B_n,\ \overline{\mathcal{B}} = \bigcup_{n\in\mathbb{N}} \overline{B}_n$.

We obtain the following corollary to (1.3.8).

(1.3.11) Corollary. *Let F be the free pro-p-group on $x = (x_1, \ldots, x_d)$ endowed with the (x, τ)-filtration for some $\tau = (\tau_1, \ldots, \tau_d)$. Then the set*

$$\overline{B}_n^\tau = \{b \in \overline{\mathcal{B}} \mid b \in F_{(\tau,n)}\} \subseteq \overline{\mathcal{B}}$$

defines a $\mathbb{F}_p$-basis of $\mathrm{gr}_n^\tau(F) = F_{(\tau,n)}/F_{(\tau,n+1)}$.

Proof. By (1.3.8) we have the isomorphism of graded restricted Lie algebras $\mathrm{gr}^\tau(F) \xrightarrow{\sim} L_{res}(X)$ sending the initial form of x_i to $X_i,\ i = 1, \ldots, d$ where $L_{res}(X)$ is endowed with the (X, τ)-filtration. By definition of the restricted Lie algebra structure on $\mathrm{gr}^\tau(F)$, it follows that the image of the set $\overline{B}_n^\tau$ in $\mathrm{gr}_n^\tau(F)$ is mapped bijectively onto the set $\overline{C}_n^\tau \subseteq L_{res}(X)$ defined in (1.2.13). Since $\overline{C}_n^\tau$ is a $\mathbb{F}_p$-basis for $L_{res}(X)_n$, the claim follows. □

The correlation to the descending p-central series stated in (1.1.10) remains true if we replace the Zassenhaus filtration (of the free pro-p-group F) by the Zassenhaus (x, τ)-filtation. More precisely, we have the following

(1.3.12) Corollary. *For any $n \geq 1$ we have*

$$F^{(n)} \subseteq F_{(\tau,n)}.$$

Equality holds if

(i) *$n \leq 2$ or*

(ii) *$p = 2,\ n = 3,\ \tau = (1, \ldots, 1)$.*

Proof. The inclusion $F^{(n)} \subseteq F_{(\tau,n)}$ is trivial. It remains to show that $F_{(\tau,2)} = F^{(2)}$. By (1.3.11) we have

$$[F : F_{(\tau,2)}] = p^{\#\overline{B}_1^\tau} = p^d = [F : F^{(2)}]$$

and hence the claim follows. □

(1.3.13) Example. We give some explicit examples in the case where $\tau_i = 1$ for $i = 1, \ldots, d$, i.e. the free pro-p-group F is endowed with the usual Zassenhaus filtration. For small n the following sets are explicit bases for the $\mathbb{F}_p$-vector spaces $\mathrm{gr}_n(F) = F_{(n)}/F_{(n+1)}$ (cf. [Vog04], Ex.1.1.21; note that in (1.3.11) we have shown that these generating sets are actually bases):

n=1:

$$\overline{B}_1 = B_1 = x = \{x_1, \ldots, x_d\}.$$

n=2:

$$\overline{B}_2 = \begin{cases} B_2, & \text{if } p \neq 2, \\ B_2 \cup B_1^2, & \text{if } p = 2 \end{cases}$$
$$\text{where } B_2 = \{[x_i, x_j] \mid 1 \leq i < j \leq d\}.$$

n=3:

$$\overline{B}_3 = \begin{cases} B_3, & \text{if } p \neq 3, \\ B_3 \cup B_1^3, & \text{if } p = 3 \end{cases}$$
$$\text{where } B_3 = \{[[x_i, x_j], x_k] \mid 1 \leq i < j \leq d, 1 \leq k \leq j\}.$$

n=4:

$$\overline{B}_4 = \begin{cases} B_4, & \text{if } p \neq 2, \\ B_4 \cup B_2^2 \cup B_1^4, & \text{if } p = 2. \end{cases}$$

1.4 Strongly free sequences in $\mathbb{F}_p\langle X\rangle$

Throughout this section let $X = \{X_1, \ldots, X_d\}$ and $A = \mathbb{F}_p\langle X\rangle$ be endowed with the (X, τ)-grading for some fixed $\tau = (\tau_1, \ldots, \tau_d)$. In particular, *homogeneous* will always mean homogeneous with respect to this grading. For $f \in \mathbb{F}_p\langle X\rangle$ we denote by $\deg^\tau(f)$ the degree of f with respect to this grading. Furthermore, we define the augmentation ideal I_A of A by

$$I_A = \{f \in \mathbb{F}_p\langle X\rangle \mid \deg^\tau(f) > 0\} = \langle X_1, \ldots, X_d\rangle.$$

(1.4.1) Definition. *Let H be a* **locally finite** *graded algebra (Lie algebra) over an arbitrary field k, i.e. $H = \oplus_{n=0}^\infty H_n$ is a graded k-algebra (Lie algebra) such that H_n is of finite dimension as k-vector space for all n. Then the* **Poincaré series** *$H(t) \in \mathbb{Z}[\![t]\!]$ of H is the formal power series*[*)]

$$H(t) = \sum_{n=0}^{\infty} (\dim_k H_n) t^n.$$

It is additive in exact sequences, i.e. if

$$0 \longrightarrow H' \longrightarrow H \longrightarrow H'' \longrightarrow 0$$

is an exact sequence of graded algebras (Lie algebras) over k, then

$$H(t) = H'(t) + H''(t).$$

[*)] The series $H(t)$ is sometimes also called **Hilbert series** of H.

We define a total ordering on $\mathbb{Z}[\![t]\!]$ by setting $f(t) > g(t)$ if the first non-zero coefficient of $f(t) - g(t)$ is positive. This ordering satisfies the usual compatibility properties with respect to addition and multiplication.

(1.4.2) Lemma. *Let $\rho_1, \ldots, \rho_m \in I_A$ be homogeneous elements of degree $\sigma_i = \deg^\tau \rho_i,\ i = 1, \ldots, m,$*

$$\mathcal{R} = \langle \rho_1, \ldots, \rho_m \rangle$$

be the two-sided ideal of A generated by the ρ_i and $B = A/\mathcal{R}$ be the quotient algebra. We endow B with the natural induced grading. Then the Poincaré series $B(t)$ satisfies

$$B(t) \geq \frac{A(t)}{1 + A(t)(t^{\sigma_1} + \ldots + t^{\sigma_m})} = \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d}) + (t^{\sigma_1} + \ldots + t^{\sigma_m})}.$$

Proof. We follow the arguments given by J. Labute in [Lab06], Prop.3.2. Since $\mathcal{R} \subseteq I_A$, the augmentation sequence

$$0 \longrightarrow I_A \longrightarrow A \longrightarrow \mathbb{F}_p \longrightarrow 0$$

gives rise to the exact sequence

$$0 \longrightarrow \mathcal{R}/\mathcal{R}I_A \longrightarrow I_A/\mathcal{R}I_A \longrightarrow B \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

By left multiplication, the quotient algebra $I_A/\mathcal{R}I_A$ is a free B-module over the images of $X_1, \ldots, X_d$. Furthermore, $\mathcal{R}/\mathcal{R}I_A$ is a left B-module generated by $\rho_1, \ldots, \rho_m$ using the fact that $RA = R(\mathbb{F}_p \oplus I_A) = R\mathbb{F}_p \oplus RI_A$ where R denotes the $\mathbb{F}_p$-span of $\rho_1, \ldots, \rho_m$ in A. Hence one has a surjective map of graded $\mathbb{F}_p$-vector spaces

$$\textstyle\bigoplus_{i=1}^m B[\sigma_i] \longrightarrow\!\!\!\!\!\rightarrow \mathcal{R}/\mathcal{R}I_A$$

where for $l \in \mathbb{N}_0$ by $B[l]$ we denote the $\mathbb{F}_p$-vector space B with grading shifted by l, i.e. $B[l](t) = t^l B(t)$. Summing up, we get an exact sequence of graded $\mathbb{F}_p$-vector spaces

$$\textstyle\bigoplus_{i=1}^m B[\sigma_i] \longrightarrow \bigoplus_{i=1}^d B[\tau_i] \longrightarrow B \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

Taking Poincaré series, we obtain

$$-(t^{\sigma_1} + \ldots + t^{\sigma_m})B(t) + (t^{\tau_1} + \ldots + t^{\tau_d})B(t) - B(t) + 1 \leq 0$$

and solving for $B(t)$, this gives the desired inequality. □

(1.4.3) Definition. *Keeping the notation of* (1.4.2)*, the sequence of homogeneous elements $\rho = \{\rho_1, \ldots, \rho_m\} \subset I_A$ is called* **strongly free** *if the inequality of Poincaré series given in* (1.4.2) *is an equality, i.e. if*

$$B(t) = \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d}) + (t^{\sigma_1} + \ldots + t^{\sigma_m})}. \tag{1.1}$$

Furthermore, we also say that the empty sequence $\rho = \varnothing$ is strongly free, in which case $B = A$ and hence

$$B(t) = \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d})}.$$

(1.4.4) Remark. Note that in the above definition, by a slight abuse of notation, $\rho = \{\rho_1, \ldots, \rho_m\}$ is considered as the *sequence* (and not just as the *subset*) consisting of $\rho_1, \ldots, \rho_m$. For example the sequence $\rho = \{X_1\}$ is strongly free, whereas the sequence $\rho = \{X_1, X_1\}$ is not. However, obviously the strong freeness of ρ does not depend on the ordering of the ρ_i.

In general the series on the right hand side of the equation (1.1) is not positive, which is of course a necessary condition for the existence of a strongly free sequence with given degrees.*) In the case where $\tau = (1, \ldots, 1)$ and $\sigma_i = \sigma$ is constant, we have the following

(1.4.5) Proposition. *Let $\tau = (1, \ldots, 1)$ and $\rho_1, \ldots, \rho_m$ be a strongly free sequence of homogeneous elements of constant degree $\sigma = \deg^\tau \rho_i \geq 2$, $i = 1, \ldots, m$. Then*

$$m \leq \frac{d^\sigma (\sigma - 1)^{\sigma - 1}}{\sigma^\sigma} < \frac{d^\sigma}{(\sigma - 1)e}$$

where $e = 2.718\ldots$.

A proof of this statement can be found in [Ani82], Lemma 3.5.

By definition, strongly free sequences minimize the Poincaré series of the quotient algebra B. They were first introduced by D. Anick (cf. [Ani82]), generalizing the notion of a **regular sequence** in the commutative case. Note that in [Ani82], an equivalent definition is used not involving the Poincaré series. Since the Poincaré series proves useful to compare these equivalent conditions with further characterizations made in terms of Lie algebras (cf. (1.4.21)), we prefer this definition. The original definition due to Anick is condition (iii) in the following proposition.

Following Anick, by $\mathcal{CGA}$ we denote the category of (non-commutative) **connected, locally finite** graded algebras over $\mathbb{F}_p$, i.e. the category of graded $\mathbb{F}_p$-algebras $H = \oplus_{n=0}^\infty H_n$ such that $H_0 = \mathbb{F}_p$ and $\dim_{\mathbb{F}_p} H_i < \infty$.

(1.4.6) Proposition. *Let $\rho_1, \ldots, \rho_m \subset I_A$ be homogeneous elements. Then the following statements are equivalent:*

(i) *$\rho_1, \ldots, \rho_m$ is a strongly free sequence.*

(ii) *The left B-module $\mathcal{R}/\mathcal{R}I_A$ is free over the images of $\rho_1, \ldots, \rho_m$.*

(iii) *The subalgebra $\mathfrak{R} \subseteq A$ generated by $\rho_1, \ldots, \rho_m$ is free over $\rho_1, \ldots, \rho_m$ and there is an isomorphism of graded $\mathbb{F}_p$-vector spaces*

$$\mathfrak{R} \amalg (A/\mathcal{R}) \xrightarrow{\sim} A$$

*) A power series $f = \sum_{i=0}^\infty a_i t^i \in \mathbb{Z}[\![t]\!]$ is called **positive** if $a_i \geq 0$ for all i.

where $\amalg$ *denotes the* **coproduct** *(or* **free product***) in the category* $\mathcal{CGA}$.

Proof. The equivalence (i)⇔(ii) follows directly from the proof of (1.4.2), cf. also [For10], Lemma 1.3. For the equivalence (i)⇔(iii) see [Ani82], Th.2.6. □

(1.4.7) Corollary. *Strong freeness is independent of the choice of the grading: If* $\rho_1, \ldots, \rho_m$ *are also homogeneous with respect to the* (X, τ')*-grading of* A *for some* τ'*, then* $\rho_1, \ldots, \rho_m$ *is strongly free with respect to the* (X, τ)*-grading if and only if it is strongly free with respect to the* (X, τ')*-grading.*

Strongly free sequences satisfy the following permanence properties:

(1.4.8) Proposition.

(i) *Any subsequence of a strongly free sequence is strongly free.*

(ii) *Let* $\rho = \{\rho_1, \ldots, \rho_m\} \subset I_A$, $\tilde{\rho} = \{\tilde{\rho}_1, \ldots, \tilde{\rho}_n\} \subset I_{\tilde{A}}$ *be homogeneous elements where* $A = \mathbb{F}_p\langle X_1, \ldots, X_d\rangle$ *and* $\tilde{A} = \mathbb{F}_p\langle \tilde{X}_1, \ldots, \tilde{X}_e\rangle$*. Then* $\rho \cup \tilde{\rho}$ *is a strongly free sequence in* $\mathbb{F}_p\langle X_1, \ldots, X_d, \tilde{X}_1 \ldots, \tilde{X}_e\rangle$ *if and only if* ρ *and* $\tilde{\rho}$ *are strongly free sequences in* A *and* $\tilde{A}$ *respectively.*

Proof. A proof of (i) is given in [Ani82], Lemma 2.7. For the sake of completeness, we give a sketch of the arguments: Let $\rho = \{\rho_1, \ldots, \rho_m, \rho_{m+1}, \ldots, \rho_n\}$ be a strongly free sequence of homogeneous elements in I_A, $A = \mathbb{F}_p\langle X\rangle$ of degrees $\sigma_i = \deg^\tau \rho_i$. Let $\mathcal{R}$ denote the two-sided ideal generated by ρ and $\tilde{\mathcal{R}}$ be the ideal generated by the subsequence $\rho_1, \ldots, \rho_m$. Setting $B = A/\mathcal{R}$, $\tilde{B} = A/\tilde{\mathcal{R}}$, we have $B = \tilde{B}/\langle\overline{\rho_{m+1}}, \ldots, \overline{\rho_n}\rangle$, i.e. B is the quotient of $\tilde{B}$ by the two-sided ideal generated by the images of $\rho_{m+1}, \ldots, \rho_n$. A similar argument as in (1.4.2) shows that

$$B(t) \geq \frac{\tilde{B}(t)}{1 + \tilde{B}(t)(t^{\sigma_{m+1}} + \ldots + t^{\sigma_n})},$$

or equivalently

$$\tilde{B}(t) \leq \frac{B(t)}{1 - B(t)(t^{\sigma_{m+1}} + \ldots + t^{\sigma_n})}.$$

By assumption we have

$$B(t) = \frac{A(t)}{1 + A(t)(t^{\sigma_1} + \ldots + t^{\sigma_n})},$$

from which it follows that

$$\begin{aligned}
\tilde{B}(t) &\leq \frac{1}{B(t)^{-1} - (t^{\sigma_{m+1}} + \ldots + t^{\sigma_n})} \\
&= \frac{1}{A(t)^{-1} + (t^{\sigma_1} + \ldots + t^{\sigma_n}) - (t^{\sigma_{m+1}} + \ldots + t^{\sigma_n})} \\
&= \frac{1}{A(t)^{-1} + (t^{\sigma_1} + \ldots + t^{\sigma_m})} = \frac{A(t)}{1 + A(t)(t^{\sigma_1} + \ldots + t^{\sigma_m})}.
\end{aligned}$$

Hence also the sequence $\rho_1, \ldots, \rho_m$ is strongly free.

For the proof of statement (ii) set $\overline{A} = \mathbb{F}_p\langle X_1, \ldots, X_d, \tilde{X}_1 \ldots, \tilde{X}_e\rangle$ and note that $A \amalg \tilde{A} \cong \overline{A}$. Let $\mathcal{R}, \tilde{\mathcal{R}}, \overline{\mathcal{R}}$ denote the two-sided ideals of $A, \tilde{A}, \overline{A}$ generated by $\rho, \tilde{\rho}, \overline{\rho} = \rho \cup \tilde{\rho}$, respectively. Let $\sigma_i = \deg^\tau \rho_i$ and $\tilde{\sigma}_i = \deg^{\tilde{\tau}} \tilde{\rho}_i$ denote the degrees of the ρ_i, $\tilde{\rho}_i$ (with respect to the chosen gradings given by $\tau = (\tau_1, \ldots, \tau_d)$, $\tilde{\tau} = (\tilde{\tau}_1, \ldots, \tilde{\tau}_e)$). The canonical surjection $\overline{A} \twoheadrightarrow \overline{A}/\overline{\mathcal{R}}$ factors via the commutative diagram (of graded homomorphisms)

$$\begin{array}{ccc} \overline{A} & \twoheadrightarrow & \overline{A}/\overline{\mathcal{R}} \\ \wr\downarrow & & \uparrow\uparrow \\ A \amalg \tilde{A} & \twoheadrightarrow & A/\mathcal{R} \amalg \tilde{A}/\tilde{\mathcal{R}}. \end{array}$$

As a general fact, for $C, D \in Ob(\mathcal{CGA})$ we have

$$(C \amalg D)(t)^{-1} = C(t)^{-1} + D(t)^{-1} - 1$$

(cf. [Lem74], 5.1.10). Supposing that ρ and $\tilde{\rho}$ are strongly free in A and $\tilde{A}$ respectively, we conclude that

$$\begin{aligned} (\overline{A}/\overline{\mathcal{R}})(t) &\leq \Big((A/\mathcal{R})(t)^{-1} + (\tilde{A}/\tilde{\mathcal{R}})(t)^{-1} - 1\Big)^{-1} \\ &= \Big(A(t)^{-1} + (t^{\sigma_1} + \ldots + t^{\sigma_m}) + \tilde{A}(t)^{-1} + (t^{\tilde{\sigma}_1} + \ldots + t^{\tilde{\sigma}_n}\Big) - 1)^{-1} \\ &= \Big(A(t)^{-1} + \tilde{A}(t)^{-1} - 1 + (t^{\sigma_1} + \ldots + t^{\sigma_m}) + (t^{\tilde{\sigma}_1} + \ldots + t^{\tilde{\sigma}_n})\Big)^{-1} \\ &= \big(\overline{A}(t)^{-1} + (t^{\sigma_1} + \ldots + t^{\sigma_m}) + (t^{\tilde{\sigma}_1} + \ldots + t^{\tilde{\sigma}_n})\big)^{-1} \end{aligned}$$

and hence $\overline{\rho}$ is strongly free in $\overline{A}$.

It remains to show the converse implication. Assume that $\overline{\rho} = \rho \cup \tilde{\rho}$ is strongly free in $\overline{A}$. The natural projection $\mathrm{id} \amalg 0 : \overline{A} = A \amalg \tilde{A} \twoheadrightarrow A$ gives rise to the commutative diagram

$$\begin{array}{ccccc} \overline{A} & \xrightarrow{\mathrm{id} \amalg 0} & A & \twoheadrightarrow & A/\mathcal{R} \\ & \searrow & & \nearrow & \\ & & \overline{A}/\mathcal{R}' & & \end{array}$$

where $\mathcal{R}'$ denotes the ideal of $\overline{A}$ generated by $\rho \cup \{\tilde{X}_1, \ldots \tilde{X}_e\}$. By (i) it follows that the subsequence ρ of $\overline{\rho}$ is strongly free in $\overline{A}$ and, using the opposite statement of (ii) which we have shown above, we conclude that $\rho \cup \{\tilde{X}_1, \ldots, \tilde{X}_e\}$ is strongly free in $\overline{A}$. Hence taking Poincaré series, we have

$$\begin{aligned} (A/\mathcal{R})(t) &\leq \frac{\overline{A}(t)}{1 + \overline{A}(t)(t^{\sigma_1} + \ldots + t^{\sigma_m} + t^{\tilde{\tau}_1} + \ldots + t^{\tilde{\tau}_e})} \\ &= \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d} + t^{\tilde{\tau}_1} + \ldots + t^{\tilde{\tau}_e}) + (t^{\sigma_1} + \ldots + t^{\sigma_m} + t^{\tilde{\tau}_1} + \ldots + t^{\tilde{\tau}_e})} \\ &= \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d}) + (t^{\sigma_1} + \ldots + t^{\sigma_m})}. \end{aligned}$$

This shows that ρ is a strongly free sequence in A. By symmetry, it follows that also $\tilde{\rho}$ is a strongly free sequence in $\tilde{A}$. □

(1.4.9) Remark. Applying (1.4.8) (ii) to $\tilde{\rho} = \varnothing$, we see that a sequence of homogeneous polynomials $\rho_1, \ldots, \rho_m \in I_A$ is strongly free in $A = \mathbb{F}_p\langle X_1, \ldots, X_d\rangle$ if and only if it is strongly free in $\overline{A} = \mathbb{F}_p\langle X_1, \ldots, X_d, X_{d+1}, \ldots, X_{d'}\rangle$ for any $d' \geq d$.

Before proceeding, we give two examples of sequences of homogeneous polynomials of Lie type of degree 2 ($\tau = (1, \ldots, 1)$), one of which is strongly free.

(1.4.10) Example.

(i) Let $d \geq 4,\ \tau = (1, \ldots, 1)$ and

$$\rho_1 = [X_1, X_2],\ \rho_2 = [X_2, X_3],\ \rho_3 = [X_3, X_4],\ \rho_4 = [X_4, X_1].$$

We claim that $\rho_1, \ldots, \rho_4$ is strongly free. By (1.4.9) we may assume $d = 4$. As above we denote by $\mathcal{R}$ the two-sided ideal of A generated by $\rho_1, \ldots, \rho_4$ and set $B = A/\mathcal{R}$. Furthermore, let $\mathcal{R}_i \subseteq \mathcal{R},\ B_i \subseteq B,\ i \geq 0$ denote the $\mathbb{F}_p$-subspaces of homogeneous elements of degree i and

$$r_i = \dim_{\mathbb{F}_p} \mathcal{R}_i,\ b_i = \dim_{\mathbb{F}_p} B_i.$$

By definition, the sequence $\rho_1, \ldots, \rho_4$ is strongly free if and only if

$$B(t) = \frac{1}{1 - 4t + 4t^2}.$$

An easy calculation shows that this is equivalent to the recursive formula

$$b_0 = 1,\ b_1 = 4,\ b_i \leq 2^{i+1} + 4b_{i-2},\ i \geq 2,$$

or equivalently

$$r_0 = r_1 = 0,\ r_i = 4 \cdot (4^{i-2} - r_{i-2}) + 4r_{i-1},\ i \geq 2.$$

Let $\mathcal{M} := \{X_i X_{i+1},\ i = 1, \ldots, 4\}$. We define the sets $\mathcal{C}_i, i \geq 0$ inductively as follows:

$$\begin{aligned} \mathcal{C}_0 &= \{1\}, \\ \mathcal{C}_1 &= \{X_1, \ldots, X_4\}, \\ \mathcal{C}_i &= \{X_{j_1} X_{j_2} \cdots X_{j_i} \mid j_1 \equiv j_2 \equiv \ldots \equiv j_i \mod 2\} \cup \mathcal{M}\mathcal{C}_{i-2},\ i \geq 2. \end{aligned}$$

Obviously $\mathcal{C}_i \subseteq A_i$ and for $c_i = \#\mathcal{C}_i$ we have the recursion formula $c_0 = 1, c_1 = 4$ und $c_i = 2^{i+1} + 4c_{i-2},\ i \geq 2$. Let $C_i \subseteq A_i$ denote the $\mathbb{F}_p$-span of $\mathcal{C}_i$. By a straightforward inductive argument one shows that $A_i = \mathcal{R}_i + C_i$. By reason of dimension, this implies the claim, since by (1.4.2) we have the upper bound $r_i \leq 4 \cdot (4^{i-2} - r_{i-2}) + 4r_{i-1},\ i \geq 2$.

(ii) Now let $d \geq 3$ and as above let $\tau = (1, \ldots, 1)$. We claim that the sequence

$$\rho_1 = [X_1, X_2],\ \rho_2 = [X_2, X_3],\ \rho_3 = [X_3, X_1]$$

is *not* strongly free. Again we may assume that $d = 3$. The Jacobi identity

$$\begin{aligned} 0 &= [X_3, \rho_1] + [X_1, \rho_2] + [X_2, \rho_3] \\ &\equiv X_3\rho_1 + X_1\rho_2 + X_2\rho_3 \mod \mathcal{R}I_A \end{aligned}$$

shows that $\mathcal{R}/\mathcal{R}I_A$ is not free as B-left module over the images of ρ_1, ρ_2, ρ_3 and hence by (1.4.6) the sequence is not strongly free. In fact, there can be no strongly free sequence of 3 homogeneous polynomials of degree 2 in 3 variables, since the series

$$\frac{1}{1 - 3t + 3t^2} = 1 + 3t + 6t^2 + 9t^3 + 9t^4 + 0t^5 - 27t^6 - \ldots$$

is not positive. A calculation of the first terms of the Poincaré series of $B = A/\mathfrak{R}$ using the computational algebra system [MAGMA] in the case $p = 2$ yields

$$B(t) = 1 + 3t + 6t^2 + 10t^3 + 15t^4 + 21t^5 + 28t^6 + \ldots.$$

In general one cannot expect that a given sequence of homogeneous polynomials is amenable to computations 'by hand' as shown in the first example, even if more sophisticated methods such as Gröbner bases are used. However, it would be desirable to have some sufficient criteria for strong freeness which can be checked without much effort for a given sequence. In the following, we will give a collection of criteria which will later prove useful. We start by a criterion due to D. Anick for which we need the notion of a **combinatorially free sequence** of monomials.

(1.4.11) Definition. *Let $\rho = \{\rho_1, \ldots, \rho_m\}$ be a sequence of monomials in I_A (i.e. $\rho_i \neq 1,\ i = 1, \ldots, m$). Then ρ is called* **combinatorially free** *if the following conditions are satisfied:*

(i) *For any $i, j \in \{1, \ldots, m\}, i \neq j$, ρ_i is not a submonomial of ρ_j.*

(ii) *For any $i, j \in \{1, \ldots, m\}$ (where not necessarily $i \neq j$) and any factorization $\rho_i = x_iy_i,\ \rho_j = x_jy_j$ into monomials $x_i, y_i, x_j, y_j \neq 1$, we have*

$$x_i \neq y_j.$$

In other words, the beginning of ρ_i is not the ending of ρ_j for any i, j.

The importance of this definition is given by the following

(1.4.12) Theorem. *Let $\rho = \{\rho_1, \ldots, \rho_m\} \in I_A$ be a sequence of monomials. Then ρ is strongly free if and only if it is combinatorially free.*

For a proof we refer to [Ani82], Th.3.1.

The above theorem yields a necessary and sufficient condition for the strong freeness of a sequence of monomials, which - for a given sequence - is not hard to check. For arbitrary homogeneous polynomials, this can be used to derive powerful criteria.

(1.4.13) Definition. *Let $<$ be an arbitrary total ordering on the set $X = \{X_1, \dots, X_d\}$. Then $<$ induces a total order on the set of all monomials of $\mathbb{F}_p\langle X\rangle$ which we also denote by $<$ as follows: For two monomials α, β we have $\alpha < \beta$ if and only if*

(i) $\deg^\tau \alpha < \deg^\tau \beta$ *or*

(ii) $\deg^\tau \alpha = \deg^\tau \beta$ *and* $\alpha <' \beta$ *where* $<'$ *denotes the lexicographic odering induced by* $<$.

For an arbitrary polynomial $0 \neq f = \sum_\alpha f_\alpha \alpha \in \mathbb{F}_p\langle X\rangle,\ f_\alpha \in \mathbb{F}_p$, *where the sum runs over all monomials, the* **high term** *of f (with respect to $<$) is the highest monomial α (with respect to $<$) such that $f_\alpha \neq 0$, i.e. $\alpha > \beta$ for all $\beta,\ f_\beta \neq 0$.*

(1.4.14) Theorem. *Let $\rho_1, \dots, \rho_m \in I_A$ be a sequence of homogeneous polynomials. Let $\tilde{\rho}_i$ denote the high term of $\rho_i,\ i = 1, \dots, m$ with respect to $<$ for some fixed ordering $<$ on $X = \{X_1, \dots, X_d\}$. If the sequence $\tilde{\rho}_1, \dots, \tilde{\rho}_m$ is combinatorially free, then $\rho_1, \dots, \rho_m$ is strongly free.*

For a proof see [Ani82], Th.3.2.

(1.4.15) Example. Let $\rho_1, \dots, \rho_4$ be as in example (1.4.10) (i). With respect to the ordering $X_2 < X_4 < X_3 < X_1$ the high terms are given by the combinatorially free sequence

$$\tilde{\rho}_1 = X_1X_2,\ \tilde{\rho}_2 = X_3X_2,\ \tilde{\rho}_3 = X_3X_4,\ \tilde{\rho}_4 = X_1X_4.$$

Hence (1.4.14) applies and this gives an alternative proof for the strong freeness of the sequence $\rho_1, \dots, \rho_4$.

It was noticed by P. Forré that the proof of (1.4.14) remains valid for a more general class of total orders on the set of all monomials (cf. [For10], Th.2.6). In particular, in definition (1.4.13) we may replace the grading by any other grading induced by $\tau' = (\tau'_1, \dots, \tau'_d)$ for arbitrary integers $\tau'_i \geq 1$. All that is needed is a total order on the set of monomials which is *multiplicative* in the following sense:

(1.4.16) Definition. *By $\mathfrak{M}$ we denote denote the set of all monomials (including 1) in $\mathbb{F}_p\langle X\rangle$. A total order $<$ on $\mathfrak{M}$ is said to be* **multiplicative** *if the following holds:*

(i) $1 < \alpha$ *for all* $1 \neq \alpha \in \mathfrak{M}$,

(ii) *if* $\alpha < \alpha'$, *then* $\beta\alpha\gamma < \beta\alpha'\gamma$ *for all* $\beta, \gamma \in \mathfrak{M}$.

(1.4.17) Remark. In the same way as in (1.4.13), we define the **high term** of a polynomial with respect to a given multiplicative order $<$. Then (1.4.14) remains true for $<$, cf. [For10], Th.2.6.

We will now construct a special class of multiplicative orders which might appear to be rather technical, but which will prove useful in order to deduce Theorem (2.3.2) in the next chapter.

(1.4.18) Definition. *Let $U \subseteq X = \{X_1, \dots, X_d\}$ be a subset and $<$ a total ordering on $X = \{X_1, \dots, X_d\}$. We define a total order $<_U$ on $\mathfrak{M}$ as follows: For a monomial $\alpha = X_{i_1} \cdots X_{i_{n_\alpha}}$ let l_α^U denote the number of X_i's in α such that $X_i \notin U$, i.e. $l_\alpha := \#\{k = 1, \dots, n_\alpha \mid X_{i_k} \notin U\}$. If $\beta = X_{j_1} \cdots X_{j_{n_\beta}}$ is another monomial, we set $\alpha <_U \beta$ if and only if*

(i) $\deg^\tau \alpha < \deg^\tau \beta$ *or*

(ii) $\deg^\tau \alpha = \deg^\tau \beta$ *and* $l_\alpha^U < l_\beta^U$ *or*

(iii) $\deg^\tau \alpha = \deg^\tau \beta$ *and* $l_\alpha^U = l_\beta^U$ *and*

$$k_\alpha^U := \sum_{\substack{1 \le k \le n_\alpha, \\ X_{i_k} \notin U}} \deg^\tau(X_{i_1} \cdots X_{i_k}) < k_\beta^U := \sum_{\substack{1 \le k \le n_\beta, \\ X_{j_k} \notin U}} \deg^\tau(X_{i_1} \cdots X_{i_k})$$

or

(iv) $\deg^\tau \alpha = \deg^\tau \beta$ *and* $l_\alpha^U = l_\beta^U$ *and* $k_\alpha^U = k_\beta^U$ *and* $\alpha <' \beta$ *with respect to the lexicographic ordering $<'$ induced by $<$.*

Very roughly speaking, the more $X_i \notin U$ are contained in a given monomial α and the more right they occur, the higher α is with respect to $<_U$. It is not hard to check that $<_U$ is indeed a multiplicative order on $\mathfrak{M}$. Note that for $U = \varnothing$ and $U = X$ it agrees with the order induced by $<$ as defined in (1.4.13). The following example illustrates that applying Anick's criterion with respect to various multiplicative orders is a powerful tool to prove the strong freeness of a given sequence.

(1.4.19) Example. Let $d \ge 4$, $\tau = (1, \dots, 1)$. We claim that the sequence

$$\rho_1 = X_1^2 + [X_1, X_2],\ \rho_2 = X_2^2 + [X_2, X_3],\ \rho_3 = [X_3, X_4],\ \rho_4 = [X_4, X_1].$$

is strongly free. It is not hard to see that with respect to any lexicographic monomial ordering defined as in (1.4.13) the sequence of high terms is never combinatorially free. However, we can apply Anick's criterion (1.4.14) with respect to an ordering of the form $<_U$ as in (1.4.18). In fact, fixing the total ordering $X_1 < X_2 < X_3 < X_4$ and setting $U = \{X_1, X_2\}$, the high terms of the ρ_i with respect to $<_U$ are given by the combinatorially free sequence

$$X_2X_1,\ X_2X_3,\ X_4X_3,\ X_4X_1.$$

We cite a result due to P. Forré on how strongly free sequences can be modified by dealing with different (X,τ)-gradings at the same time. This also provides greater flexibility in applying Anick's criterion. The exact statement is the following (cf. [For10], Cor.3.10):

(1.4.20) Theorem. *Let $\rho_1,\ldots,\rho_m \in I_A$ be homegeneous with respect to the (X,τ)-grading. Suppose that for some $\tau' = (\tau'_1,\ldots,\tau'_d)$, $\tau'_i \geq 1$ we have*

$$\rho_i = \kappa_i + \lambda_i,\ i = 1,\ldots,m$$

where $\kappa_1,\ldots,\kappa_m$ is a strongly free sequence of elements being homogeneous with respect to the (X,τ')-grading and $\deg^{\tau'}\lambda_i > \deg^{\tau'}\kappa_i$ for all $i = 1,\ldots,m$. Then $\rho_1,\ldots,\rho_m$ is also strongly free.

For homogeneous polynomials of Lie type, we have a description of strong freeness due to J. Labute (cf. [Lab06]), which coincides with the previous definition. This enables us to make use of a powerful criterion using the **elimination theorem** for free Lie algebras.

Let $\rho = \{\rho_1,\ldots,\rho_m\} \in L(X)$ be homogeneous polynomials of Lie type. By $\mathfrak{r} \subseteq L(X)$ denote the Lie ideal generated by $\rho_1,\ldots,\rho_m$ and $\mathfrak{g} = L(X)$ the quotient Lie algebra. Then $\mathfrak{r}/[\mathfrak{r},\mathfrak{r}]$ is a module over the enveloping algebra $U_\mathfrak{g}$ of $\mathfrak{g}$ via the **adjoint representation**, i.e. the operation is induced by

$$\mathfrak{g} \times \mathfrak{r}/[\mathfrak{r},\mathfrak{r}] \longrightarrow \mathfrak{r}/[\mathfrak{r},\mathfrak{r}],$$

$$(x \bmod \mathfrak{r}, y) \longmapsto ad(x)(y) \bmod \mathfrak{r} = [x,y] \bmod \mathfrak{r}.$$

Now we have the following

(1.4.21) Proposition. *The sequence ρ is strongly free if and only if $\mathfrak{r}/[\mathfrak{r},\mathfrak{r}]$ is a free $U_\mathfrak{g}$-module over the images of $\rho_1,\ldots,\rho_m$.*[*)]

Proof. Let $\sigma_i = \deg^\tau \rho_i,\ i = 1,\ldots,m$. By [Lab06], Prop.3.2, $\mathfrak{r}/[\mathfrak{r},\mathfrak{r}]$ is a free $U_\mathfrak{g}$-module over $\rho_1,\ldots,\rho_m$ if and only if the Poincaré series of $U_\mathfrak{g}$ satisfies

$$U_\mathfrak{g}(t) = \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d}) + (t^{\sigma_1} + \ldots + t^{\sigma_m})}. \tag{1.2}$$

By [Bou75], Ch.I, §2.3, Prop.1, we have a canonical exact sequence

$$1 \longrightarrow \mathcal{R} \longrightarrow U_{L(X)} \longrightarrow U_\mathfrak{g} \longrightarrow 1$$

where $\mathcal{R}$ denotes the ideal of the enveloping algebra $U_{L(X)}$ of $L(X)$ generated by $\mathfrak{r}$. By definition of $\mathfrak{r}$ it follows that $\mathcal{R} = \langle\rho_1,\ldots,\rho_m\rangle$ is the ideal generated by the ρ_i. Hence we have the identification $U_{L(X)}/\langle\rho_1,\ldots,\rho_m\rangle \cong U_\mathfrak{g}$, which by definition implies that the equality (1.2) is equivalent to ρ being strongly free. □

[*)] This is exactly Def.3.1 in [Lab06]. Note that in our situation $k = \mathbb{F}_p$ is a field, so the condition on $U_\mathfrak{g}$ being free as k-module is redundant.

By the **elimination theorem** for free Lie algebras is formulated as follows (cf. [Bou75], Ch.II, §2.9, Prop.10): Let $S \subseteq X$ be a subset and R denote set of all sequences

$$(s_1, \ldots, s_n, x),\ n \geq 0,\ s_1, \ldots, s_n \in S,\ x \in X \setminus S.$$

Let $\mathfrak{a}$ be the (Lie) ideal of $L(X)$ generated by $X \setminus S$. Then $\mathfrak{a}$ can be identified with the free Lie algebra over R, more precisely one has the natural isomorphism

$$L(R) \xrightarrow{\sim} \mathfrak{a},$$

$$(s_1, \ldots, s_n, x) \longmapsto (ad(s_1) \circ \cdots \circ ad(s_n)(x).$$

Using this general fact, one can prove the following

(1.4.22) Proposition. *Let $S \subseteq X$ and $\mathfrak{a} \subseteq L(X)$ the ideal generated by $X \setminus S$. Let U denote the enveloping algebra of $L(X)/\mathfrak{a} = L(S)$. Furthermore, consider a subset $T = \{a_1, \ldots, a_t\} \subset \mathfrak{a}$ whose elements are homogeneous and U-independent modulo $[\mathfrak{a}, \mathfrak{a}]$. If $\rho_1, \ldots, \rho_m$ are homogeneous elements of $\mathfrak{a}$ which lie in the $\mathbb{F}_p$-span of T modulo $[\mathfrak{a}, \mathfrak{a}]$ and which are linearly independent over $\mathbb{F}_p$ modulo $[\mathfrak{a}, \mathfrak{a}]$, then the sequence $\rho_1, \ldots, \rho_m$ is strongly free.*

This is shown in [Lab06], Th.3.3, noting that by (1.4.21) for Lie polynomials Labute's definition of strongly free sequences coincides with our definition.

(1.4.23) Example. We make use of Labute's criterion to give a third proof of the strong freeness of the sequence $\rho_1, \ldots, \rho_4$ given as in (1.4.10) by

$$\rho_1 = [X_1, X_2],\ \rho_2 = [X_2, X_3],\ \rho_3 = [X_3, X_4],\ \rho_4 = [X_4, X_1].$$

Then (1.4.22) applies setting

$$S = \{X_1, X_3\} \subset X, \quad T = \{[X_1, X_2], [X_1, X_4], [X_3, X_2], [X_3, X_4]\}.$$

This sequence is an example for **non-singular circuits** which will be defined in the next section.

1.5 Mild pro-p-groups with respect to Zassenhaus (x, τ)-filtrations

In this section we introduce so-called **mild** pro-p-groups. This notion has been originally introduced by D. Anick in the case of finitely presented (discrete) groups (cf. [Ani87]). In [Lab06], J. Labute gave a similar definition for finitely presented pro-p-groups. The main purpose for the study of these groups lies on the fact that they are of cohomological dimension ≤ 2.

For a pro-p-group G we set

$$H^i(G) := H^i(G, \mathbb{Z}/p\mathbb{Z}) \text{ and } h^i(G) := \dim_{\mathbb{F}_p} H^i(G),\ i \geq 0$$

(1.5.1) Definition. *Let G be a pro-p-group. A presentation*

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

of G by a free pro-p-group F is called **minimal** *if the inflation map*

$$inf: \ H^1(G) \hookrightarrow H^1(F)$$

is an isomorphism.

(1.5.2) Lemma. *Let F be the free pro-p-group on $x = \{x_1, \ldots, x_d\}$ endowed with the Zassenhaus (x, τ)-filtration for some $\tau = (\tau_1, \ldots, \tau_d)$. Then a presentation*

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

of a pro-p-group G is minimal if and only if $R \subseteq F_{(\tau,2)}$.

Proof. The presentation is minimal if and only if the induced map $H^1(G) = (G/G^{(2)})^\vee \longrightarrow H^1(F) = (F/F^{(2)})^\vee$ is surjective, which is equivalent to $R \subseteq F^{(2)}$ (recall that $F^{(n)}$ denotes the descending p-central series of F). By (1.3.12), $F^{(2)} = F_{(\tau,2)}$ and hence the claim follows. □

If F is the free pro-p-group on $x = \{x_1, \ldots, x_d\}$ endowed with the Zassenhaus (x, τ)-filtration for some $\tau = (\tau_1, \ldots, \tau_d)$ and R is the closed normal subgroup generated by $r_1, \ldots, r_m \in F_{(\tau,2)}$, then

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

is a minimal presentation for $G = F/R$ and we also write

$$G = \langle x_1, \ldots, x_d \mid r_1, \ldots, r_m \rangle.$$

(1.5.3) Definition.

(i) *Let F be the free pro-p-group on $x = \{x_1, \ldots, x_d\}$ endowed (x, τ)-filtration for some $\tau = (\tau_1, \ldots, \tau_d)$ and $r_1, \ldots, r_m \in F_{(\tau,2)} = F^{(2)}$. Let $X = \{X_1, \ldots, X_d\}$ and suppose that the sequence of the initial forms ρ_i of r_i*

$$\rho_1, \ldots, \rho_m \in \mathrm{gr}^\tau(F) \cong L_{res}(X) \subset \mathbb{F}_p\langle X \rangle$$

is strongly free. Then $G = \langle x_1, \ldots, x_d \mid r_1, \ldots, r_m \rangle$ is called **strongly free presentation with respect to the Zassenhaus (x, τ)-filtration** *of the pro-p-group G.*

(ii) *A finitely generated pro-p-group G with $d = h^1(G)$ is called* **mild (with respect to the Zassenhaus (x, τ) − filtration)** *if it possesses a strongly free presentation with respect to the Zassenhaus (x, τ)-filtration.*

(1.5.4) Remark. There exist a similar notion of strongly free presentations (and hence of mild pro-p-groups) with respect to the descending p-central series (cf. [Lab06]), i.e. where the free pro-p-group F in a minimal presentation is endowed with the descending p-central series (or more generally a (x,τ)-filtration). In order to give this definition, one has to transfer the notion of a strongly free sequence in the associated graded object

$$\bigoplus_{i\geq 1} F^{(i)}/F^{(i+1)},$$

which carries the structure of a free Lie algebra over the polynomial ring $\mathbb{F}_p[\pi]$.*) However, the latter is true only in the case $p > 2$. If $p = 2$, one has to deal with **mixed** Lie algebras introduced by Lazard, which has been worked out by J. Labute and J. Mináč (cf. [LM11]). It can be seen as an advantage of the Zassenhaus (x,τ)-filtration that $\mathrm{gr}^\tau(F) \cong L_{res}(X)$ for all p.

For pro-p-groups being mild with respect to the Zassenhaus filtration (i.e. $\tau = (1,\ldots,1)$) and having relations of constant degree, one can deduce the following statement immediately from the definition:

(1.5.5) Proposition. *Let G be a finitely presented pro-p-group and assume that $G = \langle x_1,\ldots,x_d \mid r_1,\ldots,r_m\rangle$ is a strongly free presentation with respect to the Zassenhaus filtration, such that the r_i are of constant degree $n = \deg r_1 = \ldots = \deg r_m$. Then we have*

$$h^2(G) \leq \frac{h^1(G)^n(n-1)^{n-1}}{n^n}.$$

Furthermore, unless $G \cong \mathbb{Z}_p$ or $h^1(G) = 2,\ h^2(G) = 1,\ n = 2$, G is not p-adic analytic.

Proof. Noting that $h^2(G) \leq m$,**) the first statement follows immediately from the upper bound for the length of strongly free sequences given in (1.4.5). Using a generalization of the Golod-Šafarevič inequality, this implies that G is not p-adic analytic unless $G \cong Z_p$ (i.e. $h^1(G) = 1, h^2(G) = 0$) or $h^1(G) = 2,\ h^2(G) = 1,\ n = 2$, see [Koc69], Satz 3 or [Lub83], Prop.1.3 and Rem.1.4. □

In (1.5.10)(v), we will show in greater generality that mild pro-p-groups are usually not p-adic analytic. This is also interesting from an arithmetic point of view: If G is the Galois group $G_S(p)$ of the maximal p-extension of a number field k unramified outside the set S not containing the primes above p, this should hold as a consequence of the famous **Fontaine-Mazur Conjecture** (cf. [NSW08], 10.10.12). On the other hand, these groups are often mild, e.g. see the results of J. Labute [Lab06]. In [Sch10], A. Schmidt has shown in a general setting, that $G_S(p)$ can be "made" mild (and hence it is not p-adic analytic)

*) Here the multiplication by π can be seen as the analogue of the p-power map in a restricted Lie algebra. For details see [Lab06].

**) As we will see in (1.5.10)(i), the strong freeness of the presentation implies the equality $h^2(G) = m$.

by enlarging the set S, see also (2.3.5) for details. In the third chapter, we will give a construction of arithmetic examples of mild pro-p-groups with defining relations of degree $n = 3$.

(1.5.6) Definition. *Let $\mathcal{A}$ be a ring with unit and let M be a (left-) $\mathcal{A}$-module. The* **projective dimension** *$pd_{\mathcal{A}}M$ of M is the infimum of all n such that there exists a projective resolution*

$$0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \ldots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

for M of length n. If no such n exists, we set $pd_{\mathcal{O}}M = \infty$. Furthermore, for the trivial module we set $pd_{\mathcal{O}}M = 0$.

The following result goes back to A. Brumer ([Bru66]), for a proof see [NSW08], Cor.5.2.13.

(1.5.7) Theorem. *Let G be a profinite group and $\mathcal{O}$ a complete commutative local ring with maximal ideal $\mathfrak{m}$, such that $\mathcal{O}/\mathfrak{m}^n$ is finite for all n (in particular, $\mathcal{O}$ is compact). We consider $\mathcal{O}$ as (left) module over the complete group ring $\mathcal{O}[\![G]\!]$ via the trivial action of G on $\mathcal{O}$.*[*)] *Then*

$$pd_{\mathcal{O}[\![G]\!]}\mathcal{O} = cd_p G$$

where p denotes the characteristic of the residue field $\mathcal{O}/\mathfrak{m}$.

We will apply this result in the case $\mathcal{O} = \mathbb{F}_p$:

(1.5.8) Corollary. *Let G be a pro-p-group. Then*

$$pd_{\mathbb{F}_p[\![G]\!]}\mathbb{F}_p = cd\ G$$

The following lemma is well-known. However, part of the argumentation will be reused to prove the main theorem on mild pro-p-groups (see (1.5.10)), so we have included a proof here.

(1.5.9) Lemma. *Let G be a finitely generated pro-p-group, $d = h^1(G)$ and*

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

a minimal presentation where F denotes the free pro-p-group on $x_1, \ldots x_d$. Then there is an exact sequence of $\mathbb{F}_p[\![G]\!]$-modules

$$0 \longrightarrow R/R^p[R,R] \longrightarrow \mathbb{F}_p[\![G]\!]^d \longrightarrow \mathbb{F}_p[\![G]\!] \longrightarrow \mathbb{F}_p \longrightarrow 0$$

where the $\mathbb{F}_p[\![G]\!]$-action on $R/R^p[R,R]$ is induced by conjugation.[**)]

[*)] In the following, all modules will be *left* modules. However, the inversion $\sigma \longmapsto \sigma^{-1}$ induces an equivalence between the categories of left and right $\mathcal{O}[\![G]\!]$-modules, hence all statements remain true if we consider right $\mathcal{O}[\![G]\!]$-modules instead.

[**)] Precisely, the action of $\mathbb{F}_p[\![G]\!]$ on $R/R^p[R,R]$ is induced by the *left* action $(g, \overline{r}) \longmapsto \overline{\tilde{g}r\tilde{g}^{-1}}$ where $g \in G$ and $\tilde{g} \in F$ is an arbitrary lift.

Proof. Let I_R denote the closed left (right) ideal of $\mathbb{F}_p[\![F]\!]$ generated by $r-1,\ r \in R$. Then we have the commutative exact diagram of $\mathbb{F}_p$-algebras

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & I_R I(F) & \longrightarrow & I_R & \longrightarrow & I_R/I_R I(F) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow 0 & & \\
0 & \longrightarrow & I(F) & \longrightarrow & \mathbb{F}_p[\![F]\!] & \longrightarrow & \mathbb{F}_p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
 & & I(F)/I_R I(F) & \longrightarrow & \mathbb{F}_p[\![G]\!] & \longrightarrow & \mathbb{F}_p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

and hence we obtain the exact sequence of $\mathbb{F}_p[\![G]\!]$-modules

$$0 \longrightarrow I_R/I_R I(F) \longrightarrow I(F)/I_R I(F) \longrightarrow \mathbb{F}_p[\![G]\!] \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

Since $I(F)$ is free as $\mathbb{F}_p[\![F]\!]$-module over $x_1-1,\dots,x_d-1$, it follows that $I(F)/I_R I(F)$ is free as $\mathbb{F}_p[\![G]\!]$-module over $x_1-1,\dots,x_d-1$, i.e. $I(F)/I_R I(F) \cong \mathbb{F}_p[\![G]\!]^d$. Furthermore, the mapping $R \longrightarrow I_R,\ r \longmapsto r-1$ induces a well-defined homomorphism of $\mathbb{F}_p$-vector spaces

$$\phi : R/R^p[R,R] \longrightarrow I_R/I_R I(F).$$

Since $R = \mathbb{F}_p[\![F]\!]\mathfrak{r} = (\mathbb{F}_p \oplus I(F))\mathfrak{r}$ where $\mathfrak{r}$ denotes the $\mathbb{F}_p$-span of $\{r-1,\ r \in R\}$, we see that ϕ is surjective. In fact, ϕ is an isomorphism (see [Bru66], proof of Th.5.2). Finally the identity

$$\begin{aligned}
& grg^{-1} - 1 \\
= \ & (g-1)(r-1)(g^{-1}-1) + (g-1)(r-1) + (r-1)(g^{-1}-1) + (r-1) \\
\equiv \ & g(r-1) \mod I_R I(F),\ g \in F, r \in R
\end{aligned}$$

shows that ϕ is compatible with the $\mathbb{F}_p[\![G]\!]$-action which concludes the proof. □

Together with theorem (1.5.7), the above lemma is the key step to show that mild pro-p-groups are of cohomological dimension ≤ 2. This fact is the main reason for our interest in mild pro-p-groups. However, they have some further useful properties being summed up in the following theorem:

(1.5.10) Theorem. *Let F be the free pro-p-group on $x = \{x_1,\dots,x_d\}$ endowed with the (x,τ)-filtration for some $\tau = (\tau_1,\dots,\tau_d)$. Let G be a mild pro-p-group such that $G = F/R = \langle x_1,\dots,x_d \mid r_1,\dots,r_m\rangle$ is a strongly free presentation with respect to the Zassenhaus (x,τ)-filtration where $R \subseteq F_{(\tau,2)}$ denotes the closed normal subgroup generated by $r_i,\ i = 1,\dots,m$. Set $\sigma_i := \deg^\tau r_i,\ i = 1,\dots,m$. Then the following holds:*

(i) *We have* $cd\, G = 2$ *and the relation rank* $h^2(G)$ *of* G *is equal to* m.

(ii) *The* $\mathbb{F}_p[\![G]\!]$*-module* $R/R^p[R,R]$ *is free over the images of* $r_1, \ldots, r_m$.

(iii) *We have* $\mathrm{gr}^\tau(G) = \mathrm{gr}^\tau(F)/(\rho_1, \ldots, \rho_m)$ *where* $(\rho_1, \ldots, \rho_m)$ *denotes the ideal of the restricted Lie algebra* $\mathrm{gr}^\tau(F)$ *generated by the initial forms* ρ_i *of* r_i.

(iv) *The universal enveloping algebra* $U_{\mathrm{gr}^\tau(G)}$ *of* $\mathrm{gr}^\tau(G)$ *is the graded algebra associated to the filtration on* $\mathbb{F}_p[\![G]\!]$ *induced by the* (x,τ)*-filtration on* $\mathbb{F}_p[\![F]\!]$ *and its Poincaré series satisfies*

$$U_{\mathrm{gr}^\tau(G)}(t) = \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d}) + (t^{\sigma_1} + \ldots + t^{\sigma_m})}.$$

(v) *If* $m \neq d-1$, *then* G *is not* p*-adic analytic.*

(1.5.11) Remarks.

(i) If the initial forms $\rho_1, \ldots, \rho_m$ are of Lie type, the above statements are contained in [Lab06], Th.5.1, noting that by (1.4.21) the different notions of strongly free sequences coincide. However, note that dealing with general strongly free sequences of restricted Lie type yields an important generalization and is crucial for the application to arithmetically defined pro-p-groups. A different proof of the fact mild pro-p-groups are of cohomological dimension ≤ 2 involving (associative) $\mathbb{F}_p$-algebras is given in [For10].

(ii) The fact that one can check mildness with respect to various Zassenhaus (x,τ)-filtrations is an obvious but useful property. For example, consider the pro-p-group

$$G = \langle x_1, x_2 \mid x_1^2 x_2^4 \rangle,$$

which is not mild with respect to the Zassenhaus filtration.*) However, it is mild with respect to the Zassenhaus (x,τ)-filtration where $\tau_1 = 2, \tau_2 = 1$.

In the following proof we can adopt the main ideas of the proof of [Lab06], Th.4.1. There similar results are obtained in the case of strongly free sequences with respect to (generalized) p-central series. The main difference lies in the fact that we have to deal with graded (associative) $\mathbb{F}_p$-algebras, whereas Labute's notion of strong freeness is in terms of free Lie algebras over the polynomial ring $\mathbb{F}_p[\pi]$.

*) In general checking that a pro-p-group is *not* mild with respect to some Zassenhaus (x,τ)-filtration needs some careful argumentation, since it is not sufficient to show that a given presentation is not strongly free. However, if the defining relations in a given minimal presentation are of the same degree and the initial forms are linearly independent over $\mathbb{F}_p$, then this presentation is strongly free if and only if G possesses a strongly free presentation.

Proof of (1.5.10). For the sake of simplicity and ignoring our notational conventions, we omit the indices τ during the proof, hence we set $F_{(n)} = F_{(\tau,n)}$, $\mathrm{gr}_n(F) = \mathrm{gr}_n^\tau(F)$ etc. By $(R_{(n)})_{n\in\mathbb{N}}$ we denote the induced filtration on R, i.e. $R_{(n)} = F_{(n)} \cap R$. Furthermore, we set $M = R/R^p[R,R]$ and set $M_{(n)} = \pi(R_{(n)})$ where π is the canonical surjection $\pi : R \longrightarrow M$. In the proof of (1.5.9) we have seen that we have a canonical isomorphism of graded $\mathbb{F}_p[\![G]\!]$-modules

$$\phi :\ M \xrightarrow{\ \sim\ } \hat{\mathcal{R}}/\hat{\mathcal{R}}I_{\hat{A}} \tag{1.3}$$

induced by $R \longrightarrow \hat{\mathcal{R}},\ r \longmapsto r-1$ where $I_{\hat{A}} = I(F)$ is the augmentation ideal of $\hat{A} = \mathbb{F}_p[\![F]\!]$ and $\hat{\mathcal{R}} = I_R$ denotes the closed two-sided ideal generated by $r-1,\ r \in R$. Let $\mathcal{R}$ denote the two-sided ideal of $A = \mathrm{gr}(\mathbb{F}_p[\![F]\!]) \cong \mathbb{F}_p\langle X_1,\ldots,X_d\rangle$ generated by the initial forms of ρ_i of $r_i,\ i = 1,\ldots,m$. By definition, we have the inclusion $\mathcal{R} \hookrightarrow \mathrm{gr}\,\hat{\mathcal{R}}$. We endow the ideals $\hat{\mathcal{R}}$ and $\hat{\mathcal{R}}I_{\hat{A}}$ with the filtrations induced by the filtration on $\mathbb{F}_p[\![F]\!]$. We obtain a homomorphism

$$\psi : \mathcal{R}/\mathcal{R}I_A \longrightarrow \mathrm{gr}\,\hat{\mathcal{R}}/\,\mathrm{gr}(\hat{\mathcal{R}}I_{\hat{A}}) = \mathrm{gr}(\hat{\mathcal{R}}/\hat{\mathcal{R}}I_{\hat{A}})$$

of graded $\mathbb{F}_p$-algebras. We claim that ψ is an isomorphism. Noting that the isomorphism ϕ (1.3) respects the filtrations on M and $\hat{\mathcal{R}}I_{\hat{A}}$ respectively, this is equivalent to showing that the composite

$$\xi :\ \mathcal{R}/\mathcal{R}I_A \longrightarrow \mathrm{gr}(\hat{\mathcal{R}}/\hat{\mathcal{R}}I_{\hat{A}}) \xrightarrow{\ \sim\ } \mathrm{gr}\,M$$

of ψ with the isomorphism $\mathrm{gr}\,\phi^{-1}$ is again an isomorphism. We prove this by induction on degrees. Let $k \in \mathbb{N}$ and assume that ξ is an isomorphism in degrees $< k$ (if $k = 1$, this is clearly fulfilled, since the degree zero subspaces are trivial).

Injectivity of ξ in degree k: First deduce that $\mathcal{R}_n = \mathrm{gr}_n\,\hat{\mathcal{R}}$ for all $n < k$. In fact, this follows immediately by induction on degrees from the surjectivity of ξ (and hence of ψ) in degrees $< k$. Let $\chi \in \mathrm{gr}_n(\hat{\mathcal{R}}I_{\hat{A}})$. Then χ is the initial form of some element $\sum_{i=1}^{l} x_i y_i,\ x_i \in \hat{\mathcal{R}},\ y_i \in I_{\hat{A}}$ such that $\deg x_i + \deg y_i = k$ for all i. In particular, $\deg x_i, \deg y_i < k$. Using $\mathcal{R}_n = \mathrm{gr}_n\,\hat{\mathcal{R}},\ I_A = \mathrm{gr}_n\,I_{\hat{A}},\ n < k$, we conclude that $(\mathcal{R}I_A)_k = \mathrm{gr}_k(\hat{\mathcal{R}}I_{\hat{A}})$ and consequently ψ (and hence ξ) is injective in degree k.

Surjectivity of ξ in degree k: Let β be a non-zero element in $\mathrm{gr}_k(M)$ and choose $b \in M_k = (R/R^p[R,R])_k$ whose inital form is β. Denoting by $\overline{r}_i$ the image of r_i in M, then $\overline{r}_1,\ldots,\overline{r}_m$ generate M as $\mathbb{F}_p[\![G]\!]$-module and we may therefore write

$$b = g_1\overline{r}_1 + \ldots + g_m\overline{r}_m$$

with some $g_i \in \mathbb{F}_p[\![G]\!]$. Set $\omega_i = \deg g_i,\ i = 1,\ldots,m$ (where we endow $\mathbb{F}_p[\![G]\!]$ with the filtration induced by the (x,τ)-filtration on $\mathbb{F}_p[\![F]\!]$). By definition of the operation of $\mathbb{F}_p[\![G]\!]$ on M, we have $(\mathbb{F}_p[\![G]\!])_i M_j \subseteq M_{i+j}$ and hence we may

assume that in the above sum we have $g_i = 0$ or $\omega_i + \sigma_i \leq k$ for all $i = 1, \ldots, m$. Let

$$k' := \min_{\substack{i=1,\ldots,m,\\ g_i \neq 0}} (\omega_i + \sigma_i).$$

We claim that $k' = k$. To this end, assume $k' < k$ and let $I = \{i = 1, \ldots, m \mid \omega_i + \sigma_i = k'\}$. Let $\overline{\rho}_i$ denote the image of ρ_i in $\mathcal{R}/\mathcal{R}I_A$ and set

$$\varrho := \sum_{i \in I} u_i \overline{\rho}_i \in \mathcal{R}/\mathcal{R}I_A$$

where $u_i \in A/\mathcal{R}$ is a preimage of the inital form $\overline{g}_i$ of g_i under the canonical projection

$$A/\mathcal{R} \longrightarrow\!\!\!\!\!\rightarrow \operatorname{gr}(\mathbb{F}_p[\![G]\!]) = A/\operatorname{gr}\hat{\mathcal{R}}.$$

By definition ϱ is mapped via ξ to the image of $\sum_{i \in I} g_i \overline{r}_i$ in $\operatorname{gr}_{k'} M = M_{k'}/M_{k'+1}$. Since by assumption $\deg b = k > k'$, we have $\xi(\varrho) = 0$. By the induction hypothesis, this implies $\varrho = 0$ and by (1.4.6) the strong freeness of the sequence $\rho_1, \ldots, \rho_m$ implies $u_i = 0$ for all $i \in I$ which yields a condradiction, since $\overline{g}_i \neq 0$, $i \in I$. Hence we have $k' = k$, i.e. $\omega_i + \sigma_i = k$ for all i such that $g_i \neq 0$ and consequently β lies in the image of ξ. This finishes the induction, i.e. ξ and hence ψ are isomorphisms.

By the definition of the filtrations on R and G, $\operatorname{gr} R$ is an ideal of the restricted Lie algebra $\operatorname{gr} F$ and we have $\operatorname{gr} G = \operatorname{gr} F/\operatorname{gr} R$. Let $\mathcal{R}'$ denote the (two-sided) ideal of A generated by the image of $\operatorname{gr} R$ under the inclusion $\operatorname{gr} F \hookrightarrow A = \operatorname{gr}(\mathbb{F}_p[\![F]\!]) = U_{\operatorname{gr} F}$. Then we have the inclusions

$$\mathcal{R} \subseteq \mathcal{R}' \subseteq \operatorname{gr}\hat{\mathcal{R}} \subseteq A.$$

But as we have already remarked, the surjectivity of ψ implies $\mathcal{R} = \operatorname{gr}\hat{\mathcal{R}}$ and consequently $\mathcal{R}' = \operatorname{gr}\hat{\mathcal{R}}$. By (1.2.6) the universal enveloping algebra of $\operatorname{gr} G$ is given by

$$U_{\operatorname{gr} G} = U_{\operatorname{gr} F}/\mathcal{R}' = A/\mathcal{R} = A/\operatorname{gr}\hat{\mathcal{R}} = \operatorname{gr}(\mathbb{F}_p[\![G]\!]).$$

From this, it follows immediately that

$$U_{\operatorname{gr} G}(t) = (A/\mathcal{R})(t) = \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d}) + (t^{\sigma_1} + \ldots + t^{\sigma_m})},$$

since the sequence $\rho_1, \ldots, \rho_m$ is strongly free. This shows (iv). In order to prove statement (iii), let $\mathfrak{r} := (\rho_1, \ldots, \rho_m) \subseteq \operatorname{gr} F$ denote the ideal of the restricted Lie algebra $\operatorname{gr} F$ generated by $\rho_1, \ldots, \rho_m$ and consider the exact sequence

$$0 \longrightarrow \operatorname{gr} R/\mathfrak{r} \longrightarrow \operatorname{gr} F/\mathfrak{r} \longrightarrow \operatorname{gr} G \longrightarrow 0.$$

Passing to the universal enveloping algebras and using (1.2.6), we obtain the

commutative exact diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \mathcal{R} & = & \operatorname{gr}\hat{\mathcal{R}} & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & U_{\operatorname{gr} F} & = & \operatorname{gr}\mathbb{F}_p[\![F]\!] & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \langle \operatorname{gr} R/\mathfrak{r}\rangle & \longrightarrow & U_{\operatorname{gr} F/\mathfrak{r}} & \longrightarrow & U_{\operatorname{gr} G} & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

where $\langle \operatorname{gr} R/\mathfrak{r}\rangle \subseteq U_{\operatorname{gr} F/\mathfrak{r}}$ denotes the (two-sided) ideal generated by the image of $\operatorname{gr} R/\mathfrak{r}$. However, since $U_{\operatorname{gr} F/\mathfrak{r}} \longrightarrow U_{\operatorname{gr} G}$ is an isomorphism, it follows that $\langle \operatorname{gr} R/\mathfrak{r}\rangle = 0$ and since by (1.2.5) $\operatorname{gr} F/\mathfrak{r}$ is mapped injectively into its enveloping algebra, it follows that $\operatorname{gr} R = \mathfrak{r}$, showing (iii).

Under the identification $A/\mathcal{R} = \operatorname{gr}(\mathbb{F}_p[\![G]\!])$, the isomorphism $\mathcal{R}/\mathcal{R}I_A \cong \operatorname{gr} M$ is an isomorphism of $A/\mathcal{R}$-modules. Therefore, using the equivalent characterizations of strongly free sequences given in (1.4.6), the $\operatorname{gr}(\mathbb{F}_p[\![G]\!])$-module $\operatorname{gr} M$ is free over the initial forms of the images of the r_i. Therefore, M is a free $\mathbb{F}_p[\![G]\!]$-module over the images of the r_i, cf. [Laz65], Ch.V, Cor.2.1.1.3. This proves (ii). Applying this to the standard sequence given in (1.5.9), by (1.5.8) we conclude that $cd\, G = 2$. Furthermore,

$$h^2(G) = \dim_{\mathbb{F}_p} H^2(G) = \dim_{\mathbb{F}_p} H^1(R)^F = \dim_{\mathbb{F}_p} \operatorname{Hom}(M, \mathbb{F}_p)^F = m,$$

which yields (i).

Finally, since the sequence $\rho_1, \ldots, \rho_m$ is strongly free, by [Ani82], Lemma 3.4 it follows that the polynomial

$$\operatorname{gr}(\mathbb{F}_p[\![G]\!])(t)^{-1} = A/\mathcal{R}(t)^{-1} = 1 - (t^{\tau_1} + \ldots + t^{\tau_d}) + (t^{\sigma_1} + \ldots + t^{\sigma_m})$$

has a root in the intervall $(0, 1]$. If $m \neq d-1$, there is a root in the open intervall $(0, 1)$. By a result of M. Lazard (cf. [Laz65], App.3, Cor.3.12) it follows that G is not p-adic analytic, which shows (v) and concludes the proof. □

We want to investigate the question of inheritance of mildness. It is obivous that quotients of mild pro-p-groups are in general not mild anymore. Also in general subgroups of mild pro-p-groups need not be mild.

However, we can show that mild pro-p-groups are closed under taking free products. More precisely we have the following

(1.5.12) Proposition. *Let $G_i, i = 1, \ldots, n$ be finitely generated pro-p-groups and set $d_i = h^1(G_i)$. Suppose that for all $i \in I$, G_i is mild with respect to the Zassenhaus (x, τ^i)-filtration where $\tau^i = (\tau^i_1, \ldots, \tau^i_{d_i})$. Then the free pro-p-product*

$$G = \overset{n}{\underset{i=1}{*}} G_i$$

is mild with respect to the Zassenhaus (x,τ)-filtration where

$$\tau = (\tau_1^1, \ldots, \tau_{d_1}^1, \tau_1^2, \ldots, \tau_{d_2}^2, \ldots, \tau_1^n, \ldots, \tau_{d_n}^n).$$

Proof. Set $m_i = h^2(G_i),\ i = 1, \ldots, n$. First note that by [NSW08], Th.4.1.4 and Th.4.1.5 the restriction maps $res : H^j(G) \longrightarrow H^j(G_i)$ induce isomorphisms

$$H^j(G) \cong \bigoplus_{i=1}^n H^j(G_i),\ j \geq 0.$$

In particular, it follows that $h^1(G) = \sum_{i=1}^n d_i,\ h^2(G) = \sum_{i=1}^n m_i$ and $cd\, G \leq 2$. For $i = 1, \ldots, n$ let

$$1 \longrightarrow R_i \longrightarrow F_i \longrightarrow G_i \longrightarrow 1$$

be a minimal presentation of G_i where F_i denotes the free pro-p-group on the set $x^i = (x_1^i, \ldots, x_{d_i}^i)$ endowed with the Zassenhaus (x,τ^i)-filtration. Furthermore, by assumption R_i is generated by some elements $r_1^i, \ldots, r_{m_i}^i \in (F_i)_{(\tau^i,2)}$ such that the sequence of initial forms

$$\rho_1^i, \ldots, \rho_{m_i}^i \in \mathrm{gr}^{\tau^i}(F_i) \cong L_{res}(X^i) \subset \mathbb{F}_p\langle X^i\rangle$$

is strongly free where $X^i = \{X_1^i, \ldots, X_{d_i}^i\}$. Let $F \cong \overset{n}{\underset{i=1}{*}} F_i$ be the free pro-p-group on $x_1^1, \ldots, x_{d_1}^1, x_1^2, \ldots, x_{d_2}^2, \ldots, x_1^n, \ldots, x_{d_n}^n$ endowed with the Zassenhaus (x,τ)-filtration where $\tau = (\tau_1^1, \ldots, \tau_{d_1}^1, \tau_1^2, \ldots, \tau_{d_2}^2, \ldots, \tau_1^n, \ldots, \tau_{d_n}^n)$. Then $G = \overset{n}{\underset{i=1}{*}} G_i$ possesses a minimal presentation

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

where R denotes the closed normal subgroup of F generated by the images of $r_1^1, \ldots, r_{m_1}^1, r_1^2, \ldots, r_{m_2}^2, \ldots, r_1^n, \ldots, r_{m_n}^n$. Now by (1.4.8) it follows that the sequence of initial forms

$$\bigcup_{i=1}^n \{\rho_1^i, \ldots, \rho_{m_i}^i\} \subset \mathrm{gr}^\tau(F) \cong L_{res}(X) \subset \mathbb{F}_p\langle X\rangle$$

is strongly free where $X = \bigcup_{i=1}^n X^i$. Therefore, by definition G is mild with respect to the Zassenhaus (x,τ)-filtration. □

(1.5.13) Remark. With a view towards our applications involving higher Massey products, we consider finitely presented pro-p-groups only. However, the notion of strong freeness is neither restricted to finitely generated $\mathbb{F}_p$-algebras nor to finite sequences, whereas it is of course a crucial assumption to work with graded algebras that are locally finite. For instance, if A is the free associative graded algebra on the countable set $X = \{X_1, \ldots, X_n, \ldots\}$ with weights $\tau_n \to \infty$ and $\rho = \{\rho_1, \ldots, \rho_n, \ldots\}$ is a sequence of homogeneous polynomials

of degrees $\sigma_n \to \infty$, it makes sense to ask whether the Poincaré series of the quotient algebra satisfies the condition (1.4.3) for strong freeness and the main results such as Anick's criterion (1.4.14) carry over, cf. [Ani82]. This makes it possible to extend the notion of mildness to pro-p-groups of countably infinite generator rank with respect to p-restricted filtrations with weights tending to infinity and as in the case of finitely generated groups these groups are of cohomological dimension 2.

2 Mild pro-p-groups and Massey products

2.1 Pro-p-groups with relations of degree 3

We want to consider finitely presented pro-p-groups G that admit a minimal presentation

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

such that $R \subseteq F_{(3)}$. Before giving a sufficient criterion for such groups to be mild, we deduce the following fact from the results obtained in the first chapter:

(2.1.1) Lemma. *Let F be the free pro-p-group on $x = \{x_1, \dots, x_d\}$. Then the following holds:*

(i) *Every element $f \in F_{(3)}$ may be uniquely written in the form*

$$f \equiv \begin{cases} \prod\limits_{\substack{1\le i<j\le d,\\ 1\le k\le j}} [[x_i,x_j],x_k]^{a_{ijk}} \mod F_{(4)}, & \text{if } p \neq 3, \\ \prod\limits_{1\le i\le d} x_i^{3a_i} \cdot \prod\limits_{\substack{1\le i<j\le d,\\ 1\le k\le j}} [[x_i,x_j],x_k]^{a_{ijk}} \mod F_{(4)}, & \text{if } p = 3 \end{cases}$$

with $a_i, a_{ijk} \in \mathbb{F}_p$.

(ii) *Let $f \in F_{(3)} \setminus F_{(4)}$ and the coefficients $a_i, a_{ijk} \in \mathbb{F}_p$ be given as in* (i). *Then the initial form $\overline{f} \in \mathrm{gr}(F) \cong L_{res}(X_1, \dots, X_d)$ of f is given by*

$$\overline{f} = \begin{cases} \sum\limits_{\substack{1\le i<j\le d,\\ 1\le k\le j}} a_{ijk}[[X_i,X_j],X_k], & \text{if } p \neq 3, \\ \sum\limits_{1\le i\le d} a_i X_i^3 + \sum\limits_{\substack{1\le i<j\le d,\\ 1\le k\le j}} a_{ijk}[[X_i,X_j],X_k], & \text{if } p = 3. \end{cases}$$

Proof. Statement (i) follows directly from (1.3.11). In fact, a basis of $F_{(3)}/F_{(4)}$ is given by

$$\overline{B}_3 = \begin{cases} B_3, & \text{if } p \neq 3, \\ B_3 \cup B_1^3, & \text{if } p = 3 \end{cases}$$
$$\text{where } B_3 = \{[[x_i,x_j],x_k] \mid 1 \le i < j \le d, 1 \le k \le j\},$$

see also example (1.3.13). If $f \in F_{(3)} \setminus F_{(4)}$, we have $\overline{f} \in \mathrm{gr}_3(F)$ and we deduce (ii) immediately by recalling the definition of the restricted Lie algebra structure

on $\mathrm{gr}(F)$ (cf. (1.2.14)) and the isomorphism of graded restricted Lie algebras $\mathrm{gr}(F) \cong L_{res}(X)$ where $L_{res}(X_1, \ldots, X_d) \subset \mathbb{F}_p\langle X_1, \ldots, X_d\rangle$ is endowed with natural grading (cf. (1.3.8)). □

The following result is an analogue of a theorem obtained by A. Schmidt (cf. [Sch06], Th.5.5), where relations of degree 2 are considered. As for Schmidt's theorem, in the following proof we can make use of Labute's criterion for strongly free sequences of Lie type (at least if $p \neq 3$). For relations of degrees > 3 applying the same method would be a lot more involved, since the structure of the basic commutators becomes quite unhandy. We will prove a generalization for relations of arbitrary constant degree in the third section of this chapter by applying a different method based on Anick's criterion.

(2.1.2) Theorem. *Let F be the free pro-p-group on generators $x_1, \ldots, x_d$. Let $r_1, \ldots, r_m \in F_{(3)}$ and let $a_i^n, a_{ijk}^n \in \mathbb{F}_p$ be defined by*

$$r_n \equiv \begin{cases} \displaystyle\prod_{\substack{1\le i<j\le d,\\ 1\le k\le j}} [[x_i, x_j], x_k]^{a_{ijk}^n} \mod F_{(4)}, & \text{if } p \neq 3, \\ \displaystyle\prod_{1\le i\le d} x_i^{3a_i^n} \cdot \prod_{\substack{1\le i<j\le d,\\ 1\le k\le j}} [[x_i, x_j], x_k]^{a_{ijk}^n} \mod F_{(4)}, & \text{if } p = 3. \end{cases} \tag{2.1}$$

Suppose that there exists a natural number c, $1 \le c < d$ such that the following conditions hold:

(i) $a_{ijk}^n = 0$ *if* $c < i < j, c < k \le j$ *and* $1 \le n \le m$,

(ii) *The* $m \times c\binom{d-c+1}{2}$*-matrix*

$$(a_{ijk}^n)_{n,(ijk)}, \quad 1 \le n \le m,\ 1 \le i \le c < k \le j$$

has rank m.

(iii) *If $p = 3$, then $a_i^n = 0$ if $c < i$ and $1 \le n \le m$.*

Then $G := F/R$ is a mild pro-p-group with respect to the Zassenhaus filtration where R denotes the normal subgroup of F generated by the r_i. In particular, it holds that $h^1(G) = d, h^2(G) = m$ and $\mathrm{cd}\, G = 2$.

Proof. Let $X = \{X_1, \ldots, X_d\}$ and let $\rho_n \in \mathrm{gr}(F) \cong L_{res}(X) \subset \mathbb{F}_p\langle X\rangle$ denote the initial form of r_n, $i = 1, \ldots, n$. We show that $\rho_1, \ldots, \rho_m$ is a strongly free sequence. First note that by condition (ii) for all n we have $a_{ijk}^n \neq 0$ for at least one triple (i, j, k) satisfying $1 \le i \le c < k \le j$. In particular, $\rho_n \in \mathrm{gr}_3(F)$ and therefore

$$\rho_n = \begin{cases} \displaystyle\sum_{\substack{1\le i<j\le d,\\ 1\le k\le j}} a_{ijk}^n [[X_i, X_j], X_k], & \text{if } p \neq 3, \\ \displaystyle\sum_{1\le i\le d} a_i^n X_i^3 + \sum_{\substack{1\le i<j\le d,\\ 1\le k\le j}} a_{ijk}^n [[X_i, X_j], X_k], & \text{if } p = 3, \end{cases}$$

$n = 1, \ldots, m$.

First suppose $p \neq 3$. Since the ρ_n lie in the free Lie subalgebra $L(X)$ of $L_{res}(X)$, we can make use of Labute's criterion (1.4.22) to show that $\rho_1, \ldots, \rho_m$ is a strongly free sequence in L. Let $S = \{X_{c+1}, \ldots, X_d\}$, $\mathfrak{a} \subseteq L$ be the ideal generated by $\{X_1, \ldots, X_c\}$ and B the enveloping algebra of $L/\mathfrak{a} = L(S)$. Furthermore, let

$$T = \{[[X_i, X_j], X_k] \big| \ 1 \leq i \leq c, \ c < k \leq j \leq d\} \subseteq \mathfrak{a}.$$

Since $\mathfrak{a}/[\mathfrak{a}, \mathfrak{a}]$ is a free B-module with a basis consisting of the images of $\xi_1, \ldots, \xi_c$, it follows that T is B-linearly independent modulo $[\mathfrak{a}, \mathfrak{a}]$. Now by condition (i) and since $[[\xi_i, \xi_j], \xi_k] \in [\mathfrak{a}, \mathfrak{a}]$ if $i \leq j \leq c$ or $i \leq c < j, \ k \leq c$, the elements ρ_i lie in the $\mathbb{F}_p$-span of T modulo $[\mathfrak{a}, \mathfrak{a}]$ and by condition (ii) are $\mathbb{F}_p$-linearly independent modulo $[\mathfrak{a}, \mathfrak{a}]$. Hence (1.4.22) applies and we conclude that $\rho_1, \ldots, \rho_m$ is a strongly free sequence.

In order to deal with the slightly more difficult case $p = 3$, we apply Forré's theorem (1.4.20) by endowing $L_{res}(X)$ with the (X, τ')-grading where

$$\tau_i' = \begin{cases} 2, & \text{if } i \leq c, \\ 1, & \text{if } i > c. \end{cases}$$

Then ρ_n decomposes as

$$\rho_n = \rho_{n,1} + \rho_{n,2} + \rho_{n,3}$$

where

$$\begin{aligned}
\rho_{n,1} &= \sum_{c<i\leq d} a_i^n X_i^3 + \sum_{\substack{c<i<j\leq d \\ 1 \leq k \leq j}} a_{ijk}^n [[X_i, X_j], X_k], \\
\rho_{n,2} &= \sum_{1\leq i\leq c} a_i^n X_i^3 + \sum_{\substack{1\leq i\leq c<j\leq d \\ 1 \leq k \leq c}} a_{ijk}^n [[X_i, X_j], X_k] \\
&\quad + \sum_{\substack{1\leq i<j\leq c\leq d \\ 1 \leq k \leq j}} a_{ijk}^n [[X_i, X_j], X_k], \\
\rho_{n,3} &= \sum_{1\leq i\leq c<k\leq j\leq d} a_{ijk}^n [[X_i, X_j], X_k].
\end{aligned}$$

By conditions (i) and (iii) we have $\rho_{n,1} = 0$ for all n. Furthermore, $\deg^{\tau'}(\rho_{n,2}) \geq 5$ and $\deg^{\tau'}(\rho_{n,3}) = 4$, noting that condition (iii) implies $\rho_{n,3} \neq 0$. Hence by (1.4.20) it is sufficient to show that the sequence $\rho_{1,3}, \ldots, \rho_{m,3}$ is strongly free. This follows as in the case $p \neq 3$, which concludes the proof. □

(2.1.3) Remarks.

(i) Note that condition (ii) implies that the relations $r_1, \ldots, r_m$ are linearly independent modulo $F_{(4)}$. If this is not the case, G can still be mild. However, in order to give criteria for mildness in these cases, more information about the relations is required, e.g. some conditions on $r_i \bmod F_{(5)}$.

(ii) It can be easily checked that the conditions (i)-(iii) in (2.1.2) are actually independent of the choice of a minimal system of defining relations. However, a priori they depend on the choice of the system $\{x_1, \ldots, x_d\}$ of free generators of F. In the third section of this chapter we will give a purely cohomological (and even slightly stronger) formulation of the above theorem, i.e. we formulate analogous conditions only involving the cohomology groups $H^i(G, \mathbb{Z}/p\mathbb{Z})$, $i = 1, 2$ (cf. (2.3.2)).

(2.1.4) Example. Let p be arbitrary. Let F be the free pro-p-group on x_1, x_2, x_3 and R be the normal subgroup of F generated by r_1, r_2, r_3 where

$$\begin{aligned} r_1 &= x_1^p \cdot [[x_1, x_3], x_2], \\ r_2 &= x_1^p \cdot [[x_1, x_2], x_2], \\ r_3 &= x_1^p \cdot [[x_1, x_3], x_3]. \end{aligned}$$

We claim that $G = F/R$ is mild. If $p > 2$, (2.1.2) applies with $c = 1$ and hence $G = F/R$ is mild with respect to the Zassenhaus filtration. In the case $p = 2$, G cannot be mild with respect to the Zassenhaus filtration, since there is no mild pro-p-group G with respect to the Zassenhaus filtration satisfying $h^1(G) = h^2(G) = 3$ where the generating relations in a minimal presentation of G are of degree 2, cf. (1.4.10). Instead we consider the (x, τ)-filtration on F where $\tau_1 = 3$, $\tau_2 = \tau_3 = 1$. Then the sequence of initial forms $\rho_i \in \mathrm{gr}^\tau(F) \cong L_{res}(X)$ of the r_i is given by the strongly free sequence

$$\begin{aligned} \rho_1 &= [[X_1, X_3], X_2] \in \mathrm{gr}_5^\tau(F), \\ \rho_2 &= [[X_1, X_2], X_2] \in \mathrm{gr}_5^\tau(F), \\ \rho_3 &= [[X_1, X_3], X_3] \in \mathrm{gr}_5^\tau(F). \end{aligned}$$

Hence G is mild with respect to the Zassenhaus (x, τ)-filtration.

2.2 Massey products and applications to the cohomology of pro-p-groups

In this section we recall the notion of **Massey products**, which have been introduced by W.S. Massey as higher analogues of the cup product in algebraic topology (cf. [Mas58]). After quickly recalling the basic definitions and properties, we cite an important application to the cohomology of finitely presented pro-p-groups: As noticed by H. Koch, there is a close relation between higher Massey products and relations lying in higher Zassenhaus filtration steps, cf. the remark in [Koc78], p.109. The exact results we use here have been proven independently by D. Vogel and M. Morishita ([Vog04] and [Mor04]). This connection will enable us to prove a much more general version of (2.1.2) in the next section.

Massey products can be studied in a context as general as the cohomology of complexes, i.e. they can be defined for various cohomology theories (e.g.

see [Kra66], [May69] and [Den95]). For the applications we have in mind, we introduce them for group cohomology with trivial modules as coefficients.

Let G be a profinite group, A be a trivial discrete G-module and denote by $\mathcal{C}^*(G,A)$ the standard inhomogeneous cochain complex (e.g. see [NSW08], Ch.I, §2).*)

(2.2.1) Definition. *Let $n \geq 2$ and $\alpha_1, \ldots, \alpha_n \in H^1(G,A)$. We say that the* ***n*-th Massey product $\langle \alpha_1, \ldots, \alpha_n \rangle$** *is* **defined** *if there is a collection*

$$\mathcal{A} = \{a_{ij} \in \mathcal{C}^1(G,A) \mid 1 \leq i,j \leq n,\ (i,j) \neq (1,n)\}$$

(called a **defining system** *for $\langle \alpha_1, \ldots, \alpha_n \rangle$), such that the following conditions hold:*

(i) *a_{ii} is a representative of the cohomology class α_i, $1 \leq i \leq n$.*

(ii) *For $1 \leq i < j \leq n$, $(i,j) \neq (1,n)$ it holds that*

$$\delta^2(a_{ij}) = \sum_{l=i}^{j-1} a_{il} \cup a_{(l+1)j}.^{**)}$$

If $\mathcal{A}$ is a defining system for $\langle \alpha_1, \ldots, \alpha_n \rangle$, we consider the 2-cocycle

$$b_{\mathcal{A}} = \sum_{l=1}^{n-1} a_{1l} \cup a_{(l+1)n}$$

and denote its class in $H^2(G,A)$ by $\langle \alpha_1, \ldots, \alpha_n \rangle_{\mathcal{A}}$. We set

$$\langle \alpha_1, \ldots, \alpha_n \rangle = \bigcup_{\mathcal{A}} \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathcal{A}}$$

where $\mathcal{A}$ runs over all defining systems. The Massey product $\langle \alpha_1, \ldots, \alpha_n \rangle$ is called **uniquely defined** *if $\#\langle \alpha_1, \ldots, \alpha_n \rangle = 1$. The n-th Massey product is* **uniquely defined for (G,A)** *if $\langle \alpha_1, \ldots, \alpha_n \rangle$ is uniquely defined for all $\alpha_1, \ldots, \alpha_n \in H^1(G,A)$.*

It can be shown that the n-th Massey product is uniquely defined if the Massey products of lower order are uniquely defined and identically zero, i.e. we have the following

(2.2.2) Proposition. *Let $n \geq 2$ and $\alpha_1, \ldots, \alpha_n \in H^1(G,A)$.*

(i) *For $n = 2$ the Massey product $\langle \alpha_1, \alpha_2 \rangle$ is uniquely defined and given by the cup-product, i.e.*

$$\langle \alpha_1, \alpha_2 \rangle = \alpha_1 \cup \alpha_2.$$

*) We will be mainly interested in the case where G is a pro-p-group and $A = \mathbb{Z}/p\mathbb{Z}$.

**) As usual δ^2 denotes the coboundary operator $\delta^2 : \mathcal{C}^1(G,A) \longrightarrow \mathcal{C}^2(G,A)$.

(ii) *Let $n \geq 2$. Assume that for all $2 \leq l < n$ and all $\alpha_1, \ldots, \alpha_l$ the l-th Massey product $\langle \alpha_1, \ldots, \alpha_l \rangle = 0$ is uniquely defined and given by the zero class in $H^2(G, A)$. Then for all $\beta_1, \ldots, \beta_n \in H^1(G, A)$ the n-th Massey product $\langle \beta_1, \ldots, \beta_n \rangle$ is also uniquely defined and yields a multilinear map (of $\mathbb{Z}$-modules)*

$$\langle \cdot, \ldots, \cdot \rangle : H^1(G, A)^n \longrightarrow H^2(G, A).$$

Proof. Statement (i) follows immediately from the definition. For a proof of (ii) see [Kra66], Lemma 20 and [Fen83], Lemma 6.2.4. □

It is not surprising that higher Massey products satisfy the same functoriality properties as the cup-product, provided they are uniquely defined.

(2.2.3) Proposition. *Suppose that G is a profinite group, $G' \subseteq G$ is a closed subgroup and G'' is a quotient of G. Let A be a trivial G-module and $n \geq 2$. Then the following holds:*

(i) *If the n-th Massey product is uniquely defined for (G, A) and (G'', A), then*

$$inf\, \langle \alpha_1, \ldots, \alpha_n \rangle = \langle inf\, \alpha_1, \ldots, inf\, \alpha_n \rangle$$

for $\alpha_1, \ldots, \alpha_n \in H^1(G'', A)$.

(ii) *If the n-th Massey products is uniquely defined for (G, A) and (G', A), then*

$$res\, \langle \alpha_1, \ldots, \alpha_n \rangle = \langle res\, \alpha_1, \ldots, res\, \alpha_n \rangle$$

for $\alpha_1, \ldots, \alpha_n \in H^1(G, A)$.

(iii) *If the n-th Massey products is uniquely defined for (G, A) and (G', A), then*

$$cor\, \langle \alpha_1, \ldots, \alpha_n \rangle = \langle cor\, \alpha_1, \ldots, cor\, \alpha_n \rangle$$

for $\alpha_1, \ldots, \alpha_n \in H^1(G', A)$.

Proof. This follows almost immediately from the definitions. We sketch the argument of the first statement, the other statements can be shown in the same way. Let

$$\mathcal{A}'' = \{a_{ij} \in \mathcal{C}^1(G'', A) \mid 1 \leq i, j \leq n,\ (i, j) \neq (1, n)\}$$

be a defining system for $\langle \alpha_1, \ldots, \alpha_n \rangle$. Since the inflation maps commute with the cup-product and the δ-homomorphisms on the level of cochains, it follows that the set

$$\mathcal{A} := \{(inf\, a_{ij}) \in \mathcal{C}^1(G, A) \mid 1 \leq i, j \leq n,\ (i, j) \neq (1, n)\}$$

is a defining system for $\langle inf\, \alpha_1, \ldots, inf\, \alpha_n \rangle$. For the same reason we have

$$\begin{aligned} b_{\mathcal{A}} &= \sum_{l=1}^{n-1} inf\, a_{1l} \cup inf\, a_{(l+1)n} \\ &= inf\, \big(\sum_{l=1}^{n-1} a_{1l} \cup a_{(l+1)n} \big) \\ &= inf\, b_{\mathcal{A}''}. \end{aligned}$$

Since the n-th Massey product is uniquely defined for both (G, A) and (G'', A), this yields

$$inf\,\langle\alpha_1,\ldots,\alpha_n\rangle = \langle inf\,\alpha_1,\ldots,inf\,\alpha_n\rangle.$$

□

Now assume that G is a finitely presented pro-p-group. Let $d = h^1(G)$ and

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

be a minimal presentation of G where F is a free pro-p-group on generators $x_1,\ldots,x_d$. Let $\chi_1,\ldots,\chi_d \in H^1(F) = H^1(G)$ be the dual basis corresponding to $x_1,\ldots,x_d$.*) The five term exact sequence yields the isomorphism

$$tg:\ H^1(R)^G \xrightarrow{\sim} H^2(G).$$

Hence every element $r \in R$ gives rise to the **trace map**

$$tr_r:\ H^2(G) \longrightarrow \mathbb{F}_p,$$

$$\varphi \longmapsto (tg^{-1}\varphi)(r).$$

Clearly, if $r_1,\ldots,r_m$ is a minimal system of defining relations, i.e. a minimal system of generators of R as closed normal subgroup of F, then $tr_{r_1},\ldots,tr_{r_m}$ is a basis of $H^2(G)^\vee$.

Recall that we have the topological isomorphism

$$\mathbb{F}_p[\![F]\!] \xrightarrow{\sim} \mathbb{F}_p\langle\langle X\rangle\rangle,\ x_i \longmapsto 1 + X_i.$$

By $\psi : F \hookrightarrow \mathbb{F}_p\langle\langle X\rangle\rangle$ we denote the composite of the map

$$F \hookrightarrow \mathbb{F}_p[\![F]\!],\ f \longmapsto f - 1,$$

with the above isomorphism, mapping F into the augmentation ideal of $\mathbb{F}_p\langle\langle X\rangle\rangle$. We need the following notation:

(2.2.4) Definition.

(i) *A* **multi-index** *I of height d and length $|I| = k$ is a tuple of elements $I = (i_1,\ldots,i_k) \in \mathbb{N}^k$ where k is a natural number and $1 \le i_j \le d$ for $1 \le j \le k$. We denote by $\mathcal{M}_d^k$ the set of all multi-indices of height d and length k.*

(ii) *For any multi-index I we define the continuous map $\varepsilon_{I,p} : F \to \mathbb{F}_p$ by*

$$\psi(f) = \sum_I \varepsilon_{I,p}(f) X_I$$

*where I runs over all multi-indices of height d and X_I denotes the monomial $X_I = X_{i_1}\cdots X_{i_l}$ for any $I = (i_1,\ldots,i_l)$.***)

*) Recall that for a pro-p-group G we set $H^i(G) := H^i(G, \mathbb{Z}/p\mathbb{Z})$.

) The sum $\sum_I \varepsilon_I(f)X_I$ is also called **Magnus expansion of f.

By definition we have $f \in F_{(n)},\ n \geq 1$ if and only if $\varepsilon_{I,p}(f) = 0$ for all multi-indices I of length $|I| < n$. We can now state the important

(2.2.5) Theorem. *Let G be a finitely presented pro-p-group and*

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

be a minimal presentation. Assume that $R \subseteq F_{(n)}$ for some $n \geq 2$. Then for all $k \leq n$ the k-th Massey product

$$\langle \cdot, \ldots, \cdot \rangle : H^1(G)^k \longrightarrow H^2(G),\ 1 < k \leq n$$

is uniquely defined. Furthermore, for all multi-indices I of height d and length $1 < |I| \leq n$ we have the equality

$$\varepsilon_{I,p}(r) = (-1)^{|I|-1} tr_r \langle \chi_I \rangle$$

for all $r \in R$ where for $I = (i_1, \ldots, i_k)$ we have set $\chi_I = (\chi_{i_1}, \ldots, \chi_{i_k}) \in H^1(G)^k$. In particular, for $1 < k < n$ the k-th Massey product on $H^1(G)$ is identically zero.

For a proof we refer to [Vog04], Prop.1.2.6.

As a special case we obtain the well-known result:

(2.2.6) Corollary. *For a finitely presented pro-p-group G the following assertions are equivalent:*

(i) *For any minimal presentation $1 \to R \to F \to G \to 1$ of G, we have $R \subseteq F_{(3)}$.*

(ii) *The cup-product $H^1(G) \times H^1(G) \stackrel{\cup}{\to} H^2(G)$ is identically zero.*

By (2.2.5), the n-fold Massey product is uniquely determined by the Magnus expansions of a minimal system of defining relations if $R \subseteq F_{(n)}$. The maps $\varepsilon_{I,p}(\cdot)$ satisfy certain symmetry properties which immediately carry over to the Massey products. To make this fact more precise, we need the notion of so-called **shuffles** of multi-indices.

(2.2.7) Definition. *Let $I = (i_1, \ldots, i_k)$ and $J = (j_1, \ldots, j_l)$ be multi-indices of lengths k and l respectively. A multi-index $S = (s_1, \ldots, s_{l+k})$ of length $l + k$ is called* **proper shuffle** *of I and J if there is a partition of $1, \ldots, k + l$ into sequences*

$$1 \leq \alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_l \leq l + k,\ 1 \leq \beta_1 \leq \beta_2 \leq \ldots \leq \beta_k \leq l + k$$

satisfying $\alpha_n \neq \beta_m$ for all m, n such that $s_{\alpha_n} = i_n,\ n = 1, \ldots, l$ and $s_{\beta_m} = j_m,\ m = 1, \ldots, k$. We denote by $\mathcal{S}(I, J)$ the set of all proper shuffles of I, J.

Keeping the assumptions of (2.2.5) (in particular, $R \subseteq F_{(n)}$), the n-fold Massey product satisfies the following **shuffle relations**:

(2.2.8) Proposition. *Let $I = (i_1, \dots, i_k)$ and $J = (j_1, \dots, j_l)$ be multi-indices of height d and lengths $k, l > 1$ respectively such that $l + k = n$. Furthermore, let $\xi_{i_1}, \dots, \xi_{i_k}, \xi_{j_1}, \dots \xi_{j_l} \in H^1(G)$. Then we have*

$$\sum_{S \in \mathcal{S}(I,J)} \langle \xi_S \rangle = 0$$

where for $S = (s_1, \dots, s_n) \in \mathcal{S}(I, J)$ we have set $\xi_S = (\xi_{s_1}, \dots, \xi_{s_n}) \in H^1(G)^n$.

Proof. This follows from analogous relations of the maps $\varepsilon_{I,p}(\cdot)$, see [Vog04], Prop.1.1.29 and Cor.1.2.10 for details. □

Note that if $I = (1)$, $J = (2)$, we have $\mathcal{S}(I, J) = \{(1, 2), (2, 1)\}$. Hence for $n = 2$ the shuffle relation yields $\langle \xi_1, \xi_2 \rangle + \langle \xi_2, \xi_1 \rangle = 0$, which is just the skew-commutativity of the cup product. If $n = 3$, the shuffle relations of the triple Massey product are generated by the two relations

$$\langle \xi_1, \xi_2, \xi_3 \rangle + \langle \xi_2, \xi_3, \xi_1 \rangle + \langle \xi_3, \xi_1, \xi_2 \rangle = 0, \quad \langle \xi_1, \xi_2, \xi_3 \rangle = \langle \xi_3, \xi_2, \xi_1 \rangle \tag{2.2}$$

for all $\xi_1, \xi_2, \xi_3 \in H^1(G)$ (cf. [Vog04], Ex.1.2.11).

We conclude this section by investigating the link between the basis of $F_{(3)}/F_{(4)}$ and the triple Massey product.

(2.2.9) Corollary.
Let $G = F/R$ be a finitely presented pro-p-group such that $R \subseteq F_{(3)}$. Let R be generated by $r_1, \dots, r_m$ as a normal subgroup of F where

$$r_n \equiv \begin{cases} \prod\limits_{\substack{1 \le i < j \le d, \\ 1 \le k \le j}} [[x_i, x_j], x_k]^{a^n_{ijk}} \mod F_{(4)}, & \text{if } p \neq 3, \\ \prod\limits_{1 \le i \le d} x_i^{3a_i^n} \cdot \prod\limits_{\substack{1 \le i < j \le d, \\ 1 \le k \le j}} [[x_i, x_j], x_k]^{a^n_{ijk}} \mod F_{(4)}, & \text{if } p = 3 \end{cases}$$

for $n = 1, \dots, m$ with $a_i^n, a_{ijk}^n \in \mathbb{F}_p$. Then we have the identities

$$tr_{r_n} \langle \chi_j, \chi_i, \chi_k \rangle = \begin{cases} -a^n_{ijk}, & \text{if } i < j, k < j, \\ a^n_{kjj}, & \text{if } k < j, i = j, \\ 0, & \text{if } i = j = k, p \neq 3 \\ a_i^n, & \text{if } i = j = k, p = 3. \end{cases}$$

Proof. This follows by evaluating the maps $\varepsilon_{I,p}(\cdot)$ at the basic commutators and applying (2.2.5). For a more detailed proof see [Vog04], Prop.1.3.3. □

Note that via formula (2.2) it follows that the triple Massey product is completely determined by the coefficients $a_i^n, a_{ijk}^n, n = 1, \dots, m$. The above corollary is therefore an analogue of [NSW08], Th.3.9.13, where it is shown that the cup product is determined by the exponents of the basic commutators $[x_i, x_j]$ and the squares x_i^2 (if $p = 2$) in the relations r_n.*) It is clear that if $R \subseteq F_{(n)}$, by

*) This well-known fact is usually formulated in terms of the lower q-central series for some power q of p, but it immediately carries over to the Zassenhaus filtration.

(2.2.5) analogous results can be stated relating the basis of $F_{(n)}/F_{(n+1)}$ given in (1.3.11) with the n-th Massey product. However, for higher degrees the relation between Massey products and basic commutators becomes quite unhandy. Fortunately we don't have do calculations with basic commutators in order to prove a criterion for mildness using higher Massey products.

2.3 A cohomological criterion for mildness

We introduce the following invariant of a finitely presented pro-p-group G:

(2.3.1) Definition. *Let G be a finitely presented pro-p-group. We define the* **Zassenhaus invariant** $\mathfrak{z}(G) \in \mathbb{N} \cup \{\infty\}$ *to be the supremum of all natural numbers $n \in \mathbb{N}$ satisfying one (and hence all) of the following equivalent conditions:*

(i) *If $1 \to R \to F \to G \to 1$ is a minimal presentation of G, then $R \subseteq F_{(n)}$.*

(ii) *If $1 \to R \to F \to G \to 1$ is a minimal presentation of G, then the induced homomorphism of graded restricted Lie algebras $\operatorname{gr} G \twoheadrightarrow \operatorname{gr} F$ is injective in degrees $< n$.*

(iii) *The k-fold Massey product $H^1(G)^k \to H^2(G)$ is uniquely defined and identically zero for $2 \leq k < n$.*

The equivalence (i)⇔(ii) is clear from the definition and (i)⇔(iii) is a direct consequence of (2.2.5). Obviously by definition we have $\mathfrak{z}(G) \geq 2$. Furthermore, $\mathfrak{z}(G) = \infty$ if and only if G is free. The following theorem generalizes the cup-product criterion for mildness by A. Schmidt (cf. [Sch10], Th.6.2):

(2.3.2) Theorem. *Let p be a prime number and G a finitely presented pro-p-group with Zassenhaus invariant $\mathfrak{z}(G) = n < \infty$. Assume that $H^1(G)$ admits a decomposition $H^1(G) = U \oplus V$ as $\mathbb{F}_p$-vector space such that for some natural number e with $1 \leq e \leq n-1$ the n-fold Massey product $\langle \cdot, \ldots, \cdot \rangle : H^1(G)^n \longrightarrow H^2(G)$ satisfies the following conditions:*

(a) *We have $\langle \xi_1, \ldots, \xi_n \rangle = 0$ for all tuples $(\xi_1, \ldots, \xi_n) \in H^1(G)^n$ such that $\#\{i \mid \xi_i \in V\} \geq n - e + 1$.*

(b) *$\langle \cdot, \ldots, \cdot \rangle$ maps*

$$U^{\otimes e} \otimes V^{\otimes n-e}$$

surjectively onto $H^2(G)$.

Then G is mild with respect to the Zassenhaus filtration. In particular, G is of cohomological dimension $\operatorname{cd} G = 2$.

Proof. We set $d = h^1(G)$, $m = h^2(G)$ and $c = \dim_{\mathbb{F}_p} U$. Furthermore, we choose bases $\chi_1, \ldots, \chi_c$ and $\chi_{c+1}, \ldots, \chi_d$ of U and V respectively. Let $\overline{x}_1, \ldots, \overline{x}_d \in G$ be arbitrary lifts of the dual basis of $\chi_1, \ldots, \chi_d$ in $H_1(G) = G/G^p[G,G]$. Then G admits a minimal presentation

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G \longrightarrow 1$$

where F is the free pro-p-group on generators $x_1, \ldots, x_d$ and π maps x_i to $\overline{x}_i$. As usual, we make the identification $\operatorname{gr} F \cong L_{res}(X) \subset \mathbb{F}_p\langle X\rangle$ where $X = \{X_1, \ldots, X_d\}$, mapping the initial form of x_i to X_i. Let $<$ denote the natural order on X, i.e. $X_1 < X_2 < \ldots X_d$. We order the set of monomials by the multiplicative order $<_U$ introduced in (1.4.18) where by abuse of notation we denote the subset $\{X_1, \ldots, X_c\} \subset X$ also by U. Consider the following subset of the set $\mathcal{M}_d^n$ of multi-indices of height d and length n:

$$B = \{(i_1, \ldots, i_n) \in \mathcal{M}_d^n |\ i_1, \ldots, i_e \leq c \text{ and } i_{e+1}, \ldots, i_n > c\}.$$

Note that $b := \#B = \dim_{\mathbb{F}_p}(U^{\otimes e} \otimes V^{\otimes n-e}) = c^e(d-c)^{n-e}$. Since by condition (b) the homomorphism $\varphi : U^{\otimes e} \otimes V^{\otimes n-e} \longrightarrow H^2(G)$ is surjective, there exists a basis $C = \{y_1, \ldots, y_m\}$ of $H^2(G)$, such that the transformation matrix of φ with respect to the bases

$$\mathcal{B} = \{\chi_{i_1} \otimes \cdots \otimes \chi_{i_n} \mid (i_1, \ldots, i_n) \in B\}$$

(which we order via $<_U$) and C is of the form

$$M = \begin{pmatrix} 0 & \cdots & 0 & 1 & * & \cdots & * & * & * & \cdots & * & \cdots & * & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & * & \cdots & * & \cdots & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & 1 & * & \cdots & * \end{pmatrix}. \quad (2.3)$$

In fact, first choose an arbitrary basis of $H^2(G)$ and transform the corresponding matrix M' of φ into row echelon form by applying elementary row operations, noting that $\operatorname{rank} M' = m$. For $1 \leq j \leq m$ and $I \in B$ we denote by $m_{j,I}$ the coefficient in the j-th row and the column corresponding to I of M. We choose $r_1, \ldots, r_m \in R$ such that for $1 \leq j \leq m$ the image $\overline{r}_j$ of r_j in $R/R^p[F,R]$ is dual to $tg^{-1}(y_i) \in H^1(R)^G = (R/R^p[F,R])^\vee$ where again tg denotes the transgression isomorphism

$$tg:\ H^1(R)^G \xrightarrow{\sim} H^2(G).$$

Hence, $r_1, \ldots, r_m$ is a minimal system of defining relations of G and the trace map $tr_{r_j} \in H^2(G)^\vee$ is the linear form dual to y_j. Let $\rho_j \in \operatorname{gr} F$ be the initial form of r_j. We claim that the sequence $\rho_1, \ldots, \rho_m$ is strongly free. Since $\mathfrak{z}(G) = n$, by (2.2.5) and the definition of the matrix $M = (m_{j,I})$, we have

$$\varepsilon_{I,p}(r_j) = (-1)^{|I|-1} tr_{r_j}\langle\chi_I\rangle = (-1)^{|I|-1} m_{j,I}, \text{ for all } 1 \leq j \leq m,\ I \in B.$$

First note that since every row of M is non-zero, this implies $\rho_j \in gr_n F$, i.e. the ρ_j are homogeneous polynomials of degree n. By condition (a) it follows that

$$\varepsilon_{I,p}(r_j) = (-1)^{|I|-1} tr_{r_j}\langle\chi_I\rangle = 0$$

for $1 \leq j \leq m$ and any multi-index $I = (i_1, \ldots, i_n)$ such that $\#\{k \mid i_k > c\} \geq n - e + 1$ which is equivalent to $\#\{k \mid i_k \leq c\} \leq e - 1$. That is, every

monomial of ρ_j contains at least e factors $X_i,\ i \le c$.*) Since the monomials in $X_I, I \in B$ have the property that the $X_i, i > c$ are on the right end, by definition of the ordering $<_U$ (cf. (1.4.18)) we conclude that the high terms m_j of the ρ_j with respect to $<_U$ are monomials of the form $m_j = X_{I_j}$ for some I_j in B. Furthermore, taking into account that the matrix M is in row echelon form (2.3), we see that the m_j are pairwise distinct. In particular, no m_j is contained in an m_k for $1 \le j, k \le m,\ j \ne k$ and since they begin (from the left) with e variables $X_i, i \le c$ and end with $n-e$ variables $X_i, i > c$, the beginning of m_j is never the ending of m_k for $1 \le j, k \le m$. In other words, the sequence $m_1, \dots, m_j$ is combinatorially free and by Anick's criterion (1.4.14) we conclude that $\rho_1, \dots, \rho_j$ is strongly free, noting that (1.4.14) remains valid for $<_U$ (cf. (1.4.17)). This concludes the proof. □

(2.3.3) Example.

(i) If $\mathfrak{z}(G) = 2$, the above statement is the following: Assume that $H^1(G) = U \oplus V$ and the cup-product $H^1(G) \otimes H^1(G) \xrightarrow{\cup} H^2(G)$ is trivial on $V \otimes V$ and maps $U \otimes V$ surjectively onto $H^2(G)$. Then G is mild. For odd p this result has been obtained by A. Schmidt (cf. [Sch10], Th.6.2) as a reformulation of Th.5.5 in [Sch07]. The proof is based on the work of J. Labute, more precisely on the criterion for strongly free sequences via the elimination theorem for free Lie algebras, cf. (1.4.22). In the case $p = 2$ this has been proven by J. Labute and J. Mináč (cf. [LM11]) using mixed Lie algebras and later independently by P. Forré (cf. [For10]).

(ii) Next consider the case $\mathfrak{z}(G) = 3$ and apply (2.3.2) for $e = 1$. We obtain that G is mild if $H^1(G) = U \oplus V$ and the triple Massey product is trivial on $V \otimes V \otimes V$ and maps $U \otimes V \otimes V$ surjectively onto $H^2(G)$. A straightforward application of (2.2.9) shows that these conditions are equivalent to the following: G possesses a minimal presentation $G = \langle x_1, \dots, x_d \mid r_1, \dots, r_m \rangle$ where

$$r_n \equiv \begin{cases} \displaystyle\prod_{\substack{1 \le i < j \le d,\\ 1 \le k \le j}} [[x_i, x_j], x_k]^{a^n_{ijk}} \mod F_{(4)}, & \text{if } p \ne 3, \\ \displaystyle\prod_{1 \le i \le d} x_i^{3a_i^n} \cdot \prod_{\substack{1 \le i < j \le d,\\ 1 \le k \le j}} [[x_i, x_j], x_k]^{a^n_{ijk}} \mod F_{(4)}, & \text{if } p = 3 \end{cases}$$

for $n = 1, \dots, m$ with $a_i^n, a_{ijk}^n \in \mathbb{F}_p$, such that for some $1 \le c < d$:

(I) $a_{ijk}^n = 0$ if $c < i < j, c < k \le j$ and $1 \le n \le m$,

(II) The $m \times c(d-c)^2$-matrix

$$(a_{ijk}^n)_{n,(ijk)}, \quad 1 \le n \le m,\ 1 \le i \le c < k \le j \text{ or } 1 \le k \le c < i < j$$

has rank m.

(III) If $p = 3$, then $a_i^n = 0$ if $c < i$ and $1 \le n \le m$.

*) Note that the initial form ρ_j is obtained by leaving out all monomials of degree $> n$ in the Magnus expansion of r_j.

This resembles very much the prerequisites made in (2.1.2), but comparing the matrices in conditions (II) and (ii) of (2.1.2) respectively, we see that (2.3.2) yields a stronger criterion, i.e. it applies to a bigger class of pro-p-groups with Zassenhaus invariant 3.

Applying (2.3.2) for $e = 2$, we find that G is mild if $H^1(G) = U \oplus V$, the triple Massey product is trivial on the subspaces

$$H^1(G) \otimes V \otimes V, \quad V \otimes H^1(G) \otimes V, \quad V \otimes V \otimes H^1(G)$$

and maps $U \otimes U \otimes V$ surjectively onto $H^2(G)$. It is an easy exercise to give a translation of these conditions in terms of basic commutators as in the case $e = 1$.

(2.3.4) Remark. In order to apply (2.3.2) for a finitely presented pro-p-group G with $n = \mathfrak{z}(G)$, it is necessary that the n-fold Massey product is surjective onto $H^2(G)$. If this is not the case, then G possesses a minimal presentation $G = F/R$ such that at least one of the defining relations lies in $F_{(n+1)}$. Such a group can of course still be mild, but the n-fold Massey product does not carry enough information to determine the initial forms of the defining relations.

Using (2.3.2), one can construct a large supply of mild pro-p-groups with given Zassenhaus invariant. On the other hand, the assertions are not necessary for mildness, even if the n-fold Massey product is surjective. Since being strongly free depends on the (infinite) Poincaré series of a given sequence of homogeneous polynomials, in general only sufficient (but not necessary) conditions can be expected. However, these criteria apply to many arithmetically defined pro-p-groups, e.g. the maximal pro-p-quotient $G_S(p) = \pi_1^{et}(X_S)(p)$ of the étale fundamental group of the arithmetic curve $X_S = Spec(\mathcal{O}_k) \setminus S$ where $\mathcal{O}_k$ is the ring of integers of some global field k and S is a finite set of primes. A. Schmidt has shown that if $cd\, G_S(p) \leq 2$ and the natural homomorphism

$$H^2(G_S(p), \mathbb{F}_p) \longrightarrow H^2_{et}(X_S, \mathbb{F}_p)$$

is surjective, then X_S is a $\boldsymbol{K(\pi, 1)}$ **for** $\boldsymbol{p}$, i.e. for any discrete p-torsion module M of $G_S(p)$ the Galois cohomology $H^i(G_S(p), M)$ coincides with the étale cohomology $H^i_{et}(X_S, M)$ (of the constant sheaf M). Moreover in this case $G_S(p)$ is often a pro-p duality group (cf. [Sch10], Cor.3.7 and Th.9.6). The cup-product criterion as in (2.3.3) is one key ingredient in the proof of the following remarkable theorem also due to A. Schmidt (cf. [Sch10], Th.1.1):

(2.3.5) Theorem. *Let k be a global field and p be an odd prime different from* $\mathrm{char}(k)$. *Let S be a finite set of primes and $\mathcal{M}$ an arbitrary set of primes with Dirichlet density $\delta(\mathcal{M}) = 0$. Then there exists a finite set of primes S_0 disjoint from $S \cup \mathcal{M}$ such that $Spec(\mathcal{O}_k) \setminus (S \cup S_0)$ is a $K(\pi, 1)$ for p.*[*)]

[*)] The precise statement of Schmidt's theorem is actually even stronger: Firstly the theorem deals with the more general groups $G_S^T(p)$, i.e. the Galois group of the maximal pro-p-extension of k unramified outside S and completely decomposed at the primes in T. Moreover by enlarging the set S via S_0 it can be assured that for the primes in $S \cup S_0$ the complete maximal pro-p-extensions of the associated local fields are realized and that an arithmetic version of Riemann's existence theorem holds.

In particular, we can take $\mathcal{M}$ as the set of primes S_p of k above p and hence the set S_0 can be chosen to be disjoint from S_p. This shows the crucial impact of mild pro-p-groups on the theory of *restricted ramification*, since until the work of J. Labute ([Lab06]) nothing was known about the cohomological dimension of $G_S(p)$ in the *tame case* (i.e. $S \cap S_p = \varnothing$), apart from examples where $G_S(p)$ is not torsion-free and therefore $cd\, G_S(p) = \infty$.

We finish this section by giving some heuristic results on the effectiveness of the criteria obtained in (2.3.2). As already mentioned they are not necessary for mildness. However, for a fixed generator rank $d = h^1(G)$, relation rank $r = h^2(G)$ and Zassenhaus invariant $n = \mathfrak{z}(G)$ one has only finitely many possible sequences of initial forms. Assuming that the n-fold Massey product is surjective, the sequence of initial forms $\rho_1, \ldots, \rho_m$ in a given minimal presentation $G = \langle x_1, \ldots, x_d \mid r_1, \ldots, r_m \rangle$ is strongly free if and only if this holds for *any* minimal presentation. Hence one is led to the classification of the (finite set of) equivalence classes of sequences of homogeneous polynomials of restricted Lie type $\rho_1, \ldots, \rho_m$.

To make this more precise, let $\mathcal{Q}(d, m, n)$ denote the set of all sequences $(\rho_1, \ldots, \rho_m) \in L_{res}(X),\ X = \{X_1, \ldots, X_d\}$ such that

(i) ρ_i is homogeneous of degree n for all $i = 1, \ldots, m$ and

(ii) the set $\{\rho_1, \ldots, \rho_m\}$ is $\mathbb{F}_p$-linearly independent.

We have a left action of the group $GL_m(\mathbb{F}_p) \times GL_d(\mathbb{F}_p)$ on $\mathcal{Q}(d, m, n)$ where $GL_m(\mathbb{F}_p)$ acts on the natural way and the action of $GL_d(\mathbb{F}_p)$ is given by the composite of

$$GL_d(\mathbb{F}_p) \cong \mathrm{Aut}(L_{res}(X)_1) \hookrightarrow \mathrm{Aut}(L_{res}(X)) \longrightarrow \mathrm{Aut}(L_{res}(X)_n)$$

where the first map lifts the automorphisms of the degree-1 subspace of $L_{res}(X)$ noting that $L_{res}(X)$ is freely generated by $X_1, \ldots, X_d$ and the second map denotes restriction. We consider the set of orbits of $\mathcal{Q}(d, m, n)$ under this action. An orbit is called *mild* if it can be represented by a strongly free sequence, which is equivalent to all the representing sequences being strongly free. For p odd, $d = m = 4$ and $n = 2$, it has been shown by M. Bush and J. Labute that there are exactly four orbits two of which are mild. The mild orbits are amenable to the criterion given in (2.3.2) for $n = 2$ (cf. [BL07]). In [BGLV11] a complete classification is given for arbitrary generator rank d in the case of two quadratic relations, i.e. $m = n = 2$ (including the case $p = 2$). For instance, if $d = 4, p = 2$ there are 54 orbits; 45 of these orbits are mild.

Using the computational algebra system [MAGMA], we can give analogous calculations for $p = 2$ and the case of relators of degree 3, i.e. $n = 3$. If $d = 3, m = 2$, then $\mathcal{Q}(3, 2, 3)$ decomposes into a total number of 93 orbits as follows:

- number of mild orbits satisfying the conditions in (2.3.2): 92

- number of mild orbits not satisfying the conditions in (2.3.2): 1
- number of non-mild orbits: 0

The only orbit for which our criterion fails can still shown to be mild using Anick's criterion. In particular, we see that for any 3-generator, 2-relator pro-2-group with with trivial cup-product and surjective triple Massey product, it holds that $cd\, G = 2$.

If $d = m = 3$, we have a decomposition of $\mathcal{Q}(3,3,3)$ into 658 orbits as follows:

- number of mild orbits satisfying the conditions in (2.3.2): 91
- number of mild orbits not satisfying the conditions in (2.3.2): 381
- number of non-mild orbits: 48

The non-mild orbits have Poincaré series differing in degree 6 from the series

$$\frac{1}{1-3t+3t^3} = 1 + 3t + 9t^2 + 24t^3 + 63t^4 + 162t^5 + 414t^6 + \dots.$$

For the remaining 138 orbits the first terms of their Poincaré series indicate that the representing sequences are strongly free. However, we are not able to give a proof using any of the criteria we have at hand.

2.4 One-relator pro-p-groups

We will now focus on the case where G is a ·finitely generated pro-p-group with a single defining relation. If the cup-product pairing $H^1(G) \times H^1(G) \to H^2(G)$ is non-degenerate, then G is a **Poincaré group** of dimension 2 provided it is infinite (which is always the case except if $p = 2$ and $G = \mathbb{Z}/2\mathbb{Z}$). After quickly recalling some well-known results we will show that one-relator pro-p-groups are mild provided their Zassenhaus invariant is coprime to p. This generalizes results by J. Labute already obtained in [Lab67a]. Furthermore, there is a close connection to an open question asked by D. Gildenhuys.

(2.4.1) Definition. *A* **one-relator pro-p-group** *is a pro-p-group G satisfying $h^1(G) < \infty$ and $h^2(G) = 1$. For a one-relator pro-p-group G we define the invariant q as follows: For the abelianization G^{ab} of G it holds that*

$$G^{ab} \cong \mathbb{Z}_p^n \quad or \quad G^{ab} \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}_p^{n-1}$$

where $q \neq 1$ is a p-th power and we set $q = 0$ in the first case.

An important example of one-relator pro-p-groups are the **Demuškin groups**, i.e. pro-p-groups G with $h^1(G) < \infty$, $h^2(G) = 1$ and non-degenerate cup-product pairing. Demuškin groups are of great interest in arithmetic as well as in geometry, since they occur as Galois groups of the maximal p-extension of local fields containing the p-th roots of unity or as pro-p-completions of fundamental groups of compact Riemann surfaces. Their main algebraic property is stated in the following

(2.4.2) Theorem.

(i) *An infinite Demuškin pro-p-group G is a* **Poincaré group** *of dimension 2, i.e. G is a duality group of dimension 2 and with dualizing module $D_p(G) \cong \mathbb{Q}_p/\mathbb{Z}_p$.*

(ii) *The group $G = \mathbb{Z}/2\mathbb{Z}$ is the only finite Demuškin group.*

For a proof we refer to [NSW08]: (i) follows as a special case of Prop.3.7.6 loc. cit., for a proof of statement (ii) see Prop.3.9.10 loc. cit.

In [Dem61], S.P. Demuškin has shown that these groups can be classified by the explicit form of their defining relation:

(2.4.3) Theorem. *Let G be a one-relator pro-p-group with $n = h^1(G)$ such that the invariant q of G is different from 2. Then G is a Demuškin group if and only if it admits a presentation $G = F/(r)$ where F is the free pro-p-group on generators $x_1, \ldots, x_n$ and*

$$r = x_1^q[x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n].$$

For a proof we refer to [NSW08], Th.3.9.11.

J. Labute generalized this result to the case where $q = 2$ (cf. [Lab67b]). Further characterizations of Demuškin groups are given by D. Dummit and J. Labute in [DL83], where it is shown that a one-relator pro-p-group G with $h^1(G) > 1$ is a Demuškin group if and only if every open subgroup of G is a one-relator group.

If we drop the assumption on the cup-product being non-degenerate, a one-relator pro-p-group can still to be shown to be of cohomological dimension 2 in many cases. J. Labute showed that if the generating relation of a one-relator pro-p-group is 'not too close' to being a p-th power, then the group is mild (cf. [Lab67a], Th.4). One key ingredient in his proof is the following theorem, cf. [Lab67a], Th.1.

(2.4.4) Theorem. *Let k be an arbitrary field and $L_k(X)$ be the free Lie algebra over k on the set $X = \{X_1, \ldots, X_d\}$ endowed with the (X, τ)-filtration for some $\tau = (\tau_1, \ldots, \tau_d)$. Let $\rho \in L_k(X)$ be a homogeneous element of degree n. Let $\mathfrak{r} = (\rho)$ denote the ideal of $L_k(X)$ generated by ρ and set $\mathfrak{g} = L_k(X)/\mathfrak{r}$. Then the Poincaré series of the enveloping algebra $U_\mathfrak{g}$ of $\mathfrak{g}$ satisfies*

$$U_\mathfrak{g}(t) = \frac{1}{1 - (t^{\tau_1} + \ldots + t^{\tau_d}) + t^n}.$$

In the following we are working over the field $k = \mathbb{F}_p$ again.

(2.4.5) Corollary. *Let $X = \{X_1, \ldots, X_d\}$ and $\rho \in L(X) \subset \mathbb{F}_p\langle X\rangle$ be a non-zero homogeneous element with respect to the (X, τ)-filtration for some $\tau = (\tau_1, \ldots, \tau_d)$ of Lie type. Then the sequence $\{\rho\}$ is strongly free.*

Proof. Let $\mathcal{R}$ denote the two-sided ideal of $\mathbb{F}_p\langle X\rangle$ generated by ρ. We have seen in the proof of (1.4.21) that there is an isomorphism

$$\mathbb{F}_p\langle X\rangle/\mathcal{R} \cong U_{\mathfrak{g}}$$

where as above $U_{\mathfrak{g}}$ denotes the enveloping algebra of $L(X)/(\rho)$. Hence the claim follows immediately from (2.4.4). □

We can now show the following theorem stating that one-relator pro-p-groups are 'often' mild:

(2.4.6) Theorem.

(i) *Let F be the free pro-p-group on $x_1, \ldots, x_d$. Let $r \in F_{(2)}$ such that for some $\tau = (\tau_1, \ldots, \tau_d)$, the initial form ρ of r is of Lie Type, i.e. $\rho \in L(X) \subset L_{res}(X) \cong \mathrm{gr}^\tau F$, $X = \{X_1, \ldots, X_d\}$. Then $G = F/(r)$ is mild with respect to the Zassenhaus (x, τ)-filtration.*

(ii) *Let G be a one-relator pro-p-group such that the Zassenhaus invariant $\mathfrak{z}(G)$ is prime to p. Then G is mild with respect to the Zassenhaus filtration.*

Proof. The first statement is a direct consequence of (2.4.5). Hence it remains to show (ii): Assume that $G = F/(r)$ is a one-relator pro-p-group with Zassenhaus invariant $n = \mathfrak{z}(G)$. Then $r \in F_{(n)} \setminus F_{(n+1)}$ and hence for the initial form ρ of r we have $\rho \in \mathrm{gr}_n F = L_{res}(X)_n$. Since n is coprime to p, by (1.2.11) the set C_n of Hall commutators of degree n is a basis of $L_{res}(X)_n$ and therefore $L_{res}(X)_n = L(X)_n$. In particular, $\rho \in L(X)$ is of Lie type. Now the claim follows from (i). □

The above theorem generalizes the results obtained by J. Labute in [Lab67a]. In fact, (i) can be considered to be a reformulation of Th.4' loc. cit. whereas statement (ii) is a more general version of Th.4 loc. cit. There for a finitely generated free pro-p-group F Labute defines a function $N : F \to \mathbb{Q}^+ \cup \{\infty\}$ measuring how 'far' an element is from being a p-th power*) and proves that $N(r) < p$ implies $cd\, F/(r) \leq 2$. However, one can find elements $r \in F$ with Zassenhaus degree prime to p (i.e. (2.4.6)(ii) applies for $G = F/(r)$), but $N(r) \geq p$. In our proof it was essential to combine Labute's results on quotients of free Lie algebras generated by one element with the fact that we have a complete description of the (graded) structure of $\mathrm{gr}\, F$ in terms of a free restricted Lie algebra.

In particular, if $p \neq 2$ and the cup-product $H^1(G)^2 \longrightarrow H^2(G)$ is non-trivial for the one-relator pro-p-group G, then $cd\, G \leq 2$. The same holds if $p \neq 3$, the cup-product is the zero map but the triple Massey product $H^1(G)^3 \longrightarrow H^2(G)$ has non-trivial image.

Now assume that G is a one-relator pro-p-group with $cd\, G > 2$. By (2.4.6) we have $p \mid n$. This observation is related to the following question:

*) An element $r \in F$ is a p-th power if and only if $N(r) = \infty$.

"Let G be a one-relator pro-p-group satisfying $cd\, G > 2$. Does G admit a presentation of the form $G = F/(u^p)$, i.e. is G the quotient of a free pro-p-group by a p-th power?"

This question has been originally posed by Serre in [Ser63], the above formulation is due to Gildenhuys.*) An affirmative answer would imply that for a one-relator pro-p-group G one has $cd\, G = 2$ if and only if $cd\, G < \infty$. According to the author's knowledge, this is still open (see also [RZ10], Open Question 7.10.4).

We will now focus on one-relator pro-p-groups with Zassenhaus invariant equal to p. We start with the following lemma:

(2.4.7) Lemma. *Assume that G is a finitely generated pro-p-group with Zassenhaus invariant $\mathfrak{z}(G) \geq p$. Then the p-fold Massey product*

$$\langle \cdot, \ldots, \cdot \rangle : H^1(G)^p \longrightarrow H^2(G)$$

induces a linear map

$$B_p : H^1(G) \longrightarrow H^2(G),\ \chi \longmapsto \langle \chi, \chi, \ldots, \chi \rangle.$$

Proof. This follows from the shuffle relations of the Massey product, see [Vog04], Lemma 1.2.14 for details. □

In fact, B_p equals $-B$ where B denotes the **Bockstein homomorphism** $B : H^1(G) \longrightarrow H^2(G)$, i.e. the connecting homomorphism associated to the exact sequence

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

(see [NSW08], Prop.3.9.14 for $p = 2$ and [Vog04], Prop.1.2.15 for the general case). Of course, if $\mathfrak{z}(G)$ is strictly bigger than p, then the p-fold Massey product is trivial and hence B_p is the zero map.

(2.4.8) Proposition. *Let G be a one-relator pro-p-group with generator rank $d = h^1(G)$ and Zassenhaus invariant $\mathfrak{z}(G) = p$ and $G = F/(r)$ be a minimal presentation of G. Assume that $cd\, G > 2$. Then there exists a free basis $x_1, \ldots, x_d$ of F and $y \in F$ such that*

$$r \equiv x_1^p \bmod F_{(p+1)}.$$

*) Actually, Serre asked the following: "If $cd\, F/(r) > 2$, is r a p-th power in F?" This is the pro-p-analogue of a result for discrete groups due to Lyndon (cf. [Lyn50]). However, in [Gil68] Gildenhuys gave a negative answer to this question by showing that the group $G = \langle x_1, x_2 \mid x_1^p[x_2, x_1^p] \rangle$ is a counterexample for arbitrary p, since $cd\, G = \infty$, but $x_1^p[x_2, x_1^p]$ is not a p-th power. Consequently, he came up with the above (slightly corrected) formulation of the question.

Proof. Since $\mathfrak{z}(G) = p$, we have $r \in F_{(p)} \setminus F_{(p+1)}$. Let $\rho \in \mathrm{gr}_p F$ denote the initial form of r. First choose an arbitrary basis $\tilde{x} = \{\tilde{x}_1, \ldots, \tilde{x}_d\}$ of F and denote by $\tilde{X} = \{\tilde{X}_1, \ldots, \tilde{X}_d\} \in \mathrm{gr}\, F$ the corresponding initial forms. Suppose that the homomorphism $H^1(G) \longrightarrow H^2(G)$ is zero, then by (2.2.5)

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

for any multi-index of length p of the form $I = (i, i, \ldots, i),\ i = 1, \ldots d$ (where the map $\varepsilon_{I,p}$ is defined with respect to the basis $\tilde{x}$) and hence ρ contains no summand of the form $\tilde{X}_i^p,\ i = 1, \ldots, d$. Since a basis of $\mathrm{gr}_p F$ is given by

$$\{\tilde{X}_i^p \mid i = 1, \ldots, d\} \cup C_p,$$

where C_p are the basic commutators of degree p, cf. (1.2.11), this implies that ρ is of Lie type and consequently by (2.4.6) (i) we have $cd\, G = 2$ contradicting the assumption. Therefore, B_p is not the zero map (and hence surjective). We choose a basis $\chi_1, \ldots, \chi_d$ of $H^1(G)$ such that $\chi_2, \ldots, \chi_d$ is a basis of $\ker B_p$. Let $x = \{x_1, \ldots, x_d\}$ be a basis of F lifting the corresponding dual basis of $H^1(G)^\vee = H^1(F)^\vee = F/F_{(2)}$ and denote by $X_1, \ldots, X_d \in \mathrm{gr}\, F$ the corresponding initial forms. Since $B_p(\chi_1) \neq 0$, it follows that $tr_r(B_p(\chi_1)) \neq 0$ and after replacing x_1 by x_1^a for some $a \in \mathbb{F}_p^\times$ we may assume that

$$\varepsilon_{I,p}(r) = 1,\ I = (1, 1, \ldots, 1)$$

and $\varepsilon_{I,p}(r) = 0$ for the multi-indices $I = (i, i, \ldots, i),\ i = 2, \ldots, d$ (where $\varepsilon_{I,p}$ is now defined with respect to x). Hence, using (1.3.11), we can write

$$r = x_1^p\ c\ r'$$

where c is a (possibly empty) product of basic commutators on x of weight p and $r' \in F_{(p+1)}$. We claim that $c = 1$. To this end, we consider a different filtration on F, namely the Zassenhaus (x, τ)-filtration ω_τ of F where

$$\tau_i = \begin{cases} a, & \text{if } i = 1, \\ b, & \text{else} \end{cases}$$

for arbitrary natural numbers a, b satisfying $a > b,\ a < \frac{bp}{p-1}$. Suppose $c \neq 1$. Since every basic commutator in c contains the generator x_1 at most $p-1$ times, we have

$$\omega_\tau(c) \leq a(p-1) + b.$$

Furthermore, $\omega_\tau(x_1^p) = pa > a(p-1) + b$ and $\omega_\tau(r') \geq (p+1)\min(a, b) = (p+1)b > a(p-1) + b$. Hence the initial form $\tilde{\rho} \in \mathrm{gr}^\tau F$ of r is a (non-zero) sum of Hall commutators, in particular $\tilde{\rho}$ is of Lie type. Hence G is mild with respect to the Zassenhaus (x, τ)-filtration by (2.4.6) (i), which again yields a contradiction to the assumption $cd\ > 2$. Therefore, $c = 1$ and hence $r \equiv x_1^p \mod F_{(p+1)}$. □

Unfortunately, we cannot give an answer to Gildenhuys' question. However, the above proposition shows that the generating relation of a one-relator pro-p-group of cohomological dimension > 2 is 'not far' from being a p-th power, at least if the Zassenhaus invariant equals p.

We end this chapter by studying the associated graded restricted Lie algebra $\mathrm{gr}^\tau G$ of the one-relator pro-p-group $G = F/(x_1^p)$ with defining relation $x_1^p = 1$. An explicit description of $\mathrm{gr}^\tau G$, or equivalently of the kernel of the natural map $\mathrm{gr}^\tau F \to \mathrm{gr}^\tau G$, shows which "commutator relations" are implied by the above "power relation", see also [MKS76], Section 5.11 for related questions in the case of discrete groups. An analogous description has been obtained for the lower central series by J. Labute, cf. [Lab77]. As we will see, considering p-restricted filtrations, one obtains a particularly simple description of $\mathrm{gr}^\tau G$. The author is indebted to Prof. Labute for kindly pointing out that the following statement can be obtained using the results of the first chapter.

(2.4.9) Proposition. *Let $G = F/R$ where F is the free pro-p-group on $x = \{x_1, \ldots, x_d\}$ and $R = (x_1^p)$ is the closed normal subgroup of F generated by x_1^p. Let F, G be endowed with the Zassenhaus (x, τ)-filtration for some $\tau = (\tau_1, \ldots, \tau_d)$. Then*

$$\mathrm{gr}^\tau G = \mathrm{gr}^\tau F/(X_1^p)$$

where (X_1^p) denotes the ideal of the free restricted Lie algebra $\mathrm{gr}^\tau F$ generated by the initial form X_1^p of x_1^p.

Proof. Set $\mathfrak{r} := \mathrm{gr}^\tau R \subseteq \mathrm{gr}^\tau F$. Note that we have the exact sequence

$$0 \longrightarrow \mathfrak{r} \longrightarrow \mathrm{gr}^\tau F \longrightarrow \mathrm{gr}^\tau G \longrightarrow 0$$

of graded restricted Lie algebras and that clearly $(X_1^p) \subseteq \mathfrak{r}$. We have to show that equality holds. Let $S \subseteq R$ denote the closed normal subgroup generated by $r_2, \ldots, r_d$ where $r_i = [x_i, x_1^p],\ i = 2, \ldots, d$. Set $\mathfrak{s} = \mathrm{gr}^\tau S \subseteq \mathrm{gr}^\tau F$. Since the elements

$$x_1^p,\ [f, x_1^p],\ 1 \neq f \in F$$

generate R as a closed subgroup of F, it follows that as an ideal $\mathfrak{r}$ is generated by X_1^p and $\mathfrak{s}$. Let $\rho_2, \ldots, \rho_d \in \mathfrak{s}$ denote the initial forms of $r_2, \ldots, r_d$. Making the usual identification $\mathrm{gr}^\tau F \cong L_{res}(X) \subset \mathbb{F}_p\langle X\rangle,\ X = \{X_1, \ldots, X_d\}$, the leading monomials of the ρ_i with respect to the lexicographic ordering induced by $X_1 < X_2 < \ldots < X_d$ are given by the combinatorially free sequence

$$X_i X_1^p,\ i = 2, \ldots, d.$$

Hence by Anick's criterion (1.4.14) the sequence $\rho_2, \ldots, \rho_m$ is strongly free. By (1.5.10)(iii) it follows that $\mathfrak{s} = (\rho_2, \ldots, \rho_d)$ is the ideal of $\mathrm{gr}^\tau F$ generated by the ρ_i. In particular, we have $\mathfrak{s} \subseteq (X_1^p)$ and consequently $\mathfrak{r} \subseteq (X_1^p)$ which concludes the proof. □

(2.4.10) Corollary. *Let $G = F/(x_1^p)$ be given as in* (2.4.9)*. Then the universal enveloping algebra $U_{\mathrm{gr}^\tau G}$ of $\mathrm{gr}^\tau G$ is given by*

$$U_{\mathrm{gr}^\tau G} = \mathbb{F}_p\langle X\rangle/(X_1^p).$$

In particular, we have

$$U_{\mathrm{gr}^\tau G}(t) = \frac{1 - t^{p\tau_1}}{1 - t^{\tau_1} - (t^{\tau_2} + \ldots + t^{\tau_d})(1 - t^{p\tau_1})}.$$

Proof. Using (2.4.9), by (1.2.6) we find that $U_{\mathrm{gr}^\tau G}$ is the quotient of the enveloping algebra $U_{\mathrm{gr}\, F}$ by the two-sided ideal generated by X_1^p, i.e.

$$U_{\mathrm{gr}^\tau G} = U_{\mathrm{gr}^\tau F}/(X_1^p) \cong \mathbb{F}_p\langle X\rangle/(X_1^p).$$

In order to calculate its Poincaré series, set $A = \mathbb{F}_p\langle X\rangle$, $\mathcal{R} = (X_1^p)$, $B = A/\mathcal{R} \cong U_{\mathrm{gr}^\tau G}$ and consider the standard exact sequence

$$0 \longrightarrow \mathcal{R}/\mathcal{R}I_A \longrightarrow I_A/\mathcal{R}I_A \longrightarrow B \longrightarrow \mathbb{F}_p \longrightarrow 0 \tag{2.4}$$

where I_A denotes the augmentation ideal of A (cf. also the proof of (1.4.2)). Recall that $I_A/\mathcal{R}I_A \cong \bigoplus_{i=1}^d B[\tau_i]$ as graded $\mathbb{F}_p$-vector space and hence

$$(I_A/\mathcal{R}I_A)(t) = \sum_{i=1}^d t^{\tau_i} B(t).$$

A basis of $\mathcal{R}/\mathcal{R}I_A$ as $\mathbb{F}_p$-vector space is given by the images of the monomials

$$\{X_1^p\} \cup \{X_{i_1}X_{i_2}\cdots X_{i_k}X_1^p \mid k \geq 1,\ i_k \neq 1,\ X_{i_1}\cdots X_{i_{k-1}} \notin \mathcal{R}\}.$$

Therefore, we have the isomorphism

$$\big(\mathbb{F}_p \oplus \bigoplus_{i=2}^d B[\tau_i]\big)[p\tau_1] \cong \mathcal{R}/\mathcal{R}I_A$$

of graded $\mathbb{F}_p$-vector spaces. In particular, we obtain

$$(\mathcal{R}/\mathcal{R}I_A)(t) = t^{p\tau_1} + \sum_{i=2}^d t^{p\tau_1+\tau_i} B(t).$$

Adding up the Poincaré series in the exact sequence (2.4) and solving for $B(t)$, we obtain the desired equality.

□

3 Pro-2-extensions of $\mathbb{Q}$ with wild ramification

3.1 First remarks on arithmetic examples

Having developed a criterion for a pro-p-group with vanishing cup-product to be mild, the question arises whether such groups occur as arithmetic Galois groups, in particular as Galois groups of the maximal p-extension with given ramification over a number field k. By results of I.R. Šafarevič and H. Koch (cf. [Koc02], Ch.11.4), a minimal presentation of these groups can be given explicitly with the relations determined modulo the third step of the p-central series (or the Zassenhaus filtration respectively). A description of the relations modulo the fourth step of the Zassenhaus filtration has been given in [Mor02] and [Vog05] in the special case where $k = \mathbb{Q}$, $p = 2$ and S is a set containing the infinite prime and prime numbers $\equiv 1 \bmod 4$. In this section we give a short overview of the main results in these cases. It turns out that the pro-2-groups which occur are never mild.

Let $S = \{l_1, \ldots, l_n, \infty\},\ n \geq 3$ where $l_1, \ldots, l_n$ are prime numbers $\equiv 1 \mod 4$ and ∞ denotes the infinite prime of $\mathbb{Q}$. Let $G_S(2)$ be the Galois group of the maximal pro-2-extension of $\mathbb{Q}$ unramified outside S. If the Legendre symbols $\left(\frac{l_i}{l_j}\right)_2$ satisfy

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

then the cup-product $H^1(G_S(2)) \times H^1(G_S(2)) \stackrel{\cup}{\to} H^2(G_S(2))$ is trivial. Thus, the triple Massey product of $G_S(2)$ exists. In [Mor02], M. Morishita gives a description of this product in terms of the **Rédei symbols** $[\cdot, \cdot, \cdot]$. This description has has been generalized by D. Vogel ([Vog05]). We give a definition and a detailed description of this symbol in the following chapter. We mention that it is invariant under permutations, i.e.

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

for any $\gamma \in S_3$ (cf. [Réd38], Th.2 and Th.4). Furthermore, the following theorem describes an interesting relation between the Rédei symbols and the presentation of the group $G_S(2)$.

(3.1.1) Theorem. *Let $S = \{l_1, \ldots, l_n, \infty\}$ where l_i are distinct prime numbers $\equiv 1 \mod 4$ satisfying*

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

Then we have $h^1(G_S(2)) = h^2(G_S(2)) = n$ *and* $G_S(2)$ *admits a minimal presentation*

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

where F *is the free pro-p-group on generators* $x_1, \dots, x_n$ *and* R *is generated by* $r_1, \dots, r_n$ *as a normal subgroup of* F*, such that for the basis* $\chi_1, \dots, \chi_n$ *of* $H^1(F) = H^1(G_S(2))$ *dual to* $x_1, \dots, x_n$ *the identities*

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

hold for $m = 1, \dots, n$.

This follows from [Vog05], Th.3.12.

Keeping the assumptions of (3.1.1), the initial forms $\rho_1, \dots, \rho_n \in \operatorname{gr} F \cong L_{res}(X_1, \dots, X_n)$ of $r_1, \dots, r_n$ are homogeneous polynomials of Lie type. More precisely, by (2.2.9) they are given by

$$\rho_m = \sum_{\substack{1 \le i < j \le d, \\ 1 \le k \le j}} a^m_{ijk}[[X_i, X_j], X_k], \quad m = 1, \dots, n,$$

such that for $1 \le i, k < j \le n$ we have $(-1)^{a^m_{ijk}} = [l_i, l_j, l_k]$ if and only if $m = j$ or $m = k$, for $1 \le i < k$ we have $(-1)^{a^m_{ikk}} = [l_i, l_k, l_k]$ if and only if $m = i$ or $m = k$ and otherwise $a^m_{ijk} = 0$. Thus, if $1 \le i < k \le n$, $1 \le j \le k$ and $[l_i, l_j, l_k] = -1$, the commutator $[[X_i, X_j], X_k]$ occurs exactly twice in the ρ_m, $m = 1, \dots, n$. Consequently setting $\{l_i, l_j, l_k\} := 1$ if $[l_i, l_j, l_k] = -1$ and $\{l_i, l_j, l_k\} := 0$ otherwise we have

$$\sum_{m=1}^{n} \rho_m = \sum_{m=1}^{n} \sum_{\substack{1 \le i < j \le d, \\ 1 \le k \le j}} a^m_{ijk}[[X_i, X_j], X_k] = \sum_{\substack{1 \le i < j \le d, \\ 1 \le k \le j}} 2\{l_i, l_j, l_k\}[[X_i, X_j], X_k] = 0,$$

which means that the ρ_i generate a subspace $L_{res}(X_1, \dots, X_n)$ of dimension $\le n - 1$. In other words, the triple Massey product $H^1(G_S(2)) \times H^1(G_S(2)) \times H^1(G_S(2))$ is *not* surjective. So there is no chance of applying our criteria (2.1.2) and (2.3.2) respectively.

In fact, the group $G_S(2)$ cannot be mild by the following arithmetic argument: Let $S = \{l_1, \dots, l_n, \infty\}$ where $l_1, \dots, l_n$ are odd prime numbers. Let $e := v_2(l_1 - 1)$ and let K denote the unique subfield of $\mathbb{Q}(\zeta_{l_1})$ of degree 2^e over $\mathbb{Q}$. Then we have $K \subseteq \mathbb{Q}_S(2)$ and K is totally imaginary, i.e. complex conjugation induces a non-trivial involution in $G_S(2)$ and hence $cd\, G_S(2) = \infty$.*)

This also shows the following: If one wants to obtain arithmetic examples of mild pro-2-groups over $\mathbb{Q}$, the infinite prime has to be removed from S. On

*) By a result due to A. Schmidt, the same holds in the following general setting: If k is a number field and S is a set of primes containing all primes above 2, then any real prime contained in S becomes complex in $k_S(2)$, cf. [Sch02], Th.1

the other hand, in order to have a trivial Kummer group $V_S(\mathbb{Q})$ (which by [Koc02] is an obstruction for the relations of $G_S(2)$ being generated by *local* relations), one has to add the prime 2 or primes $\equiv 3 \mod 4$ to the set S. If S contains more than one prime $\equiv 3 \mod 4$, then in a minimal presentation $1 \to R \to F \to G_S(2) \to 1$ we always have $R \not\subset F_{(3)}$. If S contains only one prime $\equiv 3 \mod 4$, then the relations of $G_S(2)$ will satisfy symmetries similar to those shown above. Thus, in the next section we will restrict ourselves to the case $2 \in S$ and show that in special cases an analogue of (3.1.1) holds. This also requires further investigation of the infinite prime, since the extensions occurring in the definition of the Rédei symbols are usually ramified at ∞.

If p is an *odd* prime, it is not hard to construct examples of groups of the form $G_S(p)$ having trivial cup-product. For instance, this holds for $k = \mathbb{Q}$ and $S = \{l_1, \ldots, l_n\}$ with primes $l_i \equiv 1 \bmod p$, such that l_i is a p-th power modulo l_j for any i, j.*) However, we don't have a convenient analogue of the Rédei symbols permitting a calculation of the higher Massey products in these cases. This is why we focus on $p = 2$, which in other contexts often needs to be considered as a rather exceptional case.

3.2 A presentation of $G_S(2)$ in the case $2 \in S,\ \infty \notin S$

Contrary to the previous section, we will now consider 2-extensions of $\mathbb{Q}$ where we allow wild ramification, i.e. we study the Galois group $G_S(2)$ of the maximal 2-extension $\mathbb{Q}_S(2)$ of $\mathbb{Q}$ unramified outside S where $2 \in S$. Recall that for a pro-2-group G we put $H^i(G) := H^i(G, \mathbb{Z}/2\mathbb{Z})$ and $h^i(G) := \dim_{\mathbb{F}_2} H^i(G)$. We start with the following

(3.2.1) Proposition. *Let $S = \{2, l_1, \ldots, l_n\}$ for some $n \geq 1$ and odd prime numbers $l_1, \ldots, l_n$. The pro-2-group $G_S(2)$ has cohomological dimension $cd\, G_S(2) = 2$ and satisfies*

$$\begin{aligned} h^1(G_S(2)) &= 1 + n, \\ h^2(G_S(2)) &= n. \end{aligned}$$

The abelianization $G_S(2)^{ab}$ is infinite.

Proof. Since by assumption $2 \in S, \infty \notin S$, [NSW08] Th.10.6.1 yields $cd\, G_S(2) \leq 2$ and $\chi_2(G_S(2)) = 0$ where $\chi_2(G_S(2)) = \sum_{i \geq 0} (-1)^i h^i(G_S(2))$ denotes the Euler-Poincaré characteristic of $G_S(2)$. Since $Ш_S(\mathbb{Q}) := (V_S(\mathbb{Q}))^\vee$ is trivial, the general formula [NSW08], Th.10.7.12 yields $h^1(G_S(2)) = 1 + n$ and thus also the second formula $h^2(G_S(2)) = n$ holds. In particular, we have $h^2(G_S(2)) < h^1(G_S(2))$ which implies the infiniteness of $G_S(2)^{ab}$ (of course this also follows from the fact that $\mathbb{Q}_S(2)$ contains the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$). □

We will now give an explicit description of $G_S(2)$ in terms of generators and relators using local Galois groups. Therefore, we will quickly recall some basic facts on local pro-2 Galois groups:

*) By Čebotarev's density theorem, one can construct infinitely many sets S with this property, cf. [Lab06], Prop.6.1. For $p = 3$ an example is given by $S = \{7, 181, 673, 3037\}$.

(3.2.2) Proposition. *Let l be a prime number and $G_l(2)$ be the Galois group of the maximal 2-extension $\mathbb{Q}_l(2)$ of $\mathbb{Q}_l$. Let $\mathcal{T}_l(2) \subseteq G_l(2)$ denote the inertia group of $G_l(2)$.*

(i) *If $l \neq 2$, then $\mathcal{T}_l(2) \cong \mathbb{Z}_2$ and $G_l(2)$ is a pro-2-group with two generators σ, τ satisfying the relation*

$$\tau^{l-1}[\tau^{-1}, \sigma^{-1}] = 1$$

where σ denotes an arbitrary lift of the Frobenius automorphism of the maximal unramified 2-extension of $\mathbb{Q}_l$ and τ is an arbitrary generator of $\mathcal{T}_l$.

(ii) *If $l = 2$, let $\sigma, \tau, \tilde{\tau}$ be arbitrary elements of $G_2(2)$ such that*

$$\begin{aligned} \sigma &\equiv (2, \mathbb{Q}_2(2)^{ab}|\mathbb{Q}_2) \mod [G_2(2), G_2(2)], \\ \tau &\equiv (5, \mathbb{Q}_2(2)^{ab}|\mathbb{Q}_2) \mod [G_2(2), G_2(2)], \\ \tilde{\tau} &\equiv (-1, \mathbb{Q}_2(2)^{ab}|\mathbb{Q}_2) \mod [G_2(2), G_2(2)] \end{aligned}$$

where $(\,\cdot\,, \mathbb{Q}_2(2)^{ab}|\mathbb{Q}_2)$ denotes the local norm residue symbol. Then σ is a lift of the Frobenius automorphism of the maximal unramified 2-extension of $\mathbb{Q}_2$, $\tau, \tilde{\tau} \in \mathcal{T}_2(2)$ and $\{\sigma, \tau, \tilde{\tau}\}$ form a minimal system of generators of $G_2(2)$. We have $h^2(G_2(2)) = 1$ and in a minimal presentation

$$1 \longrightarrow R \longrightarrow F \longrightarrow G_2(2) \longrightarrow 1$$

with preimages $s, t, \tilde{t}$ of $\sigma, \tau, \tilde{\tau}$ respectively, the single generating relation r can be chosen in the form

$$r \equiv \tilde{t}^{\,2}[t, s] \mod F_{(3)}.$$

Furthermore, τ and $\tilde{\tau}$ generate $\mathcal{T}_2(2)$ as a normal subgroup of $G_2(2)$.

Proof. The first statement is a special case of [Koc02], Th.10.2. For the second statement note that for $\pi := 2$, $\alpha_0 := 5$, $\alpha_1 := -1$ the set $\{\pi, \alpha_0, \alpha_1\}$ is a basis of $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ satisfying the conditions of [Koc02], Lemma 10.10.*) Then [Koc02], Th.10.12 yields the statement (ii). In fact, in order to see that $\tau, \tilde{\tau}$ generate $\mathcal{T}_2(2)$ as a normal subgroup of $G_2(2)$, let $\Gamma_2(2) = G_2(2)/\mathcal{T}_2(2)$ and consider the exact sequence

$$0 \longrightarrow H^1(\Gamma_2(2)) \longrightarrow H^1(G_2(2)) \longrightarrow H^1(\mathcal{T}_2(2))^{\Gamma_2(2)} \longrightarrow H^2(\Gamma_2(2)),$$

which yields $\dim_{\mathbb{F}_2} H^1(\mathcal{T}_2(2))^{\Gamma_2(2)} = 2$, since $h^1(\Gamma_2(2)) = 1$, $h^2(\Gamma_2(2)) = 0$. The elements $\tau, \tilde{\tau} \in \mathcal{T}_2(2)$ are contained in a minimal system of generators of $G_2(2)$, hence they are linearly independent modulo $\mathcal{T}_2(2)^2[G_2(2), \mathcal{T}_2(2)]$. Now the claim follows by reason of dimension. □

*) As D. Vogel pointed out to me, with a view to the correctness of the following theorem 10.12, this lemma contains a sign error in (iv); the condition $(\alpha_1, \pi) = -1$ has to be replaced by $(\alpha_1, \pi) = 1$, which holds in our case.

(3.2.3) Remark. By a classical result of K. Iwasawa, in the case of tame ramification (i.e. $l \neq 2$) one can describe the elements σ, τ explicitly (cf. [Iwa55], [Koc02]). For our purposes the description given in (3.2.2) is sufficient.

We return to the global situation and fix the following notations:

- Let $G_S(2)$ denote the Galois group of the maximal 2-extension $\mathbb{Q}_S(2)$ of $\mathbb{Q}$ unramified outside the set $S = \{l_0, \ldots, l_n\}$ where $l_0 = 2$ and $l_1, \ldots, l_n$ are odd prime numbers.
- For each $0 \leq i \leq n$ let $\mathfrak{l}_i$ denote a fixed prime of $\mathbb{Q}_S(2)$ above l_i.
- For $1 \leq i \leq n$ let $\hat{l}_i$ denote the idèle of $\mathbb{Q}$ whose l_i-component equals l_i and all other components are 1 and let $\hat{g}_i$ denote the idèle whose l_i-component equals g_i for a primitive root g_i modulo l_i and all other components are 1.
- For $i = 0$ let $\hat{l}_0,\ \hat{g}_0,\ \hat{g}'_0$ denote the idèles of $\mathbb{Q}$ whose 2-components are $2, 5$ and -1 respectively and all other components are 1.

For $0 \leq i \leq n$ we choose an element $\sigma_i \in G_S(2)$ with the following properties:

(i) σ_i is a lift of the Frobenius automorphism of $\mathfrak{l}_i$ with respect to the maximal subextension of $\mathbb{Q}_S(2)|\mathbb{Q}$ in which $\mathfrak{l}_i$ is unramified;

(ii) the restriction of σ_i to the maximal abelian subextension $\mathbb{Q}_S(2)^{ab}|\mathbb{Q}$ of $\mathbb{Q}_S(2)|\mathbb{Q}$ equals $(\hat{l}_i, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$ where $(\ \cdot\ , \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$ denotes the norm residue symbol.

For $1 \leq i \leq n$ we denote by $T_{\mathfrak{l}_i} \subseteq G_S(2)$ the inertia subgroup of $\mathfrak{l}_i$ and choose an element $\tau_i \in T_{\mathfrak{l}_i}$, such that

(i) τ_i generates $T_{\mathfrak{l}_i}$;

(ii) the restriction of τ_i to $\mathbb{Q}_S(2)^{ab}|\mathbb{Q}$ equals $(\hat{g}_i, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$.

Finally, let $\tau_0, \tilde{\tau}_0$ denote two elements of the inertia subgroup $T_{\mathfrak{l}_0} \subseteq G_S(2)$ of $\mathfrak{l}_0$ such that

(i) $\tau_0, \tilde{\tau}_0$ generate $T_{\mathfrak{l}_0}$ as a normal subgroup of the decomposition group $G_{\mathfrak{l}_0} \subseteq G_S(2)$ of $\mathfrak{l}_0$;

(ii) the restriction of τ_0 to $\mathbb{Q}_S(2)^{ab}|\mathbb{Q}$ equals $(\hat{g}_0, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$ and the restriction of $\tilde{\tau}_0$ to $\mathbb{Q}_S(2)^{ab}|\mathbb{Q}$ equals $(\hat{g}'_0, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$.

(3.2.4) Remark. The existence of elements satisfying the above properties follows from class field theory. The fact that τ_i can be chosen as a generator of $T_{\mathfrak{l}_i},\ 1 \leq i \leq n$ and $\tau_0, \tilde{\tau}_0$ can be chosen as generators of $T_{\mathfrak{l}_0}$ as a normal subgroup of $G_{\mathfrak{l}_0}$ follows from the corresponding local statements (3.2.2). This will turn out to be crucial for the correspondence between Rédei symbols and the group $G_S(2)$.

For $1 \leq i, j \leq n,\ i \neq j$ we define the **linking number** $a_{i,j} \in \mathbb{F}_2$ by

$$a_{i,j} := \begin{cases} 1, & \text{if } \left(\frac{l_i}{l_j}\right)_2 = -1, \\ 0, & \text{else.} \end{cases}$$

Furthermore, for $1 \leq i \leq n$ we define the numbers $a_{i,0}, \tilde{a}_{i,0} \in \mathbb{F}_2$ by

$$\begin{aligned} a_{i,0} &:= \begin{cases} 1, & \text{if } l_i \equiv 3,5 \mod 8, \\ 0, & \text{else} \end{cases} \qquad \textit{and} \\ \tilde{a}_{i,0} &:= \begin{cases} 1, & \text{if } l_i \equiv 3,7 \mod 8, \\ 0, & \text{else.} \end{cases} \end{aligned}$$

We can now give the desired description of the group $G_S(2)$ in terms of generators and relators which goes back to A. Fröhlich and H. Koch.

(3.2.5) Theorem. *Let $S = \{l_0, \ldots, l_n\}$ where $l_0 = 2$ and $l_1, \ldots, l_n$ are odd prime numbers. Furthermore, let F be the free pro-2-group on the $n+1$ generators $x_0, \ldots, x_n$. Then $G_S(2)$ admits a minimal presentation*

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

where π maps x_i to τ_i for $0 \leq i \leq n$. Let y_i denote a preimage of σ_i under π, then a minimal generating set of R as a normal subgroup of F is given by

$$r_i = x_i^{l_i - 1}[x_i^{-1}, y_i^{-1}],\ i = 1, \ldots, n$$

and we have

$$r_i \equiv x_i^{l_i-1} \prod_{\substack{0 \leq j \leq n \\ j \neq i}} [x_i, x_j]^{a'_{i,j}} \mod F_{(3)} \tag{3.1}$$

where the numbers $a'_{ij} \in \mathbb{F}_2$ are given by

$$a'_{i,j} = \begin{cases} a_{i,j} + \tilde{a}_{i,0}, & \textit{if } l_j \equiv 3 \bmod 4, \\ a_{i,j}, & \textit{else.} \end{cases}$$

Proof. This is a special case of [Koc02], Th.11.10. In fact, by class field theory it follows that the set $\{\tau_0, \tilde{\tau}_0, \tau_1, \ldots, \tau_n\}$ is a system of generators of $G_S(2)$ and one of the generators $\tilde{\tau}_0$ and $\tau_i, l_i \equiv 3 \mod 4$ can be omitted. We choose to omit $\tilde{\tau}_0$. Then by (3.2.1) the generating set $\{\tau_0, \tau_1, \ldots, \tau_n\}$ is minimal. Since $2 \in S$, we have $Б_S(\mathbb{Q}) = 0$ and a system of defining relations is given by the *local* relations

$$\begin{aligned} r_0 &= \tilde{x}_0^2 [x_0, y_0] r'_0, \\ r_i &= x_i^{l_i - 1}[x_i^{-1}, y_i^{-1}],\ i = 1, \ldots, n, \end{aligned}$$

for some $r'_0 \in F_{(2)}$ where $\tilde{x}_0$ denotes a preimage of $\tilde{\tau}_0$ under π. Any of these relations may be omitted and we decide to ignore r_0. According to the choices we have made and by definition of the numbers $a_{i,j}$ the elements y_i satisfy

$$y_i \equiv x_0^{a_{i,0}} \tilde{x}_0^{\tilde{a}_{i,0}} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} x_j^{a_{i,j}} \mod F_{(2)}.$$

Class field theory implies

$$\tilde{x}_0 \equiv \prod_{\substack{1\le j\le n,\\ l_j \equiv 3 \bmod 4}} x_j \mod F_{(2)},$$

and hence equation (3.1) follows. □

The above minimal presentation for $G_S(2)$ is said to be of **Koch type**. As a consequence, we obtain the following

(3.2.6) Corollary. *The cup-product $H^1(G_S(2)) \times H^1(G_S(2)) \stackrel{\cup}{\to} H^2(G_S(2))$ is trivial if and only if $l_i \equiv 1 \bmod 8,\ i = 1, \ldots, n$ and the Legendre symbols satisfy*

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

Proof. Keeping the notation of (3.2.5), the cup-product vanishes if and only if $R \subseteq F_{(3)}$, i.e. $r_i \in F_{(3)}$ for $1 \le i \le n$. The latter is equivalent to $x_i^{l_i-1} \in F_{(3)}$ and $a'_{i,j} = 0$ for $1 \le i \le n,\ 0 \le j \le n,\ i \ne j$. Noting that for $1 \le i \le n$ we have $x_i^{l_i-1} \in F_{(3)}$ if and only if $l_i \equiv 1 \bmod 4$, the claim follows immediately from the definition of the numbers $a_{i,j}$. □

3.3 Milnor invariants

In order to obtain a more detailed description of the relation structure, we will define so-called **Milnor invariants** of the group $G_S(2)$. Using analogies to link theory, these invariants have been introduced in [Mor02] and [Vog05] in the case of p-extensions over $\mathbb{Q}$ with tame ramification.

Let F be the free pro-2-group on generators $x_0, \ldots, x_n$ and as in (3.2.5) let

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

be a minimal presentation of $G_S(2)$ where $S = \{l_0, \ldots, l_n\}$ with $l_0 = 2$ and odd prime numbers $l_1, \ldots, l_n$. Recall that we have the topological isomorphism $\psi : \mathbb{F}_2[\![F]\!] \xrightarrow{\sim} \mathbb{F}_2^{nc}[\![X]\!]$ and that for any multi-index $I = (i_1, \ldots, i_r)$ with $0 \le i_k \le n$ for $1 \le k \le r$ we have a continuous map $\varepsilon_{I,2} : F \to \mathbb{F}_2$ defined by

$$\psi(f) = 1 + \sum_I \varepsilon_{I,2}(f) X_I.$$

We define a set $\mathcal{M}_n$ of multi-indices of height $n+1$ by

$$\mathcal{M}_n := \big\{(i_1, \ldots, i_r) \in \mathbb{N}_0^r \mid r \in \mathbb{N},\ 0 \le i_k \le n \text{ for } 1 \le k \le r-1,\ 1 \le i_r \le n\big\}$$

and for some $I = (i_1, \ldots, i_r) \in \mathcal{M}_n$ of length $r \ge 2$ we set $I' := (i_1, \ldots, i_{r-1})$.

(3.3.1) Definition. *Let $I = (i_1, \ldots, i_r) \in \mathcal{M}_n$. We define the* **Milnor μ_2-invariant of $G_S(2)$ corresponding to I** *by*

$$\mu_2(I) := \begin{cases} \varepsilon_{I',2}(y_{i_r}), & \text{if } r \geq 2, \\ 0, & \text{if } r = 1 \end{cases}$$

where we keep the notation of (3.2.5)*, i.e. $y_i \in F$ denotes a fixed lift of the Frobenius element $\sigma_i \in G_S(2)$ under $\pi : F \twoheadrightarrow G_S(2)$ for $1 \leq i \neq n$.*

A priori, the definition of $\mu_2(I)$ depends on the chosen presentation for $G_S(2)$, in particular on the elements $y_1, \ldots, y_n$. However, for multi-indices I having minimal length among all multi-indices with non-zero Milnor μ_2-invariant, we will show that $\mu_2(I)$ is actually independent of these choices.*) We need the following

(3.3.2) Lemma. *Let $e = \min_{1 \leq i \leq n}\{v_2(l_i - 1)\}$ where $v_2(\cdot)$ denotes the 2-adic valuation. Let r be an integer with $2 \leq r \leq 2^e$ and assume that $\mu_2(J) = 0$ for all multi-indices $J \in \mathcal{M}_n$ of length $\leq r - 1$. Then, for any $I \in \mathcal{M}_n$ of length r, $\mu_2(I)$ is invariant under the following operations:*

(1) *x_j is replaced by a conjugate for any $0 \leq j \leq n$;*

(2) *x_j is multiplied by an element in $[F, F]$ for any $0 \leq j \leq n$;*

(3) *y_i is replaced by a conjugate for any $1 \leq i \leq n$;*

(4) *y_i is multiplied by a product of conjugates of $x_j^{l_j - 1}$ for any $1 \leq i, j \leq n$;*

(5) *y_i is multiplied by a product of conjugates of $[x_j^{-1}, y_j^{-1}]$ for any $1 \leq i, j \leq n$.*

Proof. For the claims (1), (3), (4) and (5) the proof of [Mor02], Th.3.1.5 carries over immediately and we will only give the proof of the remaining statement (2). Suppose x_j is replaced by $x'_j = x_j[f_1, f_2]$ for some $0 \leq j \leq n,\ f_1, f_2 \in F$. Let X'_j, ω_1, ω_2 be defined by

$$\psi(x'_j) = 1 + X'_j, \quad , \psi(f_i^{-1}) = 1 + \omega_i,\ i = 1, 2.$$

The equation $\psi(f_2^{-1}f_1^{-1}) - \psi(f_1^{-1}f_2^{-1}) = \omega_2\omega_1 - \omega_1\omega_2$ implies

$$\begin{aligned} \psi([f_2, f_1]) &= 1 + \big(\psi(f_2^{-1}f_1^{-1}) - \psi(f_1^{-1}f_2^{-1})\big)\psi(f_2f_1) \\ &= 1 + (\omega_2\omega_1 - \omega_1\omega_2)\psi(f_2f_1) \end{aligned}$$

and hence

$$\begin{aligned} 1 + X_j = \psi(x_j) &= \psi(x'_j)\psi([f_2, f_1]) \\ &= (1 + X'_j)(1 + (\omega_2\omega_1 - \omega_1\omega_2)\psi(f_2f_1)). \end{aligned}$$

This implies $X_j = X'_j + R$ where R is of degree ≥ 2 in the system of variables $X_0, \ldots, X_{j-1}, X'_j, X_{j+1}, \ldots, X_n$. For $1 \leq i \leq n$, we obtain the new Magnus

*) This justifies the term "invariant".

expansion of y_i (i.e. the expansion with respect to this new system of variables) if we replace the factor X_j by $X_j' + R$ each time it occurs in $\psi(y_i)$. Since by assumption $\psi(y_i) - 1$ has degree at least $r-1$, R gives rise to terms of degree $\geq r$ in the new Magnus expansion of y_i and the new expansion has the same coefficients in degree $r-1$ as the old. Since $[F,F]$ is topologically generated by commutators $[f_1, f_2]$, this proves (2). □

The following proposition is crucial for the correspondence between the group $G_S(2)$ and Rédei symbols:

(3.3.3) Proposition. *Let e, r be given as in* (3.3.2). *Then, for any multi-index $I \in \mathcal{M}_n$ of length r, the Milnor number $\mu_2(I)$ is an invariant of the group $G_S(2)$, i.e. it is independent of the choices of the primes $\mathfrak{l}_i$ over l_i for $0 \leq i \leq n$, the elements $\tau_i \in G_S(2)$, $0 \leq i \leq n$, the elements $\sigma_i \in G_S(2)$, $1 \leq i \leq n$ and their lifts $y_i \in F$.*

Proof. Since the decomposition groups of any two primes in $G_S(2)$ over l_i are conjugate, (3.3.2), (1) and (3) show that the Milnor numbers don't depend on the choice of the $\mathfrak{l}_i$. For any $0 \leq i \leq n$, suppose τ_i' is any other element of $G_S(2)$ satisfying the conditions we made for τ_i in the previous chapter. In particular, τ_i and τ_i' agree on $\mathbb{Q}_S(2)^{ab}$, i.e. $\tau_i' \equiv \tau_i \mod [G_S(2), G_S(2)]$. This corresponds to multiplying x_i by an element in $[F,F]$, which by (3.3.2), (2) leaves $\mu_2(I)$ invariant. Next suppose that y_i is replaced by another lift $y_i' \in F$ of σ_i for some $1 \leq i \leq n$. Then $y_i' \equiv y_i \mod R$ and since R is topologically generated by conjugates of $y_j = x_j^{l_j - 1}[x_j^{-1}, y_j^{-1}]$, $1 \leq j \leq n$, by (3.3.2), (4) and (5) this doesn't affect $\mu_2(I)$. Finally assume that for $1 \leq i \leq n$, σ_i' is any element in $G_S(2)$ satisfying the conditions on σ_i. Then σ_i and σ_i' are both lifts of the Frobenius and agree on $\mathbb{Q}_S(2)^{ab}$ and hence $\sigma_i' = \sigma_i \vartheta$ for some $\vartheta \in T_{\mathfrak{l}_i} \cap [G_S(2), G_S(2)]$. The latter group is the closed subgroup generated by $\tau_i^{l_i - 1}$ and hence this corresponds to multiplying y_i by an element in $\langle x_i^{l_i - 1} \rangle$, which again by (3.3.2), (4) doesn't change $\mu_2(I)$. □

(3.3.4) Remark. Comparing (3.3.2) to Morishita's result ([Mor02], Th.3.1.5), we had to prove a slightly stronger algebraic statement. This is due to the fact that, being restricted to the case of tame ramification, Morishita uses a more explicit description of the elements τ_i, σ_i (cf. the remark (3.2.3)).

As an application of (2.2.5) we obtain the following

(3.3.5) Theorem. *Let $S = \{l_0, \ldots, l_n\}$ where $l_0 = 2$ and $l_1, \ldots, l_n$ are odd prime numbers. Assume that $\mu_2(J) = 0$ for all multi-indices $J \in \mathcal{M}_n$ of length $\leq r-1$ for some integer r satisfying $2 \leq r \leq 2^e$ with $e = \min_{1 \leq i \leq n}\{v_2(l_i - 1)\}$. Then there exists a well-defined r-fold Massey product*

$$\langle \cdot, \ldots, \cdot \rangle : H^1(G_S(2))^r \longrightarrow H^2(G_S(2)).$$

For all multi-indices $I = (i_1, \ldots, i_r)$, $0 \leq i_k \leq n$ of length r and all $1 \leq j \leq n$ we have

$$tr_{r_j}\langle \chi_I \rangle = \delta_{i_r, j}\mu_2(I) + \delta_{i_1, j}\mu_2(i_2, \ldots, i_r, i_1) + \binom{l_j - 1}{r}\delta_{I=(j,\ldots,j)}$$

where $\chi_0, \ldots, \chi_n \in H^1(G_S(2))$ denotes the basis dual to the system of generators $\tau_0, \ldots, \tau_n$ of $G_S(2)$ chosen as in (3.2.5).

Proof. By assumption, $\varepsilon_{J',2}(y_j) = 0$ for all $1 \leq j \leq r$ and all multi-indices J of length $1 \leq |J'| \leq r-2$. By definition of the Zassenhaus filtration, we obtain $y_j \in F_{(r-1)}$ and hence $r_j = x_j^{l_j-1}[x_j^{-1}, y_j^{-1}] \in F_{(r)}$, since $x_j \in F_{(r)}$ by assumption. Consequently, we have $R \subseteq F_{(r)}$ and we may apply (2.2.5) for $p = 2$. It follows that

$$\begin{aligned} tr_{r_j}\langle\chi_I\rangle &= \varepsilon_{I,2}(r_j) \\ &= \varepsilon_{I,2}(x_j^{l_j-1}) + \varepsilon_{I,2}([x_j^{-1}, y_j^{-1}]) \\ &= \binom{l_j-1}{r}\delta_{I=(j,\ldots,j)} + \varepsilon_{(i_1),2}(x_j^{-1})\varepsilon_{(i_2,\ldots,i_r),2}(y_j^{-1}) \\ &\quad -\varepsilon_{(i_r),2}(x_j^{-1})\varepsilon_{(i_1,\ldots,i_{r-1}),2}(y_j^{-1}) \\ &= \binom{l_j-1}{r}\delta_{I=(j,\ldots,j)} + \delta_{i_1,j}\mu_2(i_2,\ldots,i_r,i_1) + \delta_{i_r,j}\mu_2(I). \end{aligned}$$

Here we have made use of some general properties of the maps $\varepsilon_{I,2}$ for which we refer to [Vog04], Prop.1.1.22. □

It can easily be seen in the minimal presentation $G_S(2) = F/R$ (see (3.2.5)) $R \subseteq F_{(r)}$ holds if and only if $y_j \in F_{(r-1)}$, $1 \leq j \leq n$. In the following we are particularly interested in the case where $R \subseteq F_{(3)}$. In this regard we have the following

(3.3.6) Corollary. *Assume that in the minimal presentation $G_S(2) = F/R$ as in* (3.2.5) *the inclusion $R \subseteq F_{(3)}$ holds. Then for any multi-index $I = (i_1, i_2, i_3)$ and for all $1 \leq j \leq n$ we have*

$$tr_{r_j}\langle\chi_{i_1}, \chi_{i_2}, \chi_{i_3}\rangle = \begin{cases} \mu_2(i_1,i_2,i_3), & \text{if } j = i_3, j \neq i_1, \\ \mu_2(i_2,i_3,i_1), & \text{if } j = i_1, j \neq i_3, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. This follows immediately from (3.3.5) noting that $R \subseteq F_{(3)}$ implies $e \geq 2$ and hence for all $1 \leq j \leq n$ the binomial coefficient $\binom{l_j-1}{3}$ vanishes mod 2. □

3.4 Rédei symbols

We make the following notational convention: If k is a number field, we denote its ring of integers by $\mathcal{O}_k$. By $\mathcal{D}$ we denote the set of all discriminants of real quadratic number fields

$$\mathcal{D} := \{D_{k|\mathbb{Q}} |\ k \text{ real quadratic}\}.$$

The next proposition follows immediately from the classical Hasse-Minkowski theorem:

(3.4.1) Proposition. *Let $a_1, a_2 \in \mathcal{D}$, then the diophantine equation*

$$\begin{gathered} x^2 - a_1 y^2 - a_2 z^2 = 0, \\ x, y, z \in \mathbb{Z},\ (x, y, z) = 1,\ 2 \mid y,\ x + y\sqrt{a_1} \equiv 1 \mod 4\mathcal{O}_{\mathbb{Q}(\sqrt{a_1})} \end{gathered} \tag{3.2}$$

admits a solution if the following holds:

(i) *a_1 and a_2 are not both negative,*

(ii) $\left(\frac{a_i}{p}\right)_2 = 1$ *for all prime numbers $p \mid a_1 a_2,\ p \nmid a_i,\ i = 1, 2$,*

(iii) $\left(\frac{-a_1' a_2'}{p}\right)_2 = 1$ *for all prime numbers $p \mid (a_1, a_2)$ where $a_i' := a_i/p,\ i = 1, 2$,*

(iv) $2 \nmid a_2$.

For the definition of the Rédei symbol $[\cdot, \cdot, \cdot]$ we need the following notation:

(3.4.2) Definition. *Let k be a number field, $\alpha \in k$ and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_k$. Then we set*

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

(3.4.3) Proposition. *Let $a_1, a_2 \in \mathcal{D}$ satisfying the conditions* (i) *to* (iii) *of proposition* (3.4.1) *and assume that furthermore we have the condition*

(iv') $2 \nmid a_1$ *or* $2 \nmid a_2$.

Then there exists an element $\alpha_2 \in k_1 := \mathbb{Q}(\sqrt{a_1})$ satisfying the following properties:

(1) $N_{k_1|\mathbb{Q}}(\alpha_2) = a_2 z^2$ *for some $z \in \mathbb{Z}$,*

(2) $N_{k_1|\mathbb{Q}}(D_{k_{12}|k_1}) = a_2$ *where $k_{12} := k_1(\sqrt{\alpha_2})$ and $D_{k_{12}|k_1}$ denotes the discriminant of the extension $k_{12}|k_1$.*

In addition assume that $a_3 > 1$ is a prime number such that $(a_1, a_2, a_3) = 1$ and for any prime number $p \mid a_1 a_2 a_3$ the following properties are satisfied:

(ii)' $\left(\frac{a_i}{p}\right)_2 = 1$ *if $p \nmid a_i,\ i = 1, 2, 3$ except in the case $i = 3,\ p = 2$,*

(iii)' $\left(\frac{-a_i' a_j'}{p}\right)_2 = 1$ *if $p \mid (a_i, a_j),\ 1 \le i < j \le 3$ where $a_i' := a_i/p,\ i = 1, 2, 3$ except in the case $j = 3,\ p = 2$.*

Then there exists a prime ideal $\mathfrak{a}_3$ in k_1 above a_3 such that $\mathfrak{a}_3$ is unramified in k_{12}. Furthermore, for all such choices of α_2 and $\mathfrak{a}_3$, the symbol $\left(\frac{\alpha_2|k_1}{\mathfrak{a}_3}\right)$ yields the same (non-zero) value.

Proof. First suppose $2 \nmid a_2$ and let (x, y, z) be a solution of the Diophantine equation (3.2) as given in (3.4.1). Then $\alpha_2 := x + y\sqrt{a_1} \in k_1$ satisfies conditions (1) and (2) (whereas the first condition is obvious, the second one requires a thorough examination of the discriminant for which we refer the reader to [Réd38]). Now assume that $2 \nmid a_1$ and $\alpha_1 \in k_2 := \mathbb{Q}(\sqrt{a_2})$ satisfies conditions (1) and (2) after replacing a_2 by a_1. Then again by [Réd38] the element

$$\alpha_2 := Tr_{k_2|\mathbb{Q}}(\alpha_1) + 2\sqrt{N_{k_2|\mathbb{Q}}(\alpha_1)} = (\sqrt{\alpha_1} + \sqrt{\overline{\alpha}_1})^2 \in k_1$$

satisfies conditions (1) and (2).

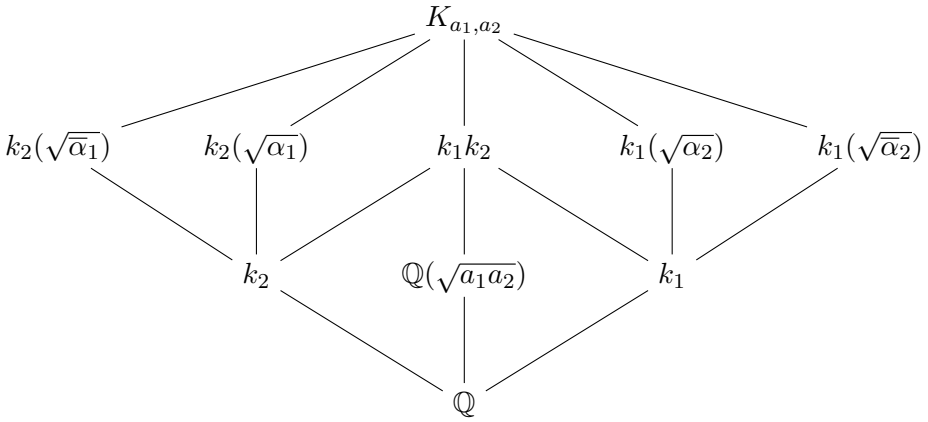
For the second part of the proposition, i.e. the existence of the ideal $\mathfrak{a}_3$ and the independence of the symbol $\left(\frac{\alpha_2|k_1}{\mathfrak{a}_3}\right)$, we refer to [Réd38], Satz 1. □

(3.4.4) Definition. *Keeping the notations and assumptions of* (3.4.3)*, we define the* **Rédei symbol** $[a_1, a_2, a_3] \in \{\pm 1\}$ *by*

$$[a_1, a_2, a_3] := \left(\frac{\alpha_2|k_1}{\mathfrak{a}_3}\right).$$

We remark that compared to [Vog05] and [Mor02] we use a slightly more general notation of the symbol $[a_1, a_2, a_3]$, which will allow us to involve the prime 2. In the original work [Réd38] even a more general definition is given where the third entry a_3 is not necessarily a prime number. For the applications we have in mind however, the above definition is sufficient.

We define K_{a_1,a_2} to be the Galois closure of $k_1(\sqrt{\alpha_2})$ over $\mathbb{Q}$. If $a_1 \neq a_2$, we have the diagram of fields



where $\overline{\alpha}_i$ denotes the conjugate of α_i, $i = 1, 2$. Clearly, K_{a_1,a_2} is a Galois extension of degree 8 over $\mathbb{Q}$. More precisely, we have the following

(3.4.5) Proposition. *Keeping the notations and assumptions of* (3.4.3)*, the following holds:*

(i) *If $a_1 \neq a_2$, then the Galois group $G(K_{a_1,a_2}|\mathbb{Q})$ of $K_{a_1,a_2}|\mathbb{Q}$ is the dihedral group of order 8. Let s, t be generators of $G(K_{a_1,a_2}|k_1(\sqrt{\alpha_2}))$ and $G(K_{a_1,a_2}|k_2(\sqrt{\alpha_1}))$ respectively, i.e.*

$$s : \sqrt{a_2} \mapsto -\sqrt{a_2}, \quad t : \sqrt{a_1} \mapsto -\sqrt{a_1}.$$

Then $G(K_{a_1,a_2}|\mathbb{Q})$ admits the presentation

$$G(K_{a_1,a_2}|\mathbb{Q}) = \langle s,t \mid s^2 = t^2 = (st)^4 = 1\rangle.$$

If $a_1 = a_2$, then K_{a_1,a_2} is a cyclic extension of degree 4 over $\mathbb{Q}$.

(ii) *The discriminant of K_{a_1,a_2} is given by*

$$D_{K_{a_1,a_2}|\mathbb{Q}} = \begin{cases} a_1^4 a_2^4, & \text{if } a_1 \neq a_2, \\ a_1^3, & \text{if } a_1 = a_2. \end{cases}$$

In particular, $K_{a_1,a_2}|\mathbb{Q}$ is unramified outside the set of prime divisors of a_1a_2 and the infinite prime.

(iii) *Suppose $2 \nmid a_2$. Then K_{a_1,a_2} is totally real if and only if the chosen solution (x,y,z) of the diophantine equation (3.2) satisfies $x > 0$. If $2 \nmid a_1$, then the same holds by interchanging a_1 and a_2 in (3.2).*

Proof. Under the assumption $a_1 \neq a_2$, one sees that the extension $k_1(\sqrt{\alpha_2})$ is not Galois over $\mathbb{Q}$, hence it follows that $G(K_{a_1,a_2}|\mathbb{Q})$ is a non-abelian group of order 8. Therefore, it is isomorphic to the dihedral group D_4 of order 8, noting that the only other non-abelian group of order 8, the quaternion group, only possesses four non-trivial subgroups all of which are normal. This also yields the presentation of $G(K_{a_1,a_2}|\mathbb{Q})$ in this case. If $a_1 = a_2$, then we have $\sqrt{\overline{\alpha_2}} = \sqrt{a_1/\alpha_2} \in k_1(\sqrt{\alpha_2})$ and hence $k_1(\sqrt{a_2})$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z}$.
The equalities for the discriminant given in (ii) follow from condition (2) in (3.4.3) and an application of the conductor discriminant formula (cf. [Neu99], Ch.VII).

For the proof of (iii) assume $2 \nmid a_2$ and K_{a_1,a_2} is constructed with respect to the solution (x,y,z) of (3.2). Then K_{a_1,a_2} is the decomposition field of the polynomial $X^4 - 2xX^2 + x^2 - y^2a_1$ over $\mathbb{Q}$ and it is totally real if and only if $x + y\sqrt{a_1},\ x - y\sqrt{a_1} > 0$ (where we have chosen a fixed embedding $k_1 \hookrightarrow \mathbb{R}$). Since $x^2 - a_1y^2 = a_2z^2 > 0$, it follows that $|x| > |y\sqrt{a_1}|$ and hence K_{a_1,a_2} is totally real if and only if $x > 0$. Clearly, K_{a_1,a_2} is also the normal closure of $k_2(\sqrt{\alpha_1})$ over $\mathbb{Q}$ and if $2 \nmid a_1$ the same condition holds after interchanging the variables a_1 and a_2. □

After having given the definition of Rédei symbols, we will study their relation to the group $G_S(2)$. In all what follows, let $S = \{l_0, l_1, \ldots, l_n\}$ such that

- $l_0 = 2$ and $l_i \equiv 1 \mod 8,\ i = 1,\ldots,n$,
- $\left(\frac{l_i}{l_j}\right)_2 = 1$ for all $1 \leq i,j \leq n,\ i \neq j$.

Recall that by (3.2.6), it follows that the cup-product

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

vanishes. In other words, the Zassenhaus invariant $\mathfrak{z}(G_S(2))$ is at least 3, cf. (2.3.1). Verifying conditions (i),(ii'),(iii'),(iv') of (3.4.1) and (3.4.3), the following symbols $[\cdot,\cdot,\cdot]$ are defined:

- $[l_i, l_j, l_k]$, if $1 \leq i, j \leq n,\ 0 \leq k \leq n$ except in the case $i = j = k$;
- $[8, l_i, l_j]$, if $1 \leq i \leq n,\ 0 \leq j \leq n$;
- $[l_i, 8, l_j]$, if $1 \leq i \leq n,\ 0 \leq j \leq n$.

(3.4.6) Definition. *For $1 \leq i, j \leq n$ we say that the pair (l_i, l_j) is* **totally real** *if the equation*

$$\begin{gathered} x^2 - l_i y^2 - l_j z^2 = 0, \\ x, y, z \in \mathbb{Z},\ (x, y, z) = 1,\ 2 \mid y,\ x + y\sqrt{l_i} \equiv 1 \mod 4\mathcal{O}_{\mathbb{Q}(\sqrt{l_i})} \end{gathered} \tag{3.3}$$

admits a solution (x, y, z) with $x > 0$. For $1 \leq i \leq n$ we say that (l_0, l_i) and (l_i, l_0) are **totally real** *if the equation*

$$\begin{gathered} x^2 - 8y^2 - l_j z^2 = 0, \\ x, y, z \in \mathbb{Z},\ (x, y, z) = 1,\ 2 \mid y,\ x + 2y\sqrt{2} \equiv 1 \mod 4\mathcal{O}_{\mathbb{Q}(\sqrt{2})} \end{gathered}$$

admits a solution (x, y, z) with $x > 0$.

We introduce the following short notation:

$$\tilde{l}_i := \begin{cases} 8, & \text{if } i = 0, \\ l_i, & \text{if } 1 \leq i \leq n. \end{cases}$$

(3.4.7) Corollary. *Suppose that (l_i, l_j) is totally real for $0 \leq i, j \leq n$ (where not both i and j are 0). Then the field $K_{\tilde{l}_i, \tilde{l}_j}$ defined as above (and chosen with respect to a solution $(x, y, z),\ x > 0$ of the equation (3.3)) is contained in $\mathbb{Q}_S(2)$.*

Proof. This follows directly from (3.4.5) (ii),(iii). □

The property of (l_i, l_j) being totally real is a crucial assumption for the relation between Rédei symbols and Milnor invariants, since in our case $\infty \notin S$, i.e. we do not allow ramification at the infinite prime (together with the fact that our calculations also involve the prime 2, this is an important difference compared to the results of Morishita and Vogel). Thus, one is led to the question under which conditions this property holds for given primes l_i, l_j. Noting that for $1 \leq i \leq n$ the prime l_i can be written as a sum $l_i = y^2 + z^2$ with $y \equiv 0 \mod 4$, we see that (l_i, y, z) is a solution of (3.3) and hence the tuple (l_i, l_i) is always totally real. More generally, for $1 \leq i, j \leq n,\ i \neq j$ the field K_{l_i, l_j} admits a purely arithmetic characterization, which provides useful equivalent conditions to (l_i, l_j) being totally real:

(3.4.8) Proposition. *For $1 \leq i \leq j \leq n,\ i \neq j$ the field K_{l_i, l_j} is the maximal abelian extension of exponent 2 of the biquadratic field $\mathbb{Q}(\sqrt{l_i}, \sqrt{l_j})$ unramified outside the infinite primes. In particular, it is independent of the particular choice of the triple (x, y, z) solving the equation (3.3). Furthermore, the following assertions are equivalent:*

(i) *The pair (l_i, l_j) is totally real.*

(ii) *The class number of* $\mathbb{Q}(\sqrt{l_i}, \sqrt{l_j})$ *is even.*

(iii) *The class number of* $\mathbb{Q}(\sqrt{l_i l_j})$ *is divisible by four.*

(iv) *For the fourth power residue symbol* $\left(\frac{\cdot}{\cdot}\right)_4$ *it holds that*

$$\left(\frac{l_i}{l_j}\right)_4 = \left(\frac{l_j}{l_i}\right)_4.$$

This can be proven using results on the parity of class numbers of totally real biquadratic fields, see [CH88]. Since we will not need this proposition for our application to the group $G_S(2)$, we omit the proof. We can now state and prove the main result of this section relating the Milnor μ_2-invariants of the group $G_S(2)$ to the Rédei symbols of the primes in S.

(3.4.9) Theorem. *Let* $S = \{l_0, \ldots, l_n\}$ *where* $l_0 = 2$ *and* $l_1, \ldots, l_n$ *are prime numbers* $\equiv 1 \bmod 8$ *satisfying* $\left(\frac{l_i}{l_j}\right)_2 = 1,\ 1 \leq i, j \leq n,\ i \neq j$.

(i) *Suppose* $0 \leq i, j \leq n,\ 1 \leq k \leq n$ *such that* $i \neq j$ *and* (l_i, l_j) *is totally real. Then*

$$(-1)^{\mu_2(i,j,k)} = [\tilde{l_i}, \tilde{l_j}, l_k] = \begin{cases} [l_i, l_j, l_k], & \text{if } i, j \neq 0, \\ [8, l_j, l_k], & \text{if } i = 0, \\ [l_i, 8, l_k], & \text{if } j = 0. \end{cases}$$

(ii) *For* $1 \leq i, j \leq n$ *we have*

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

Furthermore, for $1 \leq j \leq n$

$$(-1)^{\mu_2(0,0,j)} = \left(\frac{\alpha | \mathbb{Q}(\sqrt{2})}{\mathfrak{p}}\right)$$

where $\alpha := 2 + \sqrt{2}$ *and* $\mathfrak{p}$ *denotes a prime above* 2 *in* $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$.

Proof. The proof follows the main ideas of [Vog04], Prop.2.1.13-2.1.15. Assume that $i \neq j$ and (l_i, l_j) is totally real. By (3.4.7) we may choose the field $K_{\tilde{l_i}, \tilde{l_j}}$ as a subfield of $\mathbb{Q}_S(2)$. Furthermore, the triple $a_1 := \tilde{l_i}, a_2 := \tilde{l_j}, a_3 := l_j$ satisfies all conditions of (3.4.3) and it follows that there exists a prime $\mathfrak{p}_j$ in $k_1 = \mathbb{Q}(\sqrt{l_i})$ over l_j which is unramified in $k_1(\sqrt{\alpha_2})$. Let

$$G(K_{\tilde{l_i}, \tilde{l_j}} | \mathbb{Q}) = \langle s, t \mid s^2 = t^2 = (st)^4 = 1 \rangle$$

where s, t are chosen as in (3.4.5)(i). Since by (3.4.5)(ii) l_j ramifies in $K_{\tilde{l_i}, \tilde{l_j}}$, it follows that there is a prime $\mathfrak{P}_j$ in $K_{\tilde{l_i}, \tilde{l_j}}$ above l_j such that the inertia group $T_{\mathfrak{P}_j}$ is generated by s. By symmetry, it also follows that there is a prime $\mathfrak{P}_i$ in $K_{\tilde{l_i}, \tilde{l_j}}$ above l_i such that the inertia group $T_{\mathfrak{P}_i}$ is generated by t. We choose primes $\mathfrak{l}_i, \mathfrak{l}_j$ in $\mathbb{Q}_S(2)$ lying above $\mathfrak{P}_i, \mathfrak{P}_j$. For all $0 \leq k \leq n,\ k \neq i, j$, we choose an arbitrary prime in $\mathbb{Q}_S(2)$ above l_k.

As in (3.2.5) we have a minimal presentation $1 \to R \to F \to G_S(2) \to 1$ where F is the free pro-2-group on $x_0, \ldots, x_n$ and x_k maps to $\tau_k \in T_{\mathfrak{l}_k}$ for all $0 \leq k \leq n$. We consider the projection

$$\pi : F \to G_S(2) \to G(K_{\tilde{l}_i,\tilde{l}_j}|\mathbb{Q}).$$

Since by (3.4.5) $K_{\tilde{l}_i,\tilde{l}_j}$ is unramified outside $\{l_i, l_j\}$, we have $\pi(x_k) = 1,\ k \neq i, j$. Furthermore, $\pi(x_i) = t$ (where we keep the notation of (3.4.5), since $\pi(x_i)$ is contained in $T_{\mathfrak{P}_i}$ and must be non-trivial. In fact, if $1 \leq i \leq n$, this follows immediately from the observation that τ_i is a generator of the inertia subgroup $T_{\mathfrak{l}_i} \subseteq G_S(2)$ of $\mathfrak{l}_i$. For $i = 0$ this is no longer the case (the elements $\tau_0, \tilde{\tau}_0$ generate $T_{\mathfrak{l}_0}$ as a normal subgroup of $G_S(2)$, cf. (3.2.4)). Suppose $\pi(x_0) = 1$, then in particular the restriction of τ_0 to $k_1 = \mathbb{Q}(\sqrt{2})$ would be trivial. On the other hand the restriction of τ_0 to $\mathbb{Q}_S(2)^{ab}$ equals $(\hat{g}_0, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$ where $\hat{g}_0$ denotes the idèle whose 2-component is 5 and whose other components are 1. Since $(\hat{g}_0, \mathbb{Q}(\sqrt{2})|\mathbb{Q})$ is the non-trivial element in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$, this contradicts the assumption $\pi(x_0) = 1$. By symmetry we conclude that

$$\pi(x_k) = \begin{cases} t, & \text{if } k = i, \\ s, & \text{if } k = j, \\ 1, & \text{if } k \neq i, j. \end{cases}$$

Assume that $k \neq i, j$ and let $\mathfrak{p}_k$ denote a prime ideal in k_1 above $a_3 = l_k$ unramified in $k_1(\sqrt{\alpha_2})$. Furthermore, let $\mathfrak{P}_k$ denote a prime ideal in k_1k_2 above $\mathfrak{p}_k$. By our assumptions the prime l_k is completely decomposed in k_1k_2 and hence $\mathfrak{p}_k$ splits in $k_1(\sqrt{\alpha_2})$ if and only if $\mathfrak{P}_k$ splits in $k_1k_2(\sqrt{\alpha_2}) = K_{\tilde{l}_i,\tilde{l}_j}$, i.e. we have

$$\left(\frac{\alpha_2|k_1}{\mathfrak{p}_k}\right) = \left(\frac{\alpha_2|k_1k_2}{\mathfrak{P}_k}\right).$$

Noting that $\mathrm{Gal}(K_{\tilde{l}_i,\tilde{l}_j}|k_1k_2)$ is generated by $(st)^2$ and by definition of the element $y_k \in F$, it follows that

$$\pi(y_k) = \begin{cases} (st)^2, & \text{if } [\tilde{l}_i, \tilde{l}_j, l_k] = -1, \\ 1, & \text{if } [\tilde{l}_i, \tilde{l}_j, l_k] = 1. \end{cases}$$

By (3.4.5)(i) the kernel $\tilde{R}$ of $\pi : F \twoheadrightarrow G(K_{\tilde{l}_i,\tilde{l}_j}|\mathbb{Q})$ is generated by $x_i^2, x_j^2, (x_jx_i)^4$ and $x_k,\ k \neq i, j$ as a normal subgroup of F. Noting that the Magnus expansions of these elements are given by

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

where as in (2.2.4) ψ denotes the isomorphism $\mathbb{F}_p[\![F]\!] \xrightarrow{\sim} \mathbb{F}_p\langle\langle X\rangle\rangle$, we see that the maps $\varepsilon_{(i),2}, \varepsilon_{(j),2}, \varepsilon_{(i,j),2}$ vanish identically on $\tilde{R}$. Therefore, if $[\tilde{l}_i, \tilde{l}_j, l_k] = 1$,

we have $\pi(y_k) = 1$, i.e. $y \in \tilde{R}$ and consequently $\mu_2(i,j,k) = \varepsilon_{(i,j),2}(y_k) = 0$. If $[\tilde{l_i}, \tilde{l_j}, l_k] = -1$, then $\pi(y_k) = (st)^2$, i.e. $y_k = (x_j x_i)^2 r$ for some $r \in \tilde{R}$. This yields

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

where we have used [Vog04], Prop.1.1.22 and the equality

$$\psi((x_j x_i)^2) \equiv 1 + X_i^2 + X_j^2 + X_i X_j + X_j X_i \mod \deg \geq 3.$$

Next we consider the case $k = j$, so in particular $j \neq 0$. By definition of the Rédei symbol, if $[\tilde{l_i}, l_j, l_j] = 1$, we have the decomposition

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

with pairwise different prime ideals $\mathfrak{q}_i$. By choice of the prime $\mathfrak{P}_j$ of $K_{\tilde{l_i}, l_j}$, we have $\mathfrak{P}_j \mid \mathfrak{q}_1$ or $\mathfrak{P}_j \mid \mathfrak{q}_2$. The Frobenius automorphism of $\mathfrak{l}_j$ maps to the trivial element of $\mathrm{Gal}(k_1(\sqrt{\alpha_2})|\mathbb{Q})$, i.e. $\pi(y_j) = 1$ or $\pi(y_j) = s$. We recall that the restriction of the image σ_j of y_j in $G_S(2)$ to $\mathbb{Q}_S(2)^{ab}$ is given by $(\hat{l_j}, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$ where $\hat{l_j}$ denotes the idèle whose l_j-component equals l_j and all other components are 1, i.e. by class field theory the restriction of σ_j to $k_2 = \mathbb{Q}(\sqrt{l_j})$ is trivial. Since s maps $\sqrt{l_j}$ to $-\sqrt{l_j}$, the case $\pi(y_j) = s$ cannot occur and in particular $\mu_2(i,j,j) = 0$ holds. If $[\tilde{l_i}, l_j, l_j] = -1$, then l_j decomposes as

$$l_j \mathcal{O}_{k_1(\sqrt{\alpha_2})} = \mathfrak{q}_1 \mathfrak{q}_2{}^3$$

where $\mathfrak{P}_j \mid q_1$. In this case the Frobenius automorphism of $\mathfrak{l}_j$ maps to the non-trivial automorphism of $k_1(\sqrt{\alpha_2})|k_1$ and we have $\pi(y_j) = (st)^2$ or $\pi(y_j) = s(st)^2$ where again the latter case cannot occur, since $s(st)^2$ maps $\sqrt{l_j}$ to $-\sqrt{l_j}$. As in the case $k \neq j$ we conclude that $\mu_2(i,j,j) = \varepsilon_{(i,j),2}(y_j) = 1$.

By reason of symmetry also $(-1)^{\mu_2(i,j,i)} = [l_i, \tilde{l_j}, l_i]$ holds for $i \geq 1,\ i \neq j$ which concludes the proof of (i).

In order to determine the Milnor invariant $\mu_2(i,i,j),\ 1 \leq i,j \leq n,\ i \neq j$, first note that by (3.4.5) $K_{l_i,l_i}|\mathbb{Q}$ is a cyclic extension of degree 4 and that by (3.4.7) we may assume $K_{l_i,l_i} \subseteq \mathbb{Q}_S(2)$. More precisely, K_{l_i,l_i} is unramified outside l_i and totally ramified at l_i. As in the proof of (i) we can choose a minimal presentation $1 \to R \to F \to G_S(2) \to 1$, such that the projection

$$\pi : F \to G_S(2) \to G(K_{l_i,l_i}|\mathbb{Q}).$$

maps x_k to 1 for $k \neq i$ and x_i to s where s is a generator of $G(K_{l_i,l_i}|\mathbb{Q})$. By definition it holds that

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

Again let $\tilde{R}$ be the kernel of $\pi : F \twoheadrightarrow G(K_{\tilde{l}_i,\tilde{l}_j}|\mathbb{Q})$, i.e. $\tilde{R}$ is the closed normal subgroup of F generated by $x_i^4, x_k,\ k \neq i$. Since

$$\psi(x_i^4) = 1 + X_i^4,$$

we see that in particular $\varepsilon_{(i,i),2}, \varepsilon_{i,2}$ vanish on $\tilde{R}$. Hence if $\pi(y_j) = 1$, we have $\mu_2(i,i,j) = \varepsilon_{(i,i),2}(y_j) = 0$. If $\pi(y_j) = s^2$, then $y_j = x_i^2 r$ for some $r \in \tilde{R}$ which implies that

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

Since $\pi(y_i) = 1$, by the same argument we obtain $\mu_2(i,i,i) = 0$, showing the first part of (ii).

Finally let $k := \mathbb{Q}(\sqrt{2})$ and $K := k(\sqrt{\alpha})$ where $\alpha = 2+\sqrt{2}$. Then K is totally real and cyclic of degree 4 over $\mathbb{Q}$. Furthermore, we have $D_{K|\mathbb{Q}} = 2048 = 2^{11}$, so $K|\mathbb{Q}$ is unramified outside 2 and totally ramified at 0. If s is a generator of $G(K|\mathbb{Q})$, as above we have a projection $\pi : F \to G_S(2) \to G(K|\mathbb{Q})$, such that for all $1 \leq j \leq n$ we have

$$\pi(y_j) = \begin{cases} s^2, & \text{if } \left(\frac{\alpha|k}{\mathfrak{p}}\right) = -1, \\ 1, & \text{if } \left(\frac{\alpha|k}{\mathfrak{p}}\right) = 1 \end{cases}$$

where $\mathfrak{p}$ denotes a prime above 2 in $\mathcal{O}_k$. Now the the proof of the first part of (ii) carries over immediately. □

We calculated the Milnor invariants $\mu_2(0,0,j)$ by studying the decomposition behavior of l_j in $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. Observing that $\mathbb{Q}(\sqrt{2+\sqrt{2}}) = \mathbb{Q}(\zeta_{16} + \overline{\zeta_{16}})$ is the maximal real subfield of $\mathbb{Q}(\zeta_{16})$ where ζ_{16} denotes a primitive 16th root of unity, it follows that for $1 \leq j \leq n$ we have

$$\mu_2(0,0,j) = \begin{cases} 0, & \text{if } l_j \equiv 1 \mod 16, \\ 1, & \text{if } l_j \equiv 9 \mod 16. \end{cases}$$

Thus, we have the following

(3.4.10) Corollary. *Let $S = \{l_0, \ldots, l_n\}$ where $l_0 = 2$ and $l_1, \ldots, l_n$ are prime numbers $\equiv 1 \bmod 8$ satisfying $\left(\frac{l_i}{l_j}\right)_2 = 1,\ 1 \leq i,j \leq n,\ i \neq j$. Then the group $G_S(2)$ has Zassenhaus invariant $\mathfrak{z}(G_S(2)) \geq 3$ and the triple Massey product*

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

is given by

$$(-1)^{tr_{r_m}\langle \chi_i, \chi_j, \chi_k \rangle} = \begin{cases} [\tilde{l_i}, \tilde{l_j}, l_k], & \text{if } m = k, m \neq i, \\ [\tilde{l_j}, \tilde{l_k}, l_i], & \text{if } m = i, m \neq k, \\ 1, & \text{otherwise} \end{cases}$$

for all $1 \leq m \leq n$ *and provided that* (l_i, l_j) *and* (l_j, l_k) *are totally real where by abuse of notation we set*

$$[\tilde{l_0}, \tilde{l_0}, l_k] := \begin{cases} 1, & \text{if } l_k \equiv 1 \mod 16, \\ -1, & \text{if } l_k \equiv 9 \mod 16 \end{cases}$$

and $\chi_0, \ldots, \chi_n \in H^1(G_S(2))$ *denotes the basis dual to the system of generators* $\tau_0, \ldots, \tau_n$ *of* $G_S(2)$ *chosen as in* (3.2.5).

Proof. This is an immediate consequence of (3.3.6) and (3.4.9). □

(3.4.11) Remark. Having developed a link between triple Massey products and Rédei symbols, the shuffle property of the Massey product also implies certain symmetry relations of the Rédei symbols. This fact, which can also be shown in a direct way, is actually one of the central results in Rédei's original work, cf. [Réd38], §2.

Together with (2.2.9), the above result yields a complete description of the relations of $G_S(2)$ modulo the 4-th step of the Zassenhaus filtration, provided all pairs of primes in S are totally real. This will finally provide arithmetic examples of *mild* pro-2-groups with trivial cup-product.

(3.4.12) Theorem. *Let* $S = \{l_0, l_1, \ldots, l_n\}$ *for some* $n \geq 1$ *and prime numbers* $l_0 = 2,\ l_i \equiv 9 \mod 16,\ i = 1, \ldots, n$, *such that the Legendre symbols satisfy*

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

Then $G_S(2)$ *is a mild pro-2-group with* $h^1(G_S(2)) = n + 1,\ h^2(G_S(2)) = n$ *and Zassenhaus invariant* $\mathfrak{z}(G_S(2)) = 3$.

Proof. We have already seen that $\mathfrak{z}(G_S(2)) \geq 3$. Consider the basis $\chi_0, \ldots, \chi_n \in H^1(G_S(2))$ as given in (3.4.10). Since by assumption $l_1 \equiv \ldots \equiv l_n \equiv 9 \mod 16$, by (3.4.10) we obtain

$$tr_{r_m}\langle \chi_0, \chi_0, \chi_k \rangle = tr_{r_m}\langle \chi_k, \chi_0, \chi_0 \rangle = \delta_{mk} = \begin{cases} 1, & \text{if } m = k, \\ 0, & \text{if } m \neq k \end{cases}$$

for $m = 1, \ldots, n$.*) In particular, the triple Massey product is non-zero and therefore $\mathfrak{z}(G_S(2)) = 3$. We apply (2.3.2) with respect to the subspaces

$$U = \langle \chi_1, \ldots, \chi_n \rangle,\ V = \langle \chi_0 \rangle$$

and $e = 1$. Noting that $tr_{r_1}, \ldots, tr_{r_n}$ is a basis of $H^2(G_S(2))^\vee$, the above observation implies that the $\mathbb{F}_2$-linear map $U \otimes V \otimes V \longrightarrow H^2(G_S(2))$ is surjective (even an isomorphism by reason of dimensions), i.e. condition (b) of (2.3.2) is satisfied. Furthermore $\langle \chi_0, \chi_0, \chi_0 \rangle = 0$, hence condition (a) also holds and we conclude that $G_S(2)$ is mild with respect to the Zassenhaus filtration. □

*) Here we have used the shuffle property of the triple Massey product, see (2.2.8).

Note that in the above theorem we didn't have to assume the total realness of the pairs (l_i, l_j), $1 \le i, j \le n$, since in order to prove the mildness of $G_S(2)$ we only had to calculate the Massey products $\langle \chi_0, \chi_0, \chi_k \rangle$ which are determined by the ramification behaviour in the totally real extension $\mathbb{Q}(\zeta_{16} + \overline{\zeta_{16}})$. In the following example, we determine the triple Massey product completely.

(3.4.13) Example. Let $S = \{l_0, \ldots, l_4\}$ where

$$l_0 = 2,\ l_1 = 313,\ l_2 = 457,\ l_3 = 521.$$

We have

$$\left(\frac{313}{457}\right)_2 = \left(\frac{313}{521}\right)_2 = \left(\frac{457}{521}\right)_2 = 1$$

and a calculation of solutions of the diophantine equation (3.3) shows that all pairs (l_i, l_j) are totally real. Using the computational algebra system [MAGMA] we find that the symbol $[l_i, l_j, l_k]$ is -1 for all permutations of the triples

$$(i, j, k) = (1, 1, 3),\ (1, 2, 3),\ (1, 3, 3),$$

furthermore $[\tilde{l}_i, \tilde{l}_j, l_k]$ is -1 for all triples

$$\begin{aligned}(i, j, k) \;=\; & (0, 0, 1),\ (0, 0, 2),\ (0, 0, 3),\ (0, 1, 1),\\ & (0, 2, 2),\ (0, 3, 3),\ (0, 2, 3),\ (0, 3, 2)\end{aligned}$$

and $[\tilde{l}_i, \tilde{l}_j, l_k] = 1$ in all other cases. Combining (3.4.10) with (2.2.9), we see that $G_S(2)$ admits a minimal presentation $1 \to R \to F \to G_S(2) \to 1$ where F is the free pro-2-group on $x_0, \ldots, x_3$ and the generating relations $r_1, \ldots, r_3 \in R$ satisfy

$$\begin{aligned}
r_1 \;\equiv\;& [[x_0, x_1], x_0]\ [[x_0, x_1], x_1]\ [[x_1, x_3], x_1]\ [[x_1, x_3], x_3]\\
& [[x_2, x_3], x_1] \quad \bmod F_{(4)},\\
r_2 \;\equiv\;& [[x_0, x_2], x_0]\ [[x_0, x_2], x_2]\ [[x_0, x_3], x_2]\ [[x_1, x_3], x_2] \quad \bmod F_{(4)},\\
r_3 \;\equiv\;& [[x_0, x_3], x_0]\ [[x_0, x_3], x_2]\ [[x_0, x_3], x_3]\ [[x_1, x_3], x_1]\\
& [[x_1, x_3], x_2]\ [[x_1, x_3], x_3]\ [[x_2, x_3], x_0]\ [[x_2, x_3], x_1] \quad \bmod F_{(4)}.
\end{aligned}$$

By (3.4.12), $G_S(2)$ is mild.

We conclude by giving an example of a group $G_S(2)$ with Zassenhaus invariant $\mathfrak{z}(G_S(2)) \ge 4$.

(3.4.14) Example. Let $S = \{l_0, l_1, l_2\}$ where

$$l_0 = 2,\ l_1 = 113,\ l_2 = 593.$$

Computations using [MAGMA] show that all pairs of primes in S satisfy are totally real and that all Rédei symbols are equal to 1. By (3.4.10) and the shuffle property it follows that the triple Massey product of $G_S(2)$ is identically zero, i.e. we have $\mathfrak{z}(G_S(2)) \ge 4$.

3.5 The group $G_S^T(2)$ - Fabulous pro-p-groups with trivial cup-product

The groups $G_S(2)$ considered in the previous section are always of cohomological dimension 2 and have infinite abelianization (cf. (3.2.1)). However, it would be of great interest to give examples of (mild) pro-p-groups having trivial cup-product and *finite* abelianization. More precisely, we are looking for so-called **fab groups**, which are defined as follows:

(3.5.1) Definition. *A pro-p-group G is* **fab** *if for every open subgroup $H \subseteq G$ the abelianization $H^{ab} = H/[H,H]$ is finite. We call G* **fabulous** *if it is mild and fab.*

Note that our definition of a fabulous group is a slight generalization of the notion suggested by J. Labute (cf. [Lab08]). Trivial examples of fab groups are finite pro-p-groups. Fabulous groups occur as groups of the form $G_S(p)$ in the tame and mixed case and as Galois groups of the form $G_S^T(p)$ (cf. [Sch07], [Sch06], [Sch10], [Vog06], [Vog07], [Win07]). A nice feature of fabulous groups is the fact that they are duality groups. This follows from the following well-known result, e.g. see [Win07], Prop.1.3:

(3.5.2) Proposition. *Let G be a fab pro-p-group of cohomological dimension 2. Then G is a duality group and the strict cohomological dimension is $\mathrm{scd}\, G = 3$.*

Let k be a number field and S, T disjoint sets of primes of k. We denote by $G_S^T(p)$ the Galois group of the maximal p-extension $k_S^T(p)$ of k which is unramified outside S and completely decomposed at the primes above T. These groups carry important arithmetic information. For example, dealing with the more general groups $G_S^T(p)$ instead of $G_S(p)$ only is crucial for the proof of (2.3.5) by A. Schmidt (cf. [Sch10], Th.1.1) in the general case (i.e. without restriction on roots of unity and p-divisibility of class numbers).

In [Win07], K. Wingberg has shown that one can construct many examples of fabulous groups of the form $G_S^T(p)$ over totally real number fields for an odd prime p, such that $G_S^T(p)$ is a pro-p **Schur** group, i.e. $h^1(G_S^T(p)) = h^2(G_S^T(p))$. More precisely, S must be a finite set of primes containing the primes S_p lying above p and the order of T must equal the number of independent $\mathbb{Z}_p$-extensions of k. Furthermore, one has to assume Leopoldt's conjecture for p and all finite extensions of k lying inside $k_S^T(p)$ (for the exact statement see [Win07], Cor.2.6).

We return to the case $k = \mathbb{Q}$, $p = 2$. We will construct an example of a fabulous group of the form $G_S^T(2)$ having trivial cup product and being a pro-p Schur group with $h^1(G_S^T(2)) = h^2(G_S^T(2)) = 3$. As in the previous section, suppose $S = \{l_0, l_1, \ldots, l_n\}$ for some $n \geq 1$ and prime numbers $l_0 = 2$, $l_i \equiv 1 \mod 8$, $i = 1, \ldots, n$, such that the Legendre symbols satisfy

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

(3.5.3) Theorem. *Let $T = \{q\}$ where $q \notin S$ is a prime number $\equiv 5 \mod 8$, such that the following conditions are satisfied:*

- $\left(\frac{q}{l_i}\right)_2 = 1$ *for all* $i = 1, \ldots, n-1$,
- $\left(\frac{q}{l_n}\right)_2 = -1$.

Then for the pro-2-group $G_S^T(2)$ *the following holds:*

(i) $G_S^T(2)$ *has generator rank* $h^1(G_S^T(2)) = n$ *and relator rank* $h^2(G_S^T(2)) \leq n$ *and the cup-product*

$$H^1(G_S^T(2)) \times H^1(G_S^T(2)) \stackrel{\cup}{\to} H^2(G_S^T(2))$$

vanishes, i.e. $\mathfrak{z}(G_S^T(2)) \geq 3$.

(ii) *Assume that the pair* (l_i, l_j) *is totally real for all* $0 \leq i, j \leq n,\ i \neq j$. *Then* $G_S^T(2)$ *possesses a presentation* $G_S^T(2) = \langle \overline{x}_1, \ldots, \overline{x}_n \mid \overline{r}_1, \ldots, \overline{r}_n \rangle$ *such that the triple Massey product*

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

is given by

$$(-1)^{tr_{\overline{r}_m}\langle \overline{\chi}_i, \overline{\chi}_j, \overline{\chi}_k \rangle} = \begin{cases} [l_i, l_j, l_k], & \text{if } m = k,\ m \neq i,\ i, j \neq n, \\ [l_i, l_j, l_k] \cdot [8, l_j, l_k], & \text{if } m = k,\ i = n, j \neq n, \\ [l_i, l_j, l_k] \cdot [8, l_j, l_k], & \text{if } m = k,\ m \neq i,\ i \neq n = j, \\ [l_i, l_j, l_k] \cdot [8, l_j, l_k], & \text{if } m = k,\ i = j = n, \\ [l_j, l_k, l_i], & \text{if } m = k,\ m \neq i, i, j \neq n, \\ [l_j, l_k, l_i] \cdot [8, l_j, l_k], & \text{if } m = i,\ k = n,\ j \neq n, \\ [l_j, l_k, l_i] \cdot [8, l_k, l_i], & \text{if } m = i,\ m \neq k,\ k \neq n = j, \\ [l_j, l_k, l_i] \cdot [8, 8, l_i], & \text{if } m = i,\ k = j = n, \\ 1, & \text{otherwise} \end{cases}$$

for $m = 1, \ldots, n-1$ *and*

$$(-1)^{tr_{\overline{r}_n}\langle \overline{\chi}_i, \overline{\chi}_j, \overline{\chi}_k \rangle} = \begin{cases} [l_i, l_j, l_n], & \text{if } k = n,\ i, j \neq n, \\ [l_i, l_j, l_n] \cdot [l_i, 8, l_n], & \text{if } k = j = n,\ i \neq n, \\ [l_j, l_k, l_n], & \text{if } i = n,\ k, j \neq n, \\ [l_j, l_k, l_n] \cdot [8, l_k, l_n], & \text{if } i = j = n,\ k \neq n \\ 1, & \text{otherwise} \end{cases}$$

where $\{\overline{\chi}_1, \ldots, \overline{\chi}_n\}$ *denotes the basis of* $H^1(G_S^T(2))$ *dual to* $\overline{x}_1, \ldots, \overline{x}_n$.

Assuming in addition that the Leopoldt conjecture holds for all number fields k *contained in* $\mathbb{Q}_S^T(2)$ *and the prime* 2, *we have:*

(iii) $G_S^T(2)$ *is a fab pro-2-group and* $h^2(G_S^T(2)) = n$.

Proof. Keeping the notation and choices of the elements $\tau_0, \ldots, \tau_n \in G_S(2)$ as in the previous sections, by (3.2.5) the group $G_S(2)$ has a minimal presentation

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

where F is the free pro-p-group on $x_0, \ldots, x_n$, π maps x_i to τ_i and R is generated by $r_i = x_i^{l_i - 1}[x_i^{-1}, y_i^{-1}]$, $i = 1, \ldots, n$ as closed normal subgroup of F. We fix a prime $\mathfrak{Q}$ of $\mathbb{Q}_S(2)$ lying above q and denote by $G_{\mathfrak{Q}} \subseteq G_S(2)$ the decomposition group of $\mathfrak{Q}$, which is generated as closed subgroup by the Frobenius automorphism $\sigma_{\mathfrak{Q}}$ of $\mathfrak{Q}$. Furthermore we choose an arbitrary lift $r_{\mathfrak{Q}} \in \pi^{-1}(\sigma_{\mathfrak{Q}})$. We obtain a commutative exact diagram

$$\begin{array}{ccccccccc} & & & & & & 1 & & \\ & & & & & & \downarrow & & \\ & & & & & & (G_{\mathfrak{Q}}) & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & R & \longrightarrow & F & \xrightarrow{\pi} & G_S(2) & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & \tilde{R} & \longrightarrow & F & \xrightarrow{\tilde{\pi}} & G_S^T(2) & \longrightarrow & 1 \\ & & & & & & \downarrow & & \\ & & & & & & 1 & & \end{array} \tag{3.4}$$

where $\tilde{R}$ denotes the closed normal subgroup of F generated by $r_1, \ldots, r_n, r_{\mathfrak{Q}}$ and $(G_{\mathfrak{Q}}) \subseteq G_S(2)$ is the (closed) normal subgroup generated by $G_{\mathfrak{Q}}$. Let $\hat{q} \in I = I_{\mathbb{Q}}$ denote the idèle of $\mathbb{Q}$ whose q-th component equals q and all other components are 1. Then the restriction of $\sigma_{\mathfrak{Q}}$ to $\mathbb{Q}_S[2]$, the maximal abelian subextension of exponent 2 in $\mathbb{Q}_S(2)|\mathbb{Q}$, is given by $(\hat{q}, \mathbb{Q}_S[2]|\mathbb{Q})$. By choice of q, we have the idèlic congruence

$$\begin{aligned} \hat{q} \quad &= (1, \ldots, 1, q, 1, \ldots) \\ &\equiv (\frac{1}{q}, \ldots, \frac{1}{q}, 1, \frac{1}{q}, \ldots) \\ &\equiv \hat{g}_0 \hat{g}_n \mod I_S I^2 \mathbb{Q}^\times \end{aligned}$$

where

$$I_S := \prod_{l \in S} \{1\} \times \prod_{l \notin S} U_l$$

and $\hat{g}_i$ are the idèles as constructed in the definition of the generators τ_i of $G_S(2)$ (cf. (3.2.5)). Since by class field theory $\mathrm{Gal}(\mathbb{Q}_S[2]|\mathbb{Q}) = G_S(2)/(G_S(2))_{(2)} \cong I/I_S I^2 \mathbb{Q}^\times$, it follows that

$$\sigma_{\mathfrak{Q}} \equiv \tau_0 \tau_n \mod (G_S(2))_{(2)}, \quad r_{\mathfrak{Q}} \equiv x_0 x_n \mod F_{(2)}.$$

In particular, we see that $r_{\mathfrak{Q}} \notin F_{(2)}$ and therefore the presentation of $G_S^T(2)$ given by the bottom horizontal line of diagram (3.4) is *not* minimal. In order to obtain a minimal presentation, let $\overline{F}$ be the free pro-p-group on n generators $\overline{x}_1, \ldots, \overline{x}_n$. Noting that $r_{\mathfrak{Q}}, x_1, \ldots, x_n$ is a basis of F, the mapping $r_{\mathfrak{Q}} \longmapsto 1$, $x_i \longmapsto \overline{x}_i$, $i = 1, \ldots, n$ yields a well-defined surjective homomorphism $\psi : F \longrightarrow \overline{F}$. Let s be the section of ψ mapping $\overline{x}_i$ to x_i, $i = 1, \ldots, n$ and set

$\overline{R} := \psi(\tilde{R})$. We obtain the commutative exact diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \tilde{R} & \longrightarrow & F & \xrightarrow{\tilde{\pi}} & G_S^T(2) & \longrightarrow & 1 \\ & & \downarrow & & \psi\downarrow & \nwarrow s & & & \\ 1 & \longrightarrow & \overline{R} & \longrightarrow & \overline{F} & & & & \end{array}$$

where the composition $\tilde{\pi}\circ s$ is surjective, since $x_0 \equiv x_n \mod \tilde{R}F_{(2)}$ and therefore $G_S^T(2)$ is generated by the images of $\tau_1, \ldots, \tau_n$. Clearly, $\overline{R}$ is generated by $\overline{r}_i := \psi(r_i),\ i = 1, \ldots, n$. By the assumptions made for the primes in S, we have $r_i \in F_{(3)}$ and therefore also $\overline{R} \subseteq \overline{F}_{(3)}$. In particular, we obtain the *minimal* presentation

$$G_S^T(2) = \overline{F}/\overline{R} = \langle \overline{x}_1, \ldots, \overline{x}_n \mid \overline{r}_1, \ldots, \overline{r}_n \rangle$$

for $G_S^T(2)$. This yields $h^1(G_S^T(2)) = n,\ h^2(G_S^T(2)) \leq n$ and the cup-product $H^1(G_S^T(2)) \times H^1(G_S^T(2)) \stackrel{\cup}{\to} H^2(G_S^T(2))$ is trivial, i.e. we have proven (i).*)

Next we calculate the triple Massey product of $G_S^T(2)$. Let $\chi_0, \ldots, \chi_n \in H^1(G_S(2)) = H^1(F)$ and $\overline{\chi}_1, \ldots, \overline{\chi}_n$ denote the bases dual to $x_0, \ldots, x_n$ and $\overline{x}_1, \ldots, \overline{x}_n$ respectively. Since $\psi(x_0) \equiv \psi(x_n) = \overline{x}_n \mod F_{(2)}$, the inflation map $inf : H^1(G_S^T(2)) \longrightarrow H^1(G_S(2))$ is given by

$$\overline{\chi}_i \longmapsto \chi_i,\ i = 1, \ldots, n-1, \quad \overline{\chi}_n \longmapsto \chi_0 + \chi_n.$$

Furthermore we have the surjective homomorphism

$$inf^\vee :\ H^2(G_S(2))^\vee \twoheadrightarrow H^2(G_S^T(2))^\vee,$$

$$tr_{r_i} \longmapsto tr_{\overline{r}_i},\ i = 1, \ldots, n.$$

Since by (2.2.3) (i) the 3-fold Massey product commutes with the inflation maps, for any $1 \leq i, j, k, m \leq n$ we have

$$\begin{aligned} tr_{\overline{r}_m}\langle \overline{\chi}_i, \overline{\chi}_j, \overline{\chi}_k \rangle &= inf^\vee(tr_{r_m})\langle \overline{\chi}_i, \overline{\chi}_j, \overline{\chi}_k \rangle \\ &= tr_{r_m} inf\, \langle \overline{\chi}_i, \overline{\chi}_j, \overline{\chi}_k \rangle \\ &= tr_{r_m}\langle inf\, \overline{\chi}_i, inf\, \overline{\chi}_j, inf\, \overline{\chi}_k \rangle. \end{aligned}$$

We can now deduce (ii) by a direct calculation using (3.4.10) and the shuffle property of the triple Massey product.

Let $H \subseteq G_S^T(2)$ be an open subgroup and $k \subseteq \mathbb{Q}_S^T(2)$ the corresponding fixed field. Assume that H^{ab} is infinite. Since it is a finitely generated, it has a

*) Comparing our results to the general formula for the generator and relation ranks of the groups $G_S^T(p)$ given in [NSW08], Th.10.7.10, we have shown that the ***Kummer group*** $\mathrm{B}_S^{S\cup T}$ is trivial in our case. This can be alternatively justified as follows: By the assumption on the Legendre symbols $\left(\frac{q}{l_i}\right)_2$ we have made, the prime q is *not* completely decomposed in the extension $\mathbb{Q}_S[2]|\mathbb{Q}$, hence $h^1(G_S^T(2)) < h^1(G_S(2))$ and since $\#T = 1$, it follows that $h^1(G_S^T(2)) = h^1(G_S(2)) - 1$ (see also [Gä08], Th.7.1.1).

quotient isomorphic to $\mathbb{Z}_2$. Assuming that the Leopoldt conjecture holds for k and 2, this must be the cyclotomic $\mathbb{Z}_2$-extension, since k is totally real (e.g. see [NSW08], Th.10.3.6). However, the primes above q cannot be completely decomposed in the cyclotomic $\mathbb{Z}_2$-extension of k which yields a contradiction. Hence H^{ab} is finite showing that $G_S^T(2)$ is a fab group. In particular, $(G_S^T(2))^{ab}$ is finite. Consequently $h^2(G_S^T(2)) \geq h^1(G_S^T(2))$ and hence equality holds. □

(3.5.4) Example. The sets $S = \{2, 17, 7489, 15809\}, T = \{5\}$ satisfy the assumptions made in (3.5.3). Choosing $\overline{x}_i, \overline{r}_i, \overline{\chi}_i$ as in (3.5.3), computations of the Rédei symbols with [MAGMA] show that

$$\begin{aligned}
tr_{\overline{r}_1}\langle\overline{\chi}_i,\overline{\chi}_j,\overline{\chi}_k\rangle \neq 0 \;\Leftrightarrow\; (i,j,k) \in\; & \{(1,1,3),(1,2,3),(1,3,2),(1,3,3),(2,3,1),\\
& (3,1,1),(3,2,1),(3,3,1)\},\\
tr_{\overline{r}_2}\langle\overline{\chi}_i,\overline{\chi}_j,\overline{\chi}_k\rangle \neq 0 \;\Leftrightarrow\; (i,j,k) \in\; & \{(1,3,2),(2,1,3),(2,3,1),(3,1,2)\},\\
tr_{\overline{r}_3}\langle\overline{\chi}_i,\overline{\chi}_j,\overline{\chi}_k\rangle \neq 0 \;\Leftrightarrow\; (i,j,k) \in\; & \{(1,1,3),(1,2,3),(2,1,3),(3,1,1),\\
& (3,1,2),(3,2,1)\}.
\end{aligned}$$

Hence in the minimal presentation $1 \to R \to F \to G_S^T(2) \to 1$ the generating relations $\overline{r}_1, \overline{r}_2, \overline{r}_3 \in R$ satisfy

$$\begin{aligned}
\overline{r}_1 &\equiv [[\overline{x}_1,\overline{x}_3],\overline{x}_1]\,[[\overline{x}_1,\overline{x}_3],\overline{x}_3]\,[[\overline{x}_2,\overline{x}_3],\overline{x}_1] \mod F_{(4)}\\
\overline{r}_2 &\equiv [[\overline{x}_1,\overline{x}_3],\overline{x}_2] \mod F_{(4)},\\
\overline{r}_3 &\equiv [[\overline{x}_1,\overline{x}_3],\overline{x}_1]\,[[\overline{x}_1,\overline{x}_3],\overline{x}_2]\,[[\overline{x}_2,\overline{x}_3],\overline{x}_1] \mod F_{(4)}.
\end{aligned}$$

We claim that $G_S^T(2)$ is mild. To this end let $U := \langle\chi_1\rangle,\ V = \langle\chi_2,\chi_3\rangle$. By the above calculations the triple Massey product $\langle\cdot,\cdot,\cdot\rangle$ is trivial on $V \times V \times V$ and maps $U \times V \times V$ surjectively onto $H^2(G_S^T(2))$. Hence the mildness of $G_S^T(2)$ follows by (2.3.2). Assuming the Leopoldt conjecture, $G_S^T(2)$ is a fabulous pro-2-group. To the author's knowledge, this yields the first known example of a fabulous pro-p-group with trivial cup-product and also the first example of a fabulous pro-p-group with generator rank ≤ 3. Finally, since $h^1(G) = h^2(G)$, by (1.5.10) (v) we see that $G_S^T(2)$ is not 2-adic analytic.

The existence of fab pro-p-groups is a rather mysterious phenomenon: As we have seen, many finitely presented pro-p-Galois groups can be shown to be fab (or even fabulous) using arithmetic arguments. These methods usually lead to the question whether the associated Galois extensions can contain $\mathbb{Z}_p$-extensions. On the other hand, the fab property is far from being completely understood from a purely group theoretic point of view. In [Lab08], J. Labute has shown that a pro-p-group G is fab if the Lie algebra $L(G)$ associated to the central series of G is "fab". However, to date we don't know a single example of a fabulous pro-p-group with the relations in a minimal presentations completely described. An algebraic characterization of fab pro-p-groups could itself provide new insight into arithmetic questions related to $\mathbb{Z}_p$-extensions.

Notation

$k\langle X\rangle$	free associative algebra on the set X over k
$k\langle\langle X\rangle\rangle$	ring of formal power series in the non-commuting indeterminates X over k
$\mathcal{O}[\![G]\!]$	complete group algebra of the pro-p-group G over $\mathcal{O}$
$L(X)$	free Lie algebra (over a field) on the set X
$L_{res}(X)$	free restricted Lie algebra (over a field of characteristic $p > 0$) on the set X
U_L	universal enveloping algebra $\mathcal{U}_{res}(L)$ of the restricted Lie algebra L
$\mathrm{gr}^\omega(G)$	restricted Lie algebra associated to the p-filtered group (G, ω)
C_n	set of Hall commutators of weight n
$\overline{\mathcal{C}}$	Hall basis for the free restricted Lie algebra $L_{res}(X)$
B_n	set of basic commutators of weight n
$\langle\chi_1, \ldots, \chi_k\rangle$	k-fold Massey product
$G_S(p)$	Galois group of the maximal p-extension unramified outside S
$[l_1, l_2, l_3]$	Rédei symbol
$\mu_2(I)$	Milnor invariant corresponding to the multi-index I

Bibliography

[Ani82] D. Anick, *Non-commutative graded Algebras and their Hilbert Series*, J. of Algebra **78** (1982), 120–140.

[Ani87] _____, *Inert sets and the Lie algebra associated to a group*, J. of Algebra **111** (1987), 154–165.

[BGLV11] M.R. Bush, J. Gärtner, J. Labute, D. Vogel, *Mild 2-relator pro-p-groups*, New York J. Math. **17** (2011), 281–294.

[BL07] M.R. Bush, J. Labute, *Mild pro-p-groups with* 4 *generators*, J. of Algebra **308** (2007), 828–839.

[Bou75] N. Bourbaki, *Lie Groups and Lie Algebras, Part I*, Addison-Wesley, 1975.

[Bru66] A. Brumer, *Pseudocompact algebras, profinite groups and class formations*, J. of Algebra **4** (1966), 442–470.

[CH88] P.E. Conner, J. Hurrelbring, *Class number parity*, Series in Pure Math., vol. 8, World Scientific, Singapore, 1988.

[DdSMS99] J. Dixon, M. du Sautoy, A. Mann, D. Segal, *Analytic Pro-p-groups* second edition, Cambridge Stud. Adv. Math. 61, Cambridge University Press, 1999.

[Dem61] S.P. Demuškin, *On the maximal p-extension of a local field (in Russian)*, Izv. Akad. Nauk. USSR Math. Ser. **25** (1961), 329–346.

[Den95] C. Deninger, *Higher order operations in deligne cohomology*, Invent. Math. **120** (1995), 289–315.

[DL83] D. Dummit, J. Labute, *On a new characterization of Demuškin groups*, Invent. Math. **73** (1983), 413–418.

[Fen83] R.A. Fenn, *Techniques of geometric topology*, London Math. Soc. Lecture Notes 57, Cambridge University Press, 1983.

[FG09] P. Forré, J. Gärtner, *On the existence of $K(\pi, 1)$'s over the rationals*, preprint (2009).

[For10] P. Forré, *Strongly free sequences and pro-p-groups of cohomological dimension 2*, to appear in J. reine u. angew. Mathematik (2010).

[Gil68] D. Gildenhuys, *On pro-p-groups with a single defining relator*, Invent. Math. **5** (1968), 357–366.

[Gä08] J. Gärtner, *Über die maximale p-Erweiterung algebraischer Zahlkörper mit beschränkter Verzweigung und vorgegebener Zerlegung*, Diplomarbeit, Heidelberg, 2008.

[Hab78] K. Haberland, *Galois Cohomology of Algebraic Number Fields*, Deutscher Verlag der Wiss., Berlin, 1978.

[Iwa55] K. Iwasawa, *On Galois groups of local fields*, Trans. Amer. Math. Soc. **80** (1955), 448–469.

[Jac62] N. Jacobson, *Lie algebras*, Interscience, New York, 1962.

[Koc69] H. Koch, *Zum Satz von Golod-Schafarewitsch*, Math. Nachr. **42** (1969), 321–333.

[Koc78] ———, *On p-extensions with given ramification*, Appendix 1 in [Hab78], 1978.

[Koc02] ———, *Galois theory of p-extensions*, Springer, 2002.

[Kra66] D. Kraines, *Massey higher products*, Trans. Amer. Math. Soc. **124** (1966), 431–449.

[Lab67a] J. Labute, *Algèbres de Lie et pro-p-groupes définies par une seule relation*, Invent. Math. **4** (1967), 142–158.

[Lab67b] ———, *Classification of Demuškin groups*, Canad. J. Math. **19** (1967), 106–132.

[Lab77] ———, *The lower central series of the group* $\langle x, y : x^p = 1\rangle$, Proc. Amer. Math. Soc. **66** (1977), 197–201.

[Lab85] ———, *The determination of the Lie algebra associated to the lower central series of a group*, Trans. Amer. Math. Soc. **288, no. 2** (1985), 51–57.

[Lab06] ———, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$, J. reine u. angew. Mathematik **596** (2006), 155–182.

[Lab08] ———, *Fabulous pro-p-groups*, Ann. Sci. Math. Québec **32, no. 2** (2008), 189–197.

[Laz54] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Ec. Norm. Sup. **71** (1954), 101–190.

[Laz65] ———, *Groupes analytiques p-adiques*, Publ. Math. I.H.E.S. **26** (1965), 389–603.

[Lem74] J.-M. Lemaire, *Algèbres connexes et Homologie des Espaces de Lacets*, Lecture Notes in Mathematics 422, Springer, 1974.

[LM11] J. Labute, J. Mináč, *Mild pro-2-groups and 2-extensions of* $\mathbb{Q}$ *with restricted ramification*, J. of Algebra **332** (2011), 136–158.

[Lub83] A. Lubotzky, *Group presentation, p-adic analytic groups and lattices in* $\mathrm{SL}_2(\mathbb{C})$, Ann. Math. **118** (1983), 115–130.

[Lyn50] R.C. Lyndon, *Cohomology theory of groups with a single defining relation*, Ann. Math. **52** (1950), 650–656.

[MAGMA] W. Bosma, J. Cannon, *Handbook of Magma functions*, School of Mathematics and Statistics, University of Sydney, 1996.

[Mai05] C. Maire, *Sur la dimension cohomologique des pro-p-extensions des corps de nombres*, J. Th. des Nombres de Bordeaux **17, no. 2** (2005), 575–606.

[Mas58] W.S. Massey, *Some higher order cohomology operations*, Symposium International de Topologica Algebraica, La Universidad Nacional Autónoma de México and UNESCO, Mexico City (1958), 145–154.

[May69] J.P. May, *Matric massey products*, J. of Algebra **12** (1969), 533–568.

[MKS76] W. Magnus, A. Karrass, D. Solitar, *Combinatorial group theory, 2nd revised edition*, Dover Publications, 1976.

[Mor02] M. Morishita, *On certain analogies between knots and primes*, J. reine u. angew. Mathematik **550** (2002), 141–167.

[Mor04] ———, *Milnor invariants and Massey products for prime numbers*, Compositio Math. **140** (2004), 69–83.

[Neu99] J. Neukirch, *Algebraic number theory*, Springer, 1999.

[NSW08] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields, 2nd edition*, Springer, 2008.

[Réd38] L. Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I.*, J. reine u. angew. Mathematik **180** (1938), 1–43.

[Reu93] C. Reutenauer, *Free Lie algebras*, Clarendon Press, Oxford, 1993.

[RZ10] L. Ribes, P. Zalesskii, *Profinite groups, 2nd edition*, Springer, 2010.

[Sch02] A. Schmidt, *On the relation between* 2 *and* ∞ *in the Galois cohomology of number fields*, Compositio Math. **131** (2002), 1–22.

[Sch06] ———, *Circular sets of prime numbers and p-extensions of the rationals*, J. reine u. angew. Mathematik **596** (2006), 115–130.

[Sch07] ———, *Rings of integers of type* $K(\pi, 1)$, Doc. Math. **12** (2007), 441–471.

[Sch10] ———, *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, J. reine u. angew. Mathematik **640** (2010), 203–235.

[Ser63] J.-P. Serre, *Structure de certains pro-p-groupes (d'après Demushkin)*, Sémin. Bourbaki 1962/1963 **252** (1963).

[Vog04] D. Vogel, *Massey products in the Galois cohomology of number fields*, Ph.D. thesis, Universität Heidelberg, 2004.

[Vog05] ———, *On the Galois group of* 2*-extensions with restricted ramification*, J. reine u. angew. Mathematik **581** (2005), 117–150.

[Vog06] ———, *Circular sets of primes of imaginary quadratic number fields*, Preprints der Forschergruppe Algebraische Zykel und L-Funktionen Regensburg/Freiburg Nr. 5 (2006).

[Vog07] ———, *p-extensions with restricted ramification - the mixed case*, Preprints der Forschergruppe Algebraische Zykel und L-Funktionen Regensburg/Freiburg Nr. 11 (2007).

[Win86] K. Wingberg, *Galois groups of number fields generated by torsion points of elliptic curves*, Nagoya Math. J. **104** (1986), 43–53.

[Win89] ———, *On Galois groups of p-closed number fields with restricted ramification*, J. reine u. angew. Mathematik **400** (1989), 185–202.

[Win07] ———, *Arithmetical Koch groups*, preprint (2007).