3-8-2019 4:00 PM

Enhanced Koszulity in Galois cohomology

Marina Palaisti, *The University of Western Ontario*

Supervisor: Minac, Jan, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Mathematics

Abstract

Despite their central role in Galois theory, absolute Galois groups remain rather mysterious; and one of the main problems of modern Galois theory is to characterize which profinite groups are realizable as absolute Galois groups over a prescribed field. Obtaining detailed knowledge of Galois cohomology is an important step to answering this problem. In our work we study various forms of enhanced Koszulity for quadratic algebras. Each has its own importance, but the common ground is that they all imply Koszulity. Applying this to Galois cohomology, we prove that, in all known cases of finitely generated pro-p-groups, Galois cohomology is a Koszul algebra. In particular, we show that for all known cases where the maximal pro-p-quotient of the absolute Galois group is finitely generated, Galois cohomology is universally Koszul. Assuming the Elementary Type conjecture, this gives us infinitely many refinements of the Bloch-Kato Conjecture. We moreover obtain several unconditional results. Lastly, we show that all forms of enhanced Koszulity are preserved under certain natural operations, which generalizes results that were only known to hold in the commutative case.

Keywords: Galois theory, Koszulity, Strong Koszulity, Koszul filtration, Universal Koszulity, pro-p-group, free group, Demushkin group, rigid fields, Abstract Witt ring, Witt ring, Elementary Type, Bloch-Kato Conjecture, Elementary Type Conjecture

“*[This] science is the work of the human mind, which is destined rather to study than to know, to seek the truth rather than to find it.*”– E. Galois

Co-Authorship Statement

Chapters 5, 6, 7, 8, 9 and 10 of this thesis incorporate material which results from joint research with Professor Ján Mináč, Dr. Federico William Pasini and Dr. Nguyễn Duy Tân, and is based on the paper [MPPT]. Moreover, a compact version of this work is to be presented in [Pal].

Acknowledgments

I would like to express the most sincere and deepest gratitude to my advisor Ján Mináč for his constant support, the endless patience and for all the fantastic mathematics he taught me. Thank you for all the trust you put in me, for the guidance in and out of mathematical context, for all the fascinating moments, the laughter and joy you brought to research, the amazing fun we had together and for making this whole endeavor possible.

I would further like to thank Graham Denham and Masoud Khalkhali for sitting on my thesis committee and providing helpful comments, as well as the mathematical discussions and guidance during all my years at Western.

Along the same lines, I am really indebted to all the examiners, Dr. Keir Lockridge (external examiner), Dr. John Barron (University examiner), Dr. Masoud Khalkhali and Dr. David Riley (department examiners) not only for showing interest to this work and for putting their feedback that upgraded the content and presentation of the current document; but also, for their stimulating remarks and questions that have fired up the potential for new directions.

Moreover, I am really thankful to Adam Chapman, Sunil Chebolu, Danny Neftin, Jasmin Omanovic, Federico Pasini and Nguyễn Duy Tân for all the great math we discussed together, for sharing their thoughts with me and including me into the realization of their mathematical visions.

In addition, I thank David Eisenbud, David Harbater, Stefan Gille, Daniel Krashen, John Labute, Alexander Merkurjev, Kirsten Wickelgren and so many more for all the fruitful conversations and for their contributions to the whole way I understand mathematics.

Other friends and colleagues that formed my support system through this experience are: Jasmin Omanovic, Marine Rougnant, Patrick McFaddin, Ernest Guico, Vaidehee Thatte, Marco Vergura and Chandra Rajamani.

I am mostly indebted to my humble partner in life, Jasmin Omanovic, for everything; all the breaths we take together, the unconditional love and support, for brightening my darkest days and - since it is relevant - for the mathematical conversations.

Finally, I thank my Canadian foster parents for caring for me, and my family for believing in me and for the moral support. Special thanks to my parents for everything they have done for me: *ευχαριστώ από τα βάθη της καρδιάς μου*.

Introduction

Let $\mathbb{F}$ be a field and denote by $\mathbb{F}_s$ a separable closure of $\mathbb{F}$. The Galois group $G_{\mathbb{F}} := \mathrm{Gal}(\mathbb{F}_s/\mathbb{F})$ is called the *absolute Galois group of* $\mathbb{F}$ and it encodes all the structural information of the field $\mathbb{F}$ itself. Despite their central role in Galois theory, absolute Galois groups remain rather mysterious; and one of the main problems of modern Galois theory is to characterize which profinite groups are realizable as absolute Galois groups over a prescribed field.

The mathematical community is far from conceiving the possible structures of absolute Galois groups. Instead, historically, the most conventional way to approach this question has been through the use of *Galois cohomology*, a cohomology theory based on continuous cochains and coboundaries.

Chapters 1 and 2 contain all necessary background in Galois cohomology. Chapter 1 starts with profinite and pro-p-groups, we then introduce Galois cohomology and give a very brief presentation of the algebraic theory of quadratic forms. Chapter 2 concerns notions around cohomological dimension, an invariant that provides structural information of profinite and pro-p-groups. We close the background in Galois cohomology by presenting the work of Demushkin, J.-P. Serre and J. Labute in the structure of pro-p-groups of cohomological dimension at most two that satisfy Poincaré duality.

After the work of numerous mathematicians, the biggest achievement toward understanding Galois cohomology is the proof of the Bloch-Kato Conjecture by M. Rost and V. Voevodsky, with the contribution of various important mathematicians. These results, although of utmost depth and importance, do not directly give information on the structure of absolute Galois groups, which was the initiative of the Conjecture in the first place. However, the Voevodsky-Rost Theorem implies that if a primitive p-th root of unity $\zeta_p \in \mathbb{F}$, then $H^\bullet(G_{\mathbb{F}}, \mathbb{F}_p)$ is a *quadratic* algebra, i.e. a graded algebra all of whose generators live in degree 1 subject to homogeneous quadratic relations.

Among quadratic algebras, the significant class of *Koszul* algebras was singled out by S. Priddy in [Pri70]. These are $\mathbb{N}$-graded $\Bbbk$-algebras whose ground field $\Bbbk$, viewed as a trivial module, admits a *linear* resolution, meaning a graded free resolution $(P_\bullet, d_\bullet)$, in which each P_n is generated in degree n. Koszul algebras are characterized by uncommonly nice cohomological behavior, in the following sense: generally, it is a really hard task to describe the cohomology of an arbitrary graded algebra. But the cohomology of a Koszul $\Bbbk$-algebra $A_\bullet$ is nothing but its *quadratic dual* $A^!_\bullet$, defined as the quadratic $\Bbbk$-algebra generated by the dual space of generators of $A_\bullet$ and whose relators form the orthogonal complement of the relator space of $A_\bullet$.

Chapters 3 and 4 are dedicated to Koszulity. In Chapter 3, we introduce the notion of a quadratic algebra and its quadratic dual, and provide various basic examples of such algebras. We then build the theory around Koszul algebras and their associated complexes, called Koszul complexes. A Koszul complex is a linear free complex, so it makes a good candidate to test Koszulity: if it is exact, then it is a linear resolution of the ground field and the associated algebra is Koszul. Otherwise, the algebra is not Koszul. However, the quest of understanding whether a Koszul complex is a resolution was proven to be a rather hard task. Thus in Chapter 4, we discuss other methods that determine whether an algebra is Koszul or not. Notably, one way is to use Hilbert and Poincaré series; a method which is only helpful if one wishes to show that a quadratic algebra is not Koszul. A different approach is by trying to find the analog of a Gröbner basis of a quadratic algebra. Algebras that posses such a basis are called PBW algebras and they are Koszul. The PBW property, although promising, requires that one finds a PBW basis of generators in any degree, which makes the process quite messy. However, G.M. Bergman found a convenient way to check whether an algebra is PBW, without having to test generators in every single degree. This fantastic machinery is presented in Section 4.3.

Koszul algebras arise in various mathematical disciplines, such as representation theory, noncommutative algebra, quantum groups, noncommutative geometry, algebraic geometry and topology (cf. for instance [BGS96] and [LV12]). In the context of Galois cohomology, Koszul algebras have been studied by L. Positselski and A. Vishik (cf. [PV95]). These investigations were extended even further by Positselski (see cf. [Pos05] and [Pos14]). In particular, he explicitly formulated a conjecture, a special case of which is the following

Conjecture(Positselski). If $\mathbb{F}$ is a field containing a primitive p-th root of unity, then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is Koszul.

In [PV95], it was shown that the validity of the preceding conjecture, together with the bijectivity of the norm residue homomorphism in degree 2 and its injectivity in degree 3 imply an easier and more natural proof to the Bloch-Kato Conjecture. In this sense, Positselski's Conjecture can be understood as a strengthening of the Bloch-Kato Conjecture.

Inspired by Positselski's Conjecture, we attempted to understand the higher relations even further. To this extent, we introduced forms of enhanced Koszulity. These include the properties of strong Koszulity, universal Koszulity and Koszul filtration. Each of these notions is important in their own right; but the common grounds is that they all follow the same idea of "divide and conquer" and they all imply Koszulity. Chapter 5 is the first chapter that does not purely contain background material. We recall the formulation of the Bloch-Kato and the Milnor Conjectures. Then, we proceed to introducing the various forms of enhanced Koszulity, namely strong Koszulity, universal Koszulity and Koszul filtrations. Section 5.3 is an exposition on the family of elementary type pro-p-groups.

Chapter 6 is devoted to showing that the Galois cohomology of the family of Elementary Type pro-p-groups is strongly Koszul. We build this step by step. In section 6.1 we show the statement for free groups, we then proceed to show that the cohomology of Demushkin groups is strongly Koszul in section 6.2. Having established these, we show that the direct sum of two strongly Koszul algebras is strongly Koszul; and that the twisted extension of a strongly Koszul algebra with an exterior algebra generated by finitely many elements is strongly Koszul. Combining Propositions 6.1.1, 6.2.1, 6.2.3, 6.2.5, 6.3.1 and 6.4.1, we obtain

Theorem. *If G is an elementary type pro-p-group, such that there does not exists $1 \neq a \in G$, with the property $a^2 = 1$, then $H^\bullet(G, \mathbb{F}_p)$ is strongly Koszul.*

Let $\mathbb{F}(p)/\mathbb{F}$ denote a fixed maximal p-extension of $\mathbb{F}$ inside $\mathbb{F}_s/\mathbb{F}$ and denote by $G_{\mathbb{F}}(p) = \mathrm{Gal}(\mathbb{F}(p)/\mathbb{F})$ the maximal pro-p-quotient of $G_{\mathbb{F}}$. Applying the preceding result to $G_{\mathbb{F}}(p)$, we obtain

Corollary. Let $\mathbb{F}$ be a field and assume that a primitive p-th root of unity $\zeta_p \in \mathbb{F}$, or for $p = 2$, that $\sqrt{-1} \in \mathbb{F}$. If $G_{\mathbb{F}}(p)$ is an elementary type pro-p-group, then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is strongly Koszul.

On the other hand, the question of whether Galois cohomology is universally Koszul arises more naturally. To this extent, we show in Chapter 7 that the Galois cohomology of elementary type pro-p-groups is universally Koszul. The series of steps mimics the ones that appeared in Chapter 6, with the main result being

Theorem. *If G is an elementary type pro-p-group, then $H^\bullet(G, \mathbb{F}_p)$ is universally Koszul.*

In terms of Positseslski's Conjecture, this gives us

Corollary. If $\mathbb{F}$ is a field such that $\zeta_p \in \mathbb{F}$ and $G_{\mathbb{F}}(p)$ is an elementary type pro-p-group, then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is universally Koszul.

Chapter 8 is devoted to the illustration of why universal Koszulity fits better into the context of Galois cohomology than strong Koszulity. In fact, by removing assumption $\sqrt{-1} \in \mathbb{F}$, for $p = 2$, we find counterexamples to strong Koszulity. These include the families of rigid fields of levels zero and two that contain at least eight distinct generators. Notably, Propositions 8.2.3 and 8.3.3 give

Proposition. Let $\mathbb{F}$ be a 2-rigid field of level $s(\mathbb{F}) = 0$ or 2, such that $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} \geq 3$. Then $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is not strongly Koszul, but it is universally Koszul.

In Chapter 9, we get inspiration from the Elementary Type conjecture for abstract Witt rings. First, we recall the isomorphism between graded Witt rings and Galois cohomology via the proof of the Milnor conjecture. We then proceed to building the theory of abstract Witt rings and present the Elementary Type Conjectures. Combining our work in universal Koszulity with the results known in the aforementioned conjectures, we obtain the following statement, arising as a combination of Propositions 9.4.1, 9.4.7 and 9.4.2.

Theorem. *Assume $\mathbb{F}$ is of characteristic $\operatorname{char} \mathbb{F} \neq 2$. If one of the conditions*

(i) $\#\mathbb{F}^\times/\mathbb{F}^{\times 2} \leq 32$*;*

(ii) $\mathbb{F}$ *supports at most four quaternion algebras;*

(iii) $\mathbb{F}$ *is a pythagorean formally real field;*

holds, then $H^\bullet(\mathbb{F}, \mathbb{F}_2)$ *is universally Koszul.*

Lastly, Chapter 10 is more self-contained than any other part of this work. It is devoted to showing that the direct sum and the twisted extension of algebras that posses Koszul filtration has a Koszul filtration as well. This could arise as a Corollary of Propositions 7.3.1 and 7.4.1, since the collection of all ideals generated in degree one of a universally Koszul algebra, is a Koszul filtration. However, outside of the context of Galois cohomology, very few algebras are known to be universally Koszul. This fully justifies the existence of this chapter.

We conclude this writing by posing some new questions and potential directions that were birthed during the creation of the work presented here.

Contents

Chapter 1

Galois cohomology

One of the most fundamental and long standing problems is to characterize the profinite groups which are realizable as absolute Galois groups over a given field. The first attempt to tackle it came from E. Artin and O. Schreier in 1927, when they created a theory for Galois groups over real fields, and showed that the only nontrivial subgroups of absolute Galois groups are cyclic groups of order 2. However, despite the evolution in techniques and machinery, very little progress has been made toward classifying such groups.

Almost half a century later, in 1974, E. Becker redeveloped the Artin-Schreier theory over more general fields and demonstrated that the most vital part in understanding absolute Galois groups is to understand the structure of their maximal pro-p-quotients. This observation has since put the study of maximal pro-p-quotients and, more generally, pro-p-groups under the spotlight.

One of the most important tools used to describe profinite groups is Galois cohomology, which is a cohomology theory based on continuous cochains and coboundaries. Computing the Galois cohomology groups associated to a given profinite group provides information on their structure, their generators, relations and the relation between relations. It has therefore been established as the most mainstream way to the study of Galois and profinite groups.

Fantastic references that cover topics related to profinite groups and Galois cohomology in great detail are [Ser64], [NSW08] and [Sha72]. In addition, a thorough treatment of the algebraic theory of quadratic forms can be found in [Lam05].

1.1 Profinite and pro-p-groups

Let G be a topological Hausdorff group. If G is formed as the projective limit of finite groups, each of them endowed with the discrete topology, then it is called a *profinite group.* Since a profinite group is formed as a projective limit of finite groups equipped with the discrete topology, the only connected components of G are singletons, and thus a profinite group is totally disconnected; and by the universal property of projective limits, G is compact. On the other hand, if G is a compact and totally disconnected Hausdorff group, the only connected components are singletons. And assuming that G is compact, yields that G is locally compact, and thus the set of open subgroups of it forms a basis of neighborhoods of 1_G. By compactness, moreover, we deduce that if U is an open subgroup of G, then the index $(G : U)$ is finite. Thus, for each $g \in G$, there is a finite number of conjugates gUg^{-1} and further, the intersection $N = (gUg^{-1}) \cap (gU'g^{-1})$ of any two such conjugates is an open normal subgroup of G. These intersections are the subgroups that form a basis of 1_G. We therefore obtain a map

$$G \longrightarrow \varprojlim G/N,$$

which is injective, since all such N's form a basis of neighborhoods of 1_G, continuous, and dense. Now, by the universal property of projective limits, projective limits are unique up to unique isomorphism. Therefore, the map $G \longrightarrow \varprojlim G/N$ is an isomorphism, whence G is a profinite group. We thus have shown that G is a profinite group if and only if it is a compact totally disconnected topological group. We therefore obtain the following

Theorem 1.1.1. *For a compact Hausdorff group G the following are equivalent.*

(i) G is a profinite group;

(ii) G is totally disconnected;

(iii) there exists a set of open normal subgroups of G that forms a neighborhood basis of 1_G.

Note that direct products of profinite groups are profinite and also projective limits of profinite groups are profinite as well. Moreover, we can use a neighborhood basis of the unit of a profinite group G to construct neighborhood basis of the units of its subgroups and quotients. Namely, let G be a profinite group with neighborhood basis $\{N : N \trianglelefteq G \text{ open}, \ (G : N) < \infty\}$ of 1_G, and H is a subgroup of G, then a neighborhood basis of 1_H is $\{H \cap N : N \trianglelefteq G \text{ open}, \ (G : N) < \infty\}$. If $H \trianglelefteq G$ is normal, then the quotient group G/H has a neighborhood basis $\{NH/H : N \trianglelefteq G \text{ open}, (G : N) < \infty\}$.

Examples.

1. Let G be a compact topological group and let I be a set of normal subgroups of $N \trianglelefteq G$ in G of finite index $(G : N)$ and assume that I is closed under intersection. We put a partial order on I by setting $N_i \leq N_j$ if and only if $N_i \supseteq N_j$, for $N_i, N_j \in I$. For $N_i \leq N_j$, we consider the natural projection
$$\mathrm{pr}_i^j : G/N_j \twoheadrightarrow G/N_i.$$
The natural map
$$g \mapsto \prod_{N_i \in I} gN_i$$
induces a morphism
$$\mathrm{pr}_I : G \longrightarrow \varprojlim_{N_i \in I} G/N_i,$$
whose kernel is the intersection $\cap_{N_i \in I} N_i$.

2. In the same setting as the preceding example, if I consists of all normal subgroups of finite index, that is, if the intersection of all normal subgroups of finite index is a normal subgroup of finite index in G, then the projective limit $\varprojlim G/N_i$ is called *the profinite completion of* G and is denoted by $\hat{G}$.

3. Consider the set of integers $\mathbb{Z}$ endowed with the natural order. The profinite completion of $\mathbb{Z}$ is the *Prüfer ring*
$$\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p.$$

4. Let $\mathbb{F}$ be a field and denote by $\mathbb{F}_s$ a fixed separable closure of $\mathbb{F}$. The *absolute Galois group of* $\mathbb{F}$ is then defined as the Galois group $G_{\mathbb{F}} := \mathrm{Gal}(\mathbb{F}_s/\mathbb{F})$ and is a profinite group, as we shall see in the next section.

Theorem 1.1.2 (Cross section Theorem)**.** *Let H be a closed normal subgroup of the profinite group G. Then there exists a continuous section*

$$\sigma : G/H \longrightarrow G,$$

such that $\sigma(H) = 1$. In other words, the composite map

$$\begin{tikzcd} G/H \arrow[r, "\sigma"] \arrow[rr, bend right, "\mathrm{id}_{G/H}"'] & G \arrow[r, two heads] & G/H \end{tikzcd}$$

is the identity of G/H.

Let p be a prime number. A *pro-p-group* is a profinite group in which every open normal subgroup has a p-power index. Equivalently, a pro-p-group is a topological group that can be realized as a projective limit of finite p-groups.

Examples.

1. Let G be a topological group. Let I be the set consisting of all normal subgroups $N \trianglelefteq G$, whose index $(G : N)$ in G is a p-power. Then the projective limit $\varprojlim G/N_i$ is called *the pro-p completion of* G and is denoted by $\hat{G}_p$.

2. Consider the ring of integers $\mathbb{Z}$ endowed with the natural order. The pro-p-completion of $\mathbb{Z}$ is $\mathbb{Z}_p$.

3. The group of p-adic integers $\mathbb{Z}_p$ can be realized as

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n = \{\{a_n\}_{n\in\mathbb{N}} : a_j \equiv a_i \bmod p^i, \text{ for } i \leq j\}.$$

4. Let $\mathbb{F}$ be a field and denote by $\mathbb{F}_s$ a fixed separable closure of $\mathbb{F}$. Let $\mathbb{F}(p)$ denote the *maximal p-extension* of $\mathbb{F}$, that is, the field compositum of all finite p-extensions of $\mathbb{F}$ inside $\mathbb{F}_s/\mathbb{F}$. The Galois group $G_{\mathbb{F}}(p) := \mathrm{Gal}\,(\mathbb{F}(p)/\mathbb{F})$ is the maximal pro-p-quotient of the absolute Galois group $G_{\mathbb{F}}$. It is realizable as the inverse limit of all finite p-quotients of $G_{\mathbb{F}}$, and is thus a pro-p-group.

Assuming that G is a profinite group, a subgroup $H \leq G$ is called a *Sylow p-subgroup* of G if H is a pro-p-group and the index $(G : H)$ is prime to p. If G is a pro-p-group, then any subgroup of G of finite index is a Sylow p-subgroup. Similarly to the finite case, we have the Sylow Theorem for profinite groups.

Theorem 1.1.3 (Sylow Theorem). *(i) Every profinite group contains Sylow p-subgroups.*

(ii) Every pro-p-subgroup is contained in a Sylow p-subgroup of a profinite group. Further, if G and G' are profinite groups and $G \longrightarrow G'$ is a surjective homomorphism, then the image of a Sylow p-subgroup of G is a Sylow p-subgroup of G'.

(iii) Any two Sylow p-subgroups of a profinite group are conjugate.

Examples.

1. The Prüfer ring $\hat{Z}$ has the group $\mathbb{Z}_p$ as a Sylow p-subgroup.

2. Let G be a compact p-adic analytic group. Then all its Sylow p-subgroups are open, and thus, they form a neighborhood basis for 1_G. This means that the order of G is a p-power multiplied by a natural number.

3. Let G be a discrete group and denote by $G^{\mathrm{ab}} = G/[G,G]$ its abelianization. If G^{ab} is isomorphic to $\mathbb{Z}$, then its pro-p-completion is isomorphic to the pro-p-completion of $\mathbb{Z}$, which is nothing else but $\mathbb{Z}_p$.

Let G be a pro-p-group. We say that X is a *system of topological generators of G* if G is the smallest group that contains X and every neighborhood of 1_G contains almost all elements of X. A system X of topological generators of G is *minimal* if there is no proper subset $Y \subset X$ that is a system of topological generators for G. We denote the cardinality of generators of G by $d(G)$ and we call it the *rank* of G. The rank $d(G)$ of a group G is well defined, in the sense that any two minimal sets of topological generators of G have the same cardinality. We say that G is *finitely generated* if $d(G)$ is finite.

Definition 1.1.4. Let G be a profinite group. The *Frattini subgroup* of G is defined as

$$\Phi(G) := \cap\{M : M \leq G \text{ maximal and open }\}.$$

The Frattini subgroup becomes particularly useful when trying to understand pro-p-groups, due to the fact that it is a maximal subgroup on its own. We further have the Burnside Basis Theorem:

Theorem 1.1.5 (Burnside Basis Theorem). *Let G be a pro-p-group. Let $X = \{x_i : i \in I\}$ be a subset of G, such that every neighborhood of 1_G contains almost all elements of X. Then X is a system of generators of G if and only if $\{x_i\Phi(G) : i \in I\}$ is a system of generators of $G/\Phi(G)$.*

Other extremely remarkable properties of pro-p-groups include the following.

Proposition 1.1.6. *A pro-p-group G is finitely generated if and only if $\Phi(G)$ is open in G.*

Theorem 1.1.7 (Serre). *Every subgroup of finite index of a finitely generated pro-p-group is open.*

Corollary 1.1.8. *If G is a finitely generated pro-p-group, then*

$$\Phi(G) = G^p[G, G].$$

1.2 Galois groups

Among the class of profinite groups, we are interested in a particular family, namely the profinite Galois groups. In the classical (finite) setting, given a field $\mathbb{F}$ and a finite, normal extension $L/\mathbb{F}$, the Galois group $\mathrm{Gal}(L/\mathbb{F})$ is defined as the group of automorphisms of L that fix the elements of the ground field $\mathbb{F}$. Infinite Galois theory mimics the classical setting, extending the horizons to (possibly) infinite Galois extensions.

Let $L/\mathbb{F}$ be a normal extension, not necessarily finite. We define the *Galois group of L over $\mathbb{F}$* as the group

$$\mathrm{Gal}(L/\mathbb{F}) = \{\sigma \in \operatorname{Aut} L : \sigma(f) = f, \text{ for all } f \in \mathbb{F}\},$$

exactly like in the finite setting. We put a topology on $\mathrm{Gal}(L/\mathbb{F})$ by setting a basis of neighborhoods of $1_{\mathrm{Gal}(L/\mathbb{F})}$ to be the set

$$\{\mathrm{Gal}(L/K) : \mathbb{F} \leq K \leq L \text{ and } K/\mathbb{F} \text{ is normal and finite }\}.$$

The Galois group $\mathrm{Gal}(L/\mathbb{F})$ is a profinite group, and in fact,

$$\mathrm{Gal}(L/\mathbb{F}) = \varprojlim_{K/\mathbb{F} \text{ normal and finite}} \mathrm{Gal}(L/K).$$

On the other hand, let $\{K_i/\mathbb{F} : i \in I\}$ be a family of finite normal extensions of $\mathbb{F}$ and set

$$L = \cup_{i \in I} K_i.$$

Assume that for all $i, j \in I$ there exists an index $k \in I$, such that $K_i, K_j \subseteq K_k$. Then the family $\{\mathrm{Gal}(K_i/\mathbb{F}) : i \in I\}$ forms a projective system with projective limit

$$\varprojlim_{i \in I} \mathrm{Gal}(K_i/\mathbb{F}) \cong \mathrm{Gal}(L/\mathbb{F}).$$

Example.

Consider the ground field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root of unity and let $L = \cup_{i=1}^{\infty} \mathbb{Q}(\zeta_{p^i})$. If p is an odd prime, then

$$\mathrm{Gal}(L/\mathbb{Q}(\zeta_p)) = \varprojlim_{i} \mathrm{Gal}(\mathbb{Q}(\zeta_{p^i})/\mathbb{Q}(\zeta_p)) \cong \mathbb{Z}_p.$$

Assume now that $p = 2$. Then

$$\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \times \varprojlim_{i \geq 3} \mathrm{Gal}(\mathbb{Q}(\zeta_{2^i})/\mathbb{Q}(\zeta_4)) = \mathbb{Z}/2 \times \mathbb{Z}_2.$$

As in the finite setting, isomorphisms between subfields of an infinite Galois extension give a lift to automorphisms of Galois groups. We moreover have the Lagrange Theorem

$$(\mathrm{Gal}(L/\mathbb{F}) : \mathrm{Gal}(L/K)) = (K : F).$$

Further, recall that $L/\mathbb{F}$ is normal and let $K/\mathbb{F}$ be a subextension of $L/\mathbb{F}$. Then $\mathrm{Gal}(L/K)$ inherits the topology of $\mathrm{Gal}(L/\mathbb{F})$ and it is a closed subgroup of $\mathrm{Gal}(L/\mathbb{F})$. The subgroup $\mathrm{Gal}(L/K) \leq \mathrm{Gal}(L/\mathbb{F})$ is open if and only if the extension $K/\mathbb{F}$ is finite.

We finally present the Fundamental Theorem of Galois theory.

Theorem 1.2.1 (Fundamental Theorem of Galois Theory)**.** *Let $L/\mathbb{F}$ be a normal extension. Then the set of all intermediate fields $\mathbb{F} \leq K \leq L$ of $L/\mathbb{F}$ is in one-to-one correspondence with the set of all (closed) subgroups $\mathrm{Gal}(L/K)$ of $\mathrm{Gal}(L/\mathbb{F})$. The correspondence is given as follows:*

$$K/\mathbb{F} \mapsto \mathrm{Gal}(L/K); \text{ and } \mathrm{Gal}(L/K) \mapsto L^K,$$

where L^K denotes the fixed field by elements of K.

Two more main properties of infinite Galois theory mimic the results of the classical one. Namely, if $L/\mathbb{F}$ is a normal extension with subextension $K/\mathbb{F}$, then we have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbb{F}) \longrightarrow \mathrm{Gal}(K/\mathbb{F}) \longrightarrow 1.$$

And finally, assume that $L/\mathbb{F}$ is a normal extension and consider the subextensions $K_1/\mathbb{F}$ and $K_2/\mathbb{F}$. If $K_1/\mathbb{F}$ is normal, so is the extension K_1K_2/K_2, and we have a natural isomorphism

$$\mathrm{Gal}(K_1K_2/\mathbb{F}) \cong \mathrm{Gal}(K_1/K_1 \cap K_2).$$

If, in addition, $K_2/\mathbb{F}$ is normal, then

$$\mathrm{Gal}(K_1K_2/\mathbb{F}) \cong \mathrm{Gal}(K_1/\mathbb{F}) \times_{\mathrm{Gal}(K_1 \cap K_2/\mathbb{F})} \mathrm{Gal}(K_2/\mathbb{F}).$$

Example.
Let $\mathbb{F} = \mathbb{F}_p$ and consider an algebraic closure $\bar{\mathbb{F}_p}$ of $\mathbb{F}_p$. Then

$$\mathrm{Gal}(\bar{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim_p \mathbb{Z}_p = \prod_p \mathbb{Z}_p.$$

1.3 Galois cohomology

Galois cohomology is a cohomology theory based on continuous cochains and coboundaries, and, as the name suggest, it is the cohomology theory used in profinite and Galois groups.

A G-module A of a profinite group G is *discrete*, if the map

$$G \times A \longrightarrow A$$

$$(g, a) \mapsto {}^g a,$$

given by the action of G on A, is continuous with respect to the discrete topology on A.

Let G be a profinite group and A a discrete G-module. For each $n \geq 0$ we construct the abelian group

$$\mathscr{C}^n(G, A) = \{f : G^{n+1} \longrightarrow A : f \text{ continuous}\},$$

and call it the group of *n-cochains* of G with coefficients in A. For each $f \in \mathscr{C}^n(G,A)$, we define a differential

$$\partial^{n+1} : \mathscr{C}^n(G,A) \longrightarrow \mathscr{C}^{n+1}(G,A)$$

$$f(x_1,\dots,x_{n+1}) \mapsto \partial^{n+1} f(x_1,\dots,x_{n+2}) =$$

$$x_1 f(x_2,\dots,x_{n+2}) + \sum_{i=1}^{n+1}(-1)^i f(x_1,\dots,x_i x_{i+1},\dots,x_{n+2}) + (-1)^{n+2} f(x_1,\dots,x_{n+1}).$$

The system $(\mathscr{C}^\bullet(G,A), \partial^\bullet)_{n\geq 0}$ forms a complex

$$\mathscr{C}^0(G,A) \overset{\partial^1}{\to} \mathscr{C}^1(G,A) \overset{\partial^2}{\to} \mathscr{C}^2(G,A) \overset{\partial^3}{\to} \cdots ,$$

called the *cochain complex* of G with coefficients in A, and is not exact in general.

Now, we set

$$\mathscr{Z}^n(G,A) = \ker\left(\mathscr{C}^n(G,A) \overset{\partial^{n+1}}{\to} \mathscr{C}^{n+1}(G,A)\right)$$

and call it the *n-cocycles* and

$$\mathscr{B}^n(G,A) = \operatorname{im}\left(\mathscr{C}^{n-1}(G,A) \overset{\partial^n}{\to} \mathscr{C}^n(G,A)\right),$$

under the convention that $\mathscr{B}^0(G,A) = 0$ and call it the *n-coboundaries.* It is easy to see that $\mathscr{B}^n(G,A) \subseteq \mathscr{Z}^n(G,A)$, since $\mathscr{C}^\bullet(G,A)$ is a complex.

The *n-cohomology group* of G with coefficients in A is then defined as the factor group

$$H^n(G,A) = \mathscr{Z}^n(G,A)/\mathscr{B}^n(G,A)$$

and it measures the obstruction to the exactness of the cochain complex at the n-th term.

The cohomology groups in low dimensions are well understood. Namely,

$$H^0(G,A) = A^G,$$

where $-^G$ denotes the fixed module functor.

$$\mathscr{Z}^1(G,A) = \{f : G \longrightarrow A : f(xy) = f(x) + xf(y),\ \textit{for all } x,y \in G\},$$

is typically called *crossed homomorphisms.* For $H^2(G,A)$ the description requires a bit unraveling. We have that

$$\mathscr{Z}^2(G,A) = \{f : G^2 \longrightarrow A : f(xy,z) + f(x,y) = f(x,yz) + xf(y,z)\}$$

and

$$\mathscr{B}^2(G, A) = \{f : G^2 \longrightarrow A : f(x, y) = g(x) - g(xy) + xg(y)\},$$

for some 1-cochain $g : G \longrightarrow A$. The second cohomology group $H^2(G, A)$ is defined as the quotient of the former by the latter. It is a famous theorem of Schreier that the elements of $H^2(G, A)$ classify the group extensions of G by A.

To examine the functoriality of these groups, consider a short exact sequence of G-modules

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0.$$

Passing to the associated cochain complexes, we obtain the exact and commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathscr{C}^n(G, A) \arrow[r] \arrow[d, "\partial_A^{n+1}"] & \mathscr{C}^n(G, B) \arrow[r] \arrow[d, "\partial_B^{n+1}"] & \mathscr{C}^n(G, C) \arrow[r] \arrow[d, "\partial_C^{n+1}"] & 0\ , \\
0 \arrow[r] & \mathscr{C}^{n+1}(G, A) \arrow[r] & \mathscr{C}^{n+1}(G, B) \arrow[r] & \mathscr{C}^{n+1}(G, C) \arrow[r] & 0
\end{tikzcd}$$

which for each $n \geq 0$ gives rise to a homomorphism

$$\delta : \ker(\partial_C^n) \longrightarrow \operatorname{coker}(\partial_A^{n+1}).$$

Theorem 1.3.1 (Long exact sequence in cohomology)**.** *For every short exact sequence of G-modules*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

the homomorphism

$$\delta : H^n(G, C) \longrightarrow H^{n+1}(G, A).$$

gives rise to a long exact sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G, A) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^n(G, A) \longrightarrow H^n(G, B) \longrightarrow H^n(G, C) \xrightarrow{\delta} H^{n+1}(G, A) \longrightarrow \cdots .$$

An equivalent formulation to the preceding Theorem states that for each $n \geq 0$, $H^n(G, -)$ is an exact δ-functor between abelian categories.

Since the cohomology groups measure obstruction of exactness of the cochain complex, it is important to understand when they become trivial. A G-module A is *cohomologically trivial*, if for every subgroup H of G and for every $n \geq 1$, we have that $H^n(H, A) = 0$. Among the class of cohomologically trivial G-modules, there is a family that is of utmost interest, namely, induced modules. For a profinite group G and a discrete G-module A, we define the *induced G-module* $\mathrm{Ind}_G(A)$ as the group of all continuous functions $f : G \longrightarrow A$, where A is endowed with the discrete topology. The group $\mathrm{Ind}_G(A)$ is made into a G-module via the action

$$(\sigma f)(\tau) = \sigma f(\sigma^{-1}\tau),$$

for $\sigma, \tau \in G$, $f \in \mathrm{Ind}^G(A)$. Viewed as the functor $\mathrm{Ind}_G(-) : A \mapsto \mathrm{Ind}_G(A)$, $\mathrm{Ind}_G(-)$ is exact.

The remainder of this section is devoted to the description of some fundamental maps between Galois cohomology groups. First, for G-modules A and B, we form the tensor product $A \otimes_{\mathbb{Z}} B$. We make $A \otimes_{\mathbb{Z}} B$ into a G-module via the action

$$\sigma(a \otimes b) = \sigma a \otimes \sigma b.$$

For each $n, m \geq 0$, there is a pairing

$$\mathscr{C}^n(G, A) \times \mathscr{C}^m(G, B) \xrightarrow{\cup} \mathscr{C}^{n+m}(G, A \otimes_{\mathbb{Z}} B),$$

defined by

$$(a \cup b)(\sigma_0, \ldots, \sigma_{n+m}) = a(\sigma_0, \ldots, \sigma_n) \otimes b(\sigma_n, \ldots, \sigma_{n+m}),$$

for $a(\sigma_0, \ldots, \sigma_n) \in \mathscr{C}^n(G, A)$ and $b(\sigma_n, \ldots, \sigma_{n+m}) \in \mathscr{C}^m(G, B)$. This is a bilinear pairing and is compatible with the differentials ∂ of the cochain complex in the sense that

$$\partial(a \cup b) = (\partial a) \cup b + (-1)^n a \cup \partial b.$$

It therefore induces a pairing on the level of cohomology

$$H^n(G, A) \times H^m(G, B) \xrightarrow{\cup} H^{n+m}(G, A \otimes_{\mathbb{Z}} B)$$

$$(\alpha, \beta) \mapsto \alpha \cup \beta$$

for $\alpha \in H^n(G, A)$ and $\beta \in H^m(G, B)$, called the *cup product.* The cup product is associative, graded-commutative and compatible with the functoriality of cohomology.

We lastly investigate how cohomology groups are modified by changing the group G. Let H be a closed subgroup of G and consider the inclusion map

$$\mathrm{incl} : H \hookrightarrow G,$$

which induces a homomorphism on the level of cohomology

$$\mathrm{res}_H^G : H^n(G, A) \longrightarrow H^n(H, A)$$

called the *restriction* homomorphism. If $\alpha \in H^n(G, A)$ has a representative $a(\sigma_0, \ldots, \sigma_n) \in \mathscr{C}^n(G, A)$, then the restriction on the level of cochains restricts a to $a_{|H}$ and then maps it to the cohomology class $\alpha_H \in H^n(H, A)$.

Next, if H is a closed normal subgroup of G then the projection $G \twoheadrightarrow G/H$ induces a homomorphism

$$\inf_G^{G/H} : H^n(G/H, A^H) \longrightarrow H^n(G, A)$$

called the *inflation.* If $\alpha(\overline{\sigma_0}, \ldots, \overline{\sigma_n}) \in H^n(G/H, A)$, then the inflation maps $\alpha(\overline{\sigma_0}, \ldots, \overline{\sigma_n})$ to itself, viewed as a cohomology class from G.

The last homomorphism is in a sense opposite to restriction and is defined only in the case that H is an open subgroup of G. It is called the *corestriction* and is given by

$$\mathrm{cores}_G^H : H^n(H, A) \longrightarrow H^n(G, A).$$

The corestriction homomorphism is a rather mysterious one, however, the way one should think about it is as a higher equivalent of the *norm*

$$\mathfrak{N}_{G/H} : A^H \longrightarrow A^G$$

$$a \mapsto \mathfrak{N}_{G/H}\, a = \sum_{\sigma \in G/H} \sigma a.$$

To see this, notice that on the level of cochains, for each coset $c = H\sigma \in H\backslash G$, we fix a representative $\overline{c}$. Then the corestriction is defined as

$$\mathrm{cores}_G^H : \mathscr{C}^n(H, A) \longrightarrow \mathscr{C}^n(G, A)$$

$$a(\sigma_0, \ldots, \sigma_n) \mapsto \mathrm{cores}\, a(\sigma_0, \ldots, \sigma_n) = \sum_{c \in H\backslash G} \overline{c}^{-1} a(\overline{c}\sigma_0 \overline{c\sigma_0}^{-1}, \ldots, \overline{c}\sigma_n \overline{c\sigma_n}^{-1}).$$

Note that all three maps are functorial with respect to the group they are defined in and transitive; they moreover commute with the connecting homomorphism and with the cup product and satisfy the *projection formula*

$$\operatorname{cores}(\alpha \cup \operatorname{res} \beta) = (\operatorname{cores} \alpha) \cup \beta,$$

where $\alpha \in H^n(H, A)$, $\beta \in H^n(G, B)$ for an open subgroup H of G. Finally, If H is in addition normal, then

$$\operatorname{cores}_G^H \operatorname{res}_H^G = (G : H)$$

and

$$\operatorname{res}_H^G \operatorname{cores}_G^H = \mathfrak{N}_{G/H} .$$

Let H be a closed subgroup of G and let A be an H-module. Similarly to induced modules, we define the group $\operatorname{Ind}_G^H(A)$ as

$$\operatorname{Ind}_G^H(A) = \{f : G \longrightarrow A \text{ continuous } : f(\sigma\tau) = \sigma f(\tau) \text{ for } \sigma \in H\}.$$

We make $\operatorname{Ind}_G^H(A)$ into a G-module via the action $(\sigma f)(\tau) = f(\tau\sigma)$, for $\sigma \in G$, $f \in \operatorname{Ind}_G^H(A)$. We call this module the *induced module from H to G*. Notice that for $H = \{1\}$ we recover the definition of $\operatorname{Ind}_G(A)$. This more generalized version of induced modules is crucial to present the Shapiro Lemma, which gives a way to pass from bigger groups to smaller and vice versa by manipulating the coefficients.

Theorem 1.3.2 (Shapiro Lemma). *The Shapiro homomorphism*

$$\operatorname{sh} : H^n(G, \operatorname{Ind}_G^H(A)) \longrightarrow H^n(H, A)$$

is an isomorphism for all $n \geq 0$.

Applying Shapiro's Lemma to cohomology, it is clear that for any $n \geq 1$, $H^n(G, \operatorname{Ind}_G(A)) = 0$.

Combining this with the fact that cores res = index, we obtain that for a profinite group G and for any G-module A, the cohomology group $H^n(G, A)$ is a torsion group for each $n \geq 1$. Thus, as such, it can be decomposed into p-primary components

$$H^n(G, A) = \prod_p H^n(G, A)\{p\},$$

where p runs over all prime numbers. As a consequence, we deduce the following

Theorem 1.3.3. *Let G be a profinite group, H a closed subgroup of G and A a G-module. If the index $(G : H)$ is prime to p, then the restriction homomorphism*

$$\mathrm{res} : H^n(G, A)\{p\} \longrightarrow H^n(H, A)\{p\}$$

is injective for any $n \geq 0$. Consequently, if G is a pro-p-group, then for all $n \geq 0$ and for all G-modules A, $H^n(G, A)$ is killed by p.

We end by presenting Hilbert's Theorem 90 for Galois cohomology.

Theorem 1.3.4 (Hilbert 90)**.** *Let $L/\mathbb{F}$ be a normal extension. Then*

$$H^1(\mathrm{Gal}(L/\mathbb{F}), \mathbb{F}^\times) = \{0\}.$$

1.4 Quadratic Forms

Throughout this section assume that $\mathbb{F}$ is a field of characteristic $\mathrm{char}\,\mathbb{F} \neq 2$. A *$n$-ary quadratic form* over $\mathbb{F}$ is a (non-degenerate) homogeneous quadratic polynomial with coefficients in $\mathbb{F}$. Equivalently, a quadratic form q over $\mathbb{F}$ can be viewed as a map

$$q : V \longrightarrow \mathbb{F},$$

where V is a finite-dimensional $\mathbb{F}$-vector space. Let $\{x_1, \ldots, x_n\}$ be a basis for V; then we can write $q(v)$ as $q(v) = q(a_1x_1 + \ldots + a_nx_n) = \sum a_{ij}x_ix_j$. It follows from the non-degenerate assumption that every quadratic form can always be taken to be diagonalizable. In this case, we denote the quadratic form $q = \sum_{i=1}^n a_ix_i^2$ by $q = \langle a_1, \ldots, a_n\rangle$.

We say that the quadratic form q *represents* the element $a \in \mathbb{F}^\times$ if there exist $a_1, \ldots, a_n \in \mathbb{F}^\times$, such that $q(a_1, \ldots, a_n) = a$. Note that if a is represented by q, then b^2a is also represented by q. Therefore, we define the *value set* of q over $\mathbb{F}$ as

$$D_{\mathbb{F}}(q) = \{[a] \in \mathbb{F}^\times/\mathbb{F}^{\times 2} : q \text{ represents } a\}.$$

There are two basic operation on quadratic forms, namely, addition (denoted by $\perp$) and multiplication (denoted by $\cdot$). If $q_1 = \langle a_1, \ldots, a_n\rangle$ and $q_2 = \langle b_1, \ldots, b_m\rangle$, then

$$q_1 \perp q_2 = \langle a_1, \ldots, a_n, b_1, \ldots, b_m\rangle,$$

and

$$q_1 \cdot q_2 = q_1 \otimes q_2 = \langle a_i b_j : 1 \leq i \leq n,\ 1 \leq j \leq m \rangle .$$

Two quadratic forms q_1, q_2 are called *isometric*, denoted by $q_1 \cong q_2$, if there exists an invertible matrix M, such that $q_1(v) \cong q_2(Mv)$ for each $v \in V$. We view isometry between quadratic forms as an equivalence relation. A landmark achievement in the algebraic theory of quadratic forms is the following result due to E. Witt.

Theorem 1.4.1 (Witt's Cancellation Theorem)**.** *Let q, q_1, q_2 be quadratic forms over $\mathbb{F}$. If $q \perp q_1 \cong q \perp q_2$, then $q_1 \cong q_2$.*

The *hyperbolic plane* is the quadratic form $\mathbb{H} = \langle 1, -1 \rangle = x^2 - y^2$. A *hyperbolic form* is the sum of hyperbolic planes

$$\langle 1, -1, 1, -1, \ldots, 1, -1 \rangle \cong n \langle 1, -1 \rangle = n\mathbb{H}.$$

A quadratic form is called *isotropic* if it contains a hyperbolic form. Note that a form q is isotropic if and only if there are nontrivial solutions to the equation $q = 0$; so isotropic forms are not interesting, because one can reduce the study of these forms to their non-hyperbolic parts. We say that a quadratic form q is *anisotropic*, if the equation $q = 0$ has only trivial solutions, that is, a forms that contains no hyperbolic part. Therefore, it would be nice if one could single out only anisotropic quadratic forms over a given field. This is, however, complicated in principle, as it is not clear a priori how to decompose a quadratic form into its anisotropic part. The solution to this problem was again given by Witt in 1936.

Theorem 1.4.2 (Witt's Decomposition Theorem)**.** *Any quadratic form q can be decomposed as*

$$q = q_{an} \perp n\mathbb{H},$$

where q_{an} denotes the anisotropic part of q and n is a positive integer.

It follows from Witt's Cancellation Theorem that the quadratic form q uniquely determines both q_{an} and n. Using Witt's Decomposition Theorem we can now say that quadratic forms are classified by their anisotropic parts, and restrict our study to these, with the goal being to define an algebraic structure that captures the different classes of anisotropic quadratic forms.

We first wish to impose some algebraic structure on the set $\{[q_{\text{an}}]\}$ of all classes of anisotropic quadratic forms. For this, we need to define what "zero" means. Since a hyperbolic quadratic form has no anisotropic part, we consider the zero element to be the class $[\mathbb{H}]$ of the hyperbolic plane. Denote by $W\mathbb{F}$ the set

$$W\mathbb{F} = \{[\mathbb{H}], [q_{\text{an}}] : q \text{ quadratic form}\}.$$

We define an algebraic structure on $W\mathbb{F}$ using the operations defined on quadratic forms. If $[q_1], [q_2] \in W\mathbb{F}$ are classes represented by the quadratic forms q_1 and q_2, we have the following operations:

$$[q_1] \perp [q_2] = [q_1 \perp q_2]_{\text{an}},$$

and

$$[q_1] \cdot [q_2] = [q_1 \otimes q_2]_{\text{an}}.$$

Endowed with the above operations, the set $W\mathbb{F}$ is made into a ring, which we refer to as the *Witt ring* of $\mathbb{F}$.

The *fundamental ideal* of $W\mathbb{F}$ is the ideal $I\mathbb{F}$ consisting of all elements in $W\mathbb{F}$ represented by even-dimensional quadratic forms. As an additive group, $I\mathbb{F}$ is generated by quadratic forms of the form $\langle 1, a\rangle$, for $a \in F^\times$.

In particular, there exists a filtration

$$W\mathbb{F} = I^0\mathbb{F} \supseteq I\mathbb{F} \supseteq I^2\mathbb{F} \supseteq I^n\mathbb{F} \supseteq \cdots,$$

where $I^n\mathbb{F}$ denotes the n-th power of the ideal $I\mathbb{F}$. We associate a graded object to this filtration

$$\text{gr}W\mathbb{F} = \oplus_{n=0}^{\infty} I^n\mathbb{F}/I^{n+1}\mathbb{F}.$$

Similarly to $I\mathbb{F}$, for each n, $I^n\mathbb{F}$ is additively generated by forms $\langle 1, a_1\rangle \cdots \langle 1, a_n\rangle$, for $a_1, \ldots, a_n \in F^\times$. The latter product is denoted by

$$\langle\langle a_1, \ldots, a_n\rangle\rangle = \langle 1, a_1\rangle \cdots \langle 1, a_n\rangle$$

and is called a *n-fold Pfister forms.*

Examples.
Below we calculate some basic examples of Witt rings.

1. $\mathbb{F} = \bar{\mathbb{F}}$: If $\mathbb{F}$ is algebraically closed, then $\mathbb{F}^\times = \mathbb{F}^{\times 2}$. Therefore, every anisotropic quadratic form q is isometric to $\langle 1, 1, \ldots, 1\rangle$. Since $\langle 1, -1\rangle = \mathbb{H}$, we have $W\mathbb{F} = \mathbb{Z}/2$ and $I\mathbb{F} = 0$. This implies that $\text{gr}W\mathbb{F} = \mathbb{Z}/2$.

2. $\mathbb{F} = \mathbb{R}$: Notice that $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$. This means that the coefficients of an anisotropic quadratic form all must have the same sign. Therefore, any anisotropic quadratic form is either $q \cong n\langle 1\rangle$ or $q \cong \langle -1\rangle$ for $n \in \mathbb{N}$. Letting n run through all natural numbers, we have that $W\mathbb{R} = \mathbb{Z}$. And since $W\mathbb{R}/I\mathbb{R} \cong \mathbb{Z}/2$, we obtain that $I\mathbb{R} \cong 2\mathbb{Z}$. The graded Witt ring is $\mathrm{gr}W\mathbb{R} = \mathbb{Z}/2 \oplus 2\mathbb{Z}$.

3. $\mathbb{F} = \mathbb{F}_q$, $q = p^n$ for some n, $p \neq 2$: Recall that any element in $\mathbb{F}_q$ is a sum of two squares, therefore there are two square classes. We need to distinguish two cases.

   (a) $q \equiv 1 \bmod 4$. In this case, -1 is a square, so let σ be the nontrivial square class. Then all anisotropic forms are $\langle 1\rangle$, $\langle\sigma\rangle$ and $\langle 1, \sigma\rangle$. In other words,
   $$W\mathbb{F}_q = \mathbb{Z}/2[\langle 1\rangle, \langle\sigma\rangle] \cong \mathbb{Z}/2[\mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}].$$
   The fundamental ideal is generated by $\langle 1, \sigma\rangle$, giving us $I\mathbb{F}_q = \mathbb{Z}/2$. Thus
   $$\mathrm{gr}W\mathbb{F}_q = \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

   (b) $q \equiv 3 \bmod 4$. In this case the nontrivial square class is -1, so all quadratic forms are $\mathbb{H}$, $\langle 1\rangle$, $\langle 1, 1\rangle$ and $\langle -1\rangle$. Therefore, $W\mathbb{F}_q \cong \mathbb{Z}/4$ with the fundamental ideal being $I\mathbb{F}_q = \langle 1, 1\rangle$. We conclude that
   $$\mathrm{gr}W\mathbb{F}_q = \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

   This is the first illustration of the strength of the graded Witt ring compared to the Witt ring. Notice that even in fields of small complexity, such as finite fields, the structure of the Witt ring is closely related to the square classes. Contrary to that, the filtration of the Witt ring by powers of the fundamental ideal annihilates this issue. This gives us a good motivation for the study of the graded objects associated to Witt rings, rather than Witt rings on their own.

4. $\mathbb{F} = \mathbb{Q}_p$, p odd: Note that $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$, with elements represented by 1, σ, τ and $\sigma\tau$. We distinguish two cases again.

   (a) $p \equiv 1 \bmod 4$: In this case, -1 is a square, and so $\langle 1\rangle = \langle -1\rangle$. This implies that
   $$\langle\sigma, \sigma\rangle = \langle\sigma, -\sigma\rangle = \langle 1, -1\rangle = 0 \in W\mathbb{Q}_p,$$

and

$$\langle \sigma, \tau \rangle = \langle \sigma\tau, \sigma\tau \rangle \langle 1, 1 \rangle .$$

Therefore, all the generators of $W\mathbb{Q}_p$ are $\langle 1 \rangle$, $\langle 1 \rangle - \langle \tau \rangle$ and $\langle 1 \rangle - \langle \sigma\tau \rangle$. This gives us that

$$W\mathbb{Q}_p = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

The fundamental ideal $I\mathbb{Q}_p$ is generated by $\langle 1, \sigma \rangle$, $\langle 1, \tau \rangle$ and $\langle 1, \sigma\tau \rangle$. This means that $I^2\mathbb{Q}_p$ is generated by $\langle 1, \sigma, \tau, \sigma\tau \rangle$ and so $I^3\mathbb{Q}_p = 0$. Hence the structure of the graded Witt ring is

$$\mathrm{gr}W\mathbb{Q}_p = \mathbb{Z}_2 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_2 \cong \mathbb{Z}_2[K],$$

where K is the Kleinian group.

(b) $p \equiv 3 \bmod 4$: Then we can take $\sigma = -1$. Note that $\langle 1, -1 \rangle = \langle 1, 1 \rangle$. Moreover, $\langle \tau, \tau, \tau, \tau \rangle = \langle 1, 1, 1, 1 \rangle$, so $4(\langle \tau \rangle - \langle 1 \rangle) = 0$, and it is not hard to see that any other quadratic form is generated by $\langle 1 \rangle$ or $\langle 1 \rangle - \langle \tau \rangle$. Therefore,

$$W\mathbb{Q}_p = \mathbb{Z}_4 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_4[C_2].$$

The fundamental ideal $I\mathbb{Q}_p$ is generated by the form $2(\langle 1 \rangle - \langle \tau \rangle)$, and so $I^2\mathbb{Q}_p$ is generated by $\langle 1, \tau \rangle$ and $I^3\mathbb{Q}_p = 0$. Thus, the graded Witt ring is

$$\mathrm{gr}W\mathbb{Q}_p = \mathbb{Z}_2 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_2.$$

5. $\mathbb{F} = \mathbb{Q}$: The idea behind computing $W\mathbb{Q}$ would be to pass into completions. Using the ideas of Milnor and Tate, we have an isomorphism

$$W\mathbb{Q} \cong \mathbb{Z}/2 \oplus W\mathbb{R} \oplus \oplus_{p \neq 2, \infty} W\mathbb{Q}_p.$$

We have seen that $W\mathbb{R} = \mathbb{Z}$ and that $W\mathbb{Q}_p = W\mathbb{F}_p$ depends on whether -1 is a square modulo 4. This makes it difficult to explicitly compute the Witt ring of $\mathbb{Q}$. And this is where the strength of the graded Witt ring is illustrated in the best way. As we say, the graded Witt ring of $\mathbb{Q}_p$ is independent of whether p is congruent to 1 or 3 modulo 4. Since $\mathrm{gr}W\mathbb{R} = \mathbb{Z}/2$ and $\mathrm{gr}W\mathbb{Q}_p = \mathbb{Z}/2 \oplus (\mathbb{Z}/2 \oplus \mathbb{Z}/2) \oplus \mathbb{Z}/2$, we have that

$$\mathrm{gr}W\mathbb{Q} = \mathbb{Z}_2 \oplus \mathbb{Z}/2 \oplus (\oplus_{p \neq 2, \infty} \mathbb{Z}/2 \oplus (\mathbb{Z}/2 \oplus \mathbb{Z}/2) \oplus \mathbb{Z}/2).$$

Chapter 2

Characterizing pro-p-groups

After E. Becker's work on the redevelopment of the Artin-Schreier theory, pro-p-groups were put under the spotlight as a means of understanding absolute Galois groups. One of the fundamental notions in the study of pro-p-groups is cohomological dimension, which is a group invariant that encodes information related to the group structure. For instance, pro-p-groups of cohomological dimension 1 are free. In contrast, groups of cohomological dimension 2 are far less understood in general, however, under the assumption that they satisfy Poincaré duality, a complete classification of them was given by J. Labute.

First, we recall the main background on cohomological dimension, emphasizing the case of pro-p-groups. After describing the most fundamental properties of pro-p-groups of cohomological dimensions 1 and 2, we illustrate the results in the classification of Demushkin groups.

The background on cohomological dimension is treated in [Ser64] and [Koch02] and a thorough exposition of properties of pro-p-groups can be found in [DSMS99]. Finally, the work on the classification of Demushkin groups appearing in Section 2.3 can be found in [Dem61], [Dem63] and [Lab67].

2.1 Cohomological dimension

Let G be a profinite group. The cohomological dimension is a fundamental invariant of the group G which measures its cohomological complexity. In other words, cohomological dimension indicates whether and where the cohomology associated to a given group becomes trivial, yielding strong implications to structural properties of that group.

Definition 2.1.1. The *cohomological dimension* of a profinite group G, denoted by $\operatorname{cd} G$, is the smallest positive integer n, such that $H^k(G, A) = 0$ for all $k > n$ and for all torsion G-modules A. If no such n exists, we then write $\operatorname{cd} G = \infty$ and say that G has *infinite cohomological dimension.*

In practice, computing the cohomological dimension of a group G can be a rather hard task, as we must find a minimum index after which the cohomology group of G with coefficients in any torsion G-module vanishes, or else show that for any such module, no such n ever exists. Recall that the idea behind understanding a profinite group is to divide it into pro-p-groups and understand the latter. The moral of the story is the same here. Namely, since cohomological dimension is defined in a very general way and is too hard to capture, we define a more restricted notion of cohomological dimension that is easier to compute.

Definition 2.1.2. For a prime number p, the *p-cohomological dimension* of G, denoted by $\operatorname{cd}_p G$, is the smallest integer n, such that $H^k(G, A)\{p\} = 0$ for all $k > n$ and for all torsion G-modules A. Again, if no such n exists, we then say that G has *infinite p-cohomological dimension* and we write $\operatorname{cd}_p G = \infty$.

By grouping all G-modules according to their type of torsion, it is easy to see that $\operatorname{cd} G = \sup \operatorname{cd}_p G$. From this, it also follows that if G is a pro-p-group, then $\operatorname{cd} G = \operatorname{cd}_p G$. Another implication is that if H is a closed subgroup of G, then $\operatorname{cd} H \leq \operatorname{cd} G$ and if, in addition, H is normal, then $\operatorname{cd} G/H \leq \operatorname{cd} G$. A fundamental property of cohomological dimension is described in the following

Theorem 2.1.3 (Tower Theorem)**.** *Let G be a profinite group and let H be a closed normal subgroup of G. Then*

$$\operatorname{cd}_p G \leq \operatorname{cd}_p H + \operatorname{cd}_p G/H.$$

If, in addition, $\operatorname{cd}_p H = m < \infty$ and $\operatorname{cd}_p G/H = n < \infty$, we then have an isomorphism

$$H^{n+m}(G, A)\{p\} \overset{\cong}{\to} H^n(G/H, H^m(H, A))\{p\}.$$

Thus if H is a pro-p-group, such that $\#H^m(H, \mathbb{Z}/p) < \infty$, or if H is contained in the center of G, then

$$\operatorname{cd}_p G = \operatorname{cd}_p H + \operatorname{cd}_p G/H.$$

Proof. If either $\operatorname{cd}_p G \leq \operatorname{cd}_p H$ or $\operatorname{cd}_p G \leq \operatorname{cd}_p G/H$, then there is nothing to prove. To treat the remaining cases, we consider the Hochschild-Serre spectral sequence

$$H^i(G/H, H^j(H, A)) \overset{i}{\Rightarrow} H^\bullet(G, A)$$

and assume that $i + j > m + n$, that is, $i > m$ or $j > n$. In either case, $E_2^{ij} = \{0\}$ and consequently $E_{>2}^{ij} = \{0\}$. This gives us that $E_\infty^{ij} = \{0\}$ for $i + j > m + n$, which means that all the composition factors of $H^{i+j}(G, A)$ disappear. Therefore

$$\operatorname{cd}_p G \leq \operatorname{cd}_p H + \operatorname{cd}_p G/H,$$

as we wanted.

Now consider a Sylow p-subgroup $(G/H)_p$ of G/H and denote by G' its preimage in G under the group extension

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1.$$

Then G' is a closed subgroup of G, and thus $\operatorname{cd}_p G' \leq \operatorname{cd}_p G$, and so we can reduce the proof by replacing G with G'. Notice that we can now assume that G/H is a pro-p-group. But then $H^m(H, \mathbb{Z}/p)$ is a finite p-group, and so

$$H^n(G/H, H^m(H, \mathbb{Z}/p))\{p\} \neq 0.$$

The differential d_2 goes from E_2^{nm} to $E_2^{n+2,m-1}$, which is zero, since $\operatorname{cd}_p G/H = n$. Therefore, $E_2^{nm} = Z_2^{nm}$, $B_2^{nm} = 0$ and so $E_2^{nm} = E_3^{nm} = \ldots = E_\infty^{nm}$. However, as already shown, the only nonzero term on E_∞^{nm} happens on the line $i + j = m + n$. This gives us the isomorphism

$$H^{n+m}(G, A)\{p\} \overset{\cong}{\to} H^n(G/H, H^m(H, A))\{p\}.$$

Finally, assume that H is contained in the center of G and assume as before that G/H can be taken to be a pro-p-group. As H is contained in the center of G, it is an abelian group, and so $H = \coprod_p H\{p\}$. This means that we can express H as

$$H = H_p \times H',$$

where H_p is a Sylow p-subgroup of H and H' denotes the coproduct of all subgroups of H whose cardinality $\#H$ is prime to p. However, since $\#H'$ is prime to p, we have that

$$H^i(H', \mathbb{Z}/p) = 0$$

for all $i \geq 0$. Therefore,

$$H^m(H, \mathbb{Z}/p) = H^m(H_p, \mathbb{Z}/p) \neq 0.$$

Since $\operatorname{cd}_p H_p = \operatorname{cd} H_p \leq m$, we know that $H^m(H_p, \mathbb{Z}/p)$ is a $\mathbb{Z}/p$-vector space and is thus of the form $(\mathbb{Z}/p)^k$ for some exponent k. This gives us that

$$H^{n+m}(G, \mathbb{Z}/p) = H^n(G/H, H^m(H, \mathbb{Z}/p)) = H^n(G/H, (\mathbb{Z}/p)^k).$$

But now, the group H is abelian, so the action of G/H on $(Z/p)^k$ is trivial, implying that

$$H^n(G/H, (\mathbb{Z}/p)^k) = H^n(G/H, \mathbb{Z}/p)^k.$$

Therefore,

$$H^{n+m}(G, \mathbb{Z}/p) = H^n(G/H, \mathbb{Z}/p)^k \neq 0,$$

and the cohomological dimension of G is precisely $n + m$, concluding our proof. □

Examples.

1. If $G = \hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n$, then $\operatorname{cd}_p G = 1$. To see this, let A be a finite G-module of p-power order. In fact, by [Ser64, Proposition 21, page 27], it is enough to consider $\mathbb{Z}/p$ as a coefficient module, so take $A = \mathbb{Z}/p$. Consider the group extension

$$0 \longrightarrow \mathbb{Z}/p \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1.$$

Then, the closed subgroup $\overline{(\sigma)}$ of $\tilde{G}$ that is topologically generated by a preimage $\sigma \in \tilde{G}$ of $1 \in G$ is mapped isomorphically onto G. Since $H^1(G, \mathbb{Z}/p) = \mathbb{Z}/p \neq \{0\}$, we have that $\operatorname{cd}_p G \geq 1$. On the other hand, $H^2(G, \mathbb{Z}) \cong (H^1(G, \mathbb{Q}/\mathbb{Z}))^* \cong \mathbb{Q}/\mathbb{Z}$, and thus $H^2(G, \mathbb{Z}/p) = \{0\}$. As a result, we find that $\operatorname{cd}_p G = 1$.

As we shall see below, $cd_pG = 1$ if and only if any group extension of G by a pro-p-group splits.

An alternative way to arrive at this is by computing the cohomology groups below.

$$\begin{aligned} H^0(G, \mathbb{Z}/p)\{p\} = & \quad \mathbb{Z}/p \neq 0. \\ H^1(G, \mathbb{Z}/p)\{p\} = & \quad \mathbb{Z}/p \neq 0. \\ H^2(G, \mathbb{Z}/p)\{p\} = & \qquad \{0\}, \end{aligned}$$

so $\operatorname{cd}_p G = \operatorname{cd}_p \hat{\mathbb{Z}} = 1$.

2. If $\operatorname{cd}_p G \neq 0, \infty$, then the exponent of p in the order of G is infinite. Indeed, assume that p has finite exponent. If $G = 0$, then $\operatorname{cd}_p G = 0$, while if $G \neq 0$, then $\operatorname{cd}_p G = \infty$.

3. If $H^{n+1}(U, \mathbb{Z}) = H^{n+2}(U, \mathbb{Z}) = 0$, for all open subgroups U of G, then $\operatorname{cd}_p G \leq n$. Since $\operatorname{cd}_p G = \operatorname{cd}_p G_p = \operatorname{cd} G_p$, where G_p is a Sylow p-subgroup of G, it is enough to show that $\operatorname{cd} G_p \leq n$. We consider the short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{p} \mathbb{Z} \longrightarrow \mathbb{Z}/p \longrightarrow 0.$$

Associated to this short exact sequence in coefficients, there exists a long exact sequence in cohomology. In particular, a part of it reads as

$$H^n(G_p, \mathbb{Z}/p) \xrightarrow{\cdot p} H^{n+1}(G_p, \mathbb{Z}) \longrightarrow H^{n+1}(G_p, \mathbb{Z}) \longrightarrow H^{n+1}(G_p, \mathbb{Z}/p).$$

But since the map $H^{n+1}(G_p, \mathbb{Z}) \longrightarrow H^{n+1}(G_p, \mathbb{Z})$ is multiplication by p, we have that $H^{n+1}(G_p, \mathbb{Z}) = 0$. Thus $H^{n+1}(G_p, \mathbb{Z}/p) = 0$, which gives us that $\operatorname{cd} G_p = \operatorname{cd}_p G \leq n$.

2.2 Groups of small cohomological dimension

Groups of small cohomological dimensions have been studied extensively. Here, we present the most basic information on the development of that theory.

For this, let G be a pro-p-group. Recall that a subset X of G is a *system of topological generators of* G if

(i) G is the smallest group containing X;

(ii) every neighborhood of the identity 1_G contains almost all elements of X.

We say that a system of topological generators X of G is *minimal* if there is no proper subset of X that is a system of generators of G.

To begin our inquiry, we start by free pro-p-groups. To see how they are constructed, we consider an index set $\mathcal{I}$ and denote by $F_{\mathcal{I}}$ the free group on generators $\{x_i : i \in \mathcal{I}\}$. For each normal subgroup N of $F_{\mathcal{I}}$, we consider the projective system

$$\{F_{\mathcal{I}}/N : (F_{\mathcal{I}} : N) \text{ is a } p \text{ power and almost all } x_i \text{ belong to } N\},$$

whose projective limit $F(\mathcal{I}) = \varprojlim F_{\mathcal{I}}/N$ is a pro-p-group, called the *free pro-p-group generated by* $\{x_i : i \in \mathcal{I}\}$.

We say that a group extension

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

splits if there is a continuous section $C \longrightarrow B$ which is a homomorphism. Group extensions of G by A are in one-to-one correspondence with classes of $H^2(G, A)$. As a consequence, a group extension is split if and only if the corresponding class in $H^2(G, A)$ is trivial. This implies that if every group extension of G by A splits, then the cohomology group $H^2(G, A)$ is trivial and vice versa. Moreover, we have the following

Theorem 2.2.1. *For a pro-p-group G the following are equivalent.*

(i) $\operatorname{cd} G = 1$*;*

(ii) every group extension of G by a pro-p-group G′ splits;

(iii) G is free.

Proof. (i) ⇔ (ii) has already been shown.
(iii) ⇒ (ii): Assume that G is a free pro-p-group generated by $\{x_i : i \in \mathcal{I}\}$ and consider the group extension

$$1 \longrightarrow G' \longrightarrow \tilde{G}' \overset{\phi}{\to} G \longrightarrow 1.$$

Let $\sigma : G \longrightarrow \tilde{G}'$ be a continuous section. To continue, we need the next

Lemma. Let G be the pro-p-group freely generated by $\{x_i : i \in \mathcal{I}\}$, let G' be a pro-p-group and let $\{g_i : i \in \mathcal{I}\}$ be a subset of G, such that every neighborhood of the identity 1_G contains almost all elements of $\{g_i : i \in \mathcal{I}\}$. Then there exists a unique homomorphism

$$\phi : G \longrightarrow G',$$

such that $\phi(x_i) = g_i$ for all $i \in \mathcal{I}$.

Applying the Lemma to the free groups G, $\tilde{G}'$ and to the subset $\{\sigma x_i : i \in \mathcal{I}\}$ of G', we find a homomorphism

$$\sigma' : G \longrightarrow \tilde{G}',$$

such that $\phi\sigma' = \mathrm{id}_G$ or, equivalently, σ' is the inverse of ϕ. We therefore have found a continuous section from G to $\tilde{G}'$ that is a homomorphism, and thus the group extension splits.

(ii) $\Rightarrow$ (iii): Now assume that every group extension of G by a pro-p-group splits. Then in the category of pro-p-groups, G is a projective object. Note that since G is a pro-p-group,

$$G/\Phi(G) \cong \prod_{\mathcal{I}} \mathbb{F}_p$$

for some index $\mathcal{I}$. By the Lemma above, there exists a homomorphism

$$F(\mathcal{I}) \longrightarrow \prod_{\mathcal{I}} \mathbb{F}_p$$

whose kernel is $\Phi(F(\mathcal{I}))$. Moreover, by projectivity of G, there exists a unique morphism

$$\phi : G \longrightarrow F(\mathcal{I}),$$

such that the diagram

$$\begin{tikzcd}
 & G \arrow[dl, "\phi"'] \arrow[d] & \\
F(\mathcal{I}) \arrow[r] & \prod_{\mathcal{I}} \mathbb{F}_p \arrow[r] & 1
\end{tikzcd}$$

commutes. Since

$$G/\Phi(G) \cong F(\mathcal{I})/\Phi(F(\mathcal{I})),$$

the map

$$\phi : G \longrightarrow F(\mathcal{I})$$

is surjective. By the freeness of $F(\mathcal{I})$ there is a homomorphism

$$\psi : F(\mathcal{I}) \longrightarrow G,$$

such that $\phi\psi = \mathrm{id}_{F(\mathcal{I})}$. Since ϕ is surjective, we deduce that ψ is also surjective and so an isomorphism. Thus G is a free pro-p-group. □

In terms of functoriality, we have the following result.

Theorem 2.2.2. *Let $f : G \longrightarrow G'$ be a homomorphism of pro-p-groups. Then f is surjective if and only if $f^* : H^1(G', \mathbb{F}_p) \longrightarrow H^1(G, \mathbb{F}_p)$ is injective.*

Proof. Simply note that the dual of a pro-p-group G is $H^1(G, \mathbb{F}_p)$ and that a map is injective if and only if its dual is surjective. □

Recall that an equivalent definition to the (generator) rank, $d(G)$, of a pro-p-group G is the dimension of $H^1(G, \mathbb{F}_p)$ as a $\mathbb{F}_p$-vector space. The rank of G describes the minimal number of (topological) generators needed to construct G.

Assume that there exists an exact sequence

$$1 \longrightarrow R \longrightarrow F \overset{\phi}{\to} G \longrightarrow 1,$$

such that F is a free pro-p-group generated by a set $\{x_i : i \in \mathcal{I}\}$. Such a sequence is called a *presentation of G by F*. If $\{\phi x_i : i \in \mathcal{I}\}$ is a minimal system of generators of G, then we say that the presentation of G by F is *minimal.* A subset of $R' \subseteq R$ is called a *system of relations* of G or a *relator system* of G *with respect to the given presentation* if

(i) R is the smallest normal subgroup of F containing R'; and

(ii) every open normal subgroup of R contains almost all elements of R'.

We say that R' is *minimal* if there is no subset of R' that is a system of relations of G. We denote the cardinality of R' by $r(G)$ and call it the *relator rank.* Equivalently, $r(G)$ is the dimension of $H^2(G, \mathbb{F}_p)$ as a $\mathbb{F}_p$-vector space.

Before we are ready to present a characterization of pro-p-groups of cohomological dimension ≤ 2, we need the following technical result.

Theorem 2.2.3. *Consider a presentation*

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

of the pro-p-group G and let A be a discrete torsion G-module. If R acts trivially on A, then

$$H^1(G, H^1(R, A)) \cong H^3(G, A).$$

Proof. Consider the induced G-module $\mathrm{Ind}_G(A)$ and form the exact sequence of G-modules

$$0 \longrightarrow A \longrightarrow \mathrm{Ind}_G(A) \longrightarrow A' \longrightarrow 0.$$

Taking the associated long exact sequence in cohomology gives

$$0 \longrightarrow A^R \longrightarrow \mathrm{Ind}_G(A)^R \longrightarrow (A')^R \longrightarrow H^1(R, A) \rightarrow$$

$$\longrightarrow H^1(R, \mathrm{Ind}_G(A)) \longrightarrow H^1(R, A') \longrightarrow H^2(R, A) \longrightarrow H^2(R, \mathrm{Ind}_G(A)) \longrightarrow \cdots .$$

By assumption, R acts trivially on A, and so acts trivially on both $\mathrm{Ind}_G(A)$ and A'. Moreover, R is a subgroup of a free group, so it is free as well, and thus every cohomology group of R disappears after the first degree. Therefore, the above sequence takes the shape

$$0 \longrightarrow H^1(R, A) \longrightarrow H^1(R, \mathrm{Ind}_G(A)) \longrightarrow H^1(R, A') \longrightarrow 0.$$

Now, consider the homomorphism

$$f : H^1(R, \mathrm{Ind}_G(A)) \longrightarrow \mathrm{Ind}_G(H^1(R, A)).$$

$$\alpha(r, g) \mapsto f\alpha(r, g) = \alpha(\hat{g}^{-1} r \hat{g}, g),$$

for $r \in R, g \in G$ and where $\hat{g}$ is a lift of g in F. It follows that f is an isomorphism, and thus $H^1(R, \mathrm{Ind}_G(A)) \cong \mathrm{Ind}_G(H^1(R, A))$ meaning that the G-module $H^1(R, \mathrm{Ind}_G(A))$ is induced as well. Taking cohomology with respect to the short exact coefficient sequence

$$0 \longrightarrow H^1(R, A) \longrightarrow H^1(R, \mathrm{Ind}_G(A)) \longrightarrow H^1(R, A') \longrightarrow 0$$

induces the exact sequence

$$0 \longrightarrow H^1(R, A)^G \longrightarrow H^1(R, \mathrm{Ind}_G(A))^G \longrightarrow H^1(R, A')^G \longrightarrow H^1(G, H^1(R, A)) \longrightarrow 0.$$

On the other hand, the spectral sequence

$$H^p(G, H^q(R, \operatorname{Ind}_G(A))) \longrightarrow H^{p+q}(F, \operatorname{Ind}_G(A))$$

gives rise to the isomorphism

$$H^1(F, \operatorname{Ind}_G(A)) = H^0(G, H^1(R, \operatorname{Ind}_G(A))) \oplus H^1(G, \operatorname{Ind}_G(A)^R).$$

Since R acts trivially on $\operatorname{Ind}_G(A)$, we obtain the isomorphism

$$H^1(F, \operatorname{Ind}_G(A)) \cong H^0(G, H^1(R, \operatorname{Ind}_G(A))) = H^1(R, \operatorname{Ind}_G(A))^G.$$

Moreover, the inflation-restriction sequence induces

$$0 \longrightarrow H^1(G, A') \longrightarrow H^1(F, A') \longrightarrow H^1(R, A')^G \longrightarrow H^2(G, A') \longrightarrow 0.$$

Finally, since $\operatorname{Ind}_G(A)$ is cohomologically trivial, for each $n \geq 1$, we obtain the isomorphism

$$0 \longrightarrow H^n(G, A') \longrightarrow H^{n+1}(G, A) \longrightarrow 0$$

implying that $H^2(G, A') \cong H^3(G, A)$. Putting all these sequences together, we obtain the exact and commutative diagram

$$\begin{tikzcd}
 & & & H^1(R, A)^G \arrow[d] & & \\
 & 0 \arrow[r] & H^1(F, \operatorname{Ind}_G(A)) \arrow[r, "\cong"] \arrow[d] & H^1(R, \operatorname{Ind}_G(A))^G \arrow[r] \arrow[d] & 0 & \\
0 \arrow[r] & H^1(G, A') \arrow[r] & H^1(F, A') \arrow[r] \arrow[d] & H^1(R, A')^G \arrow[r] \arrow[d] & H^2(G, A') \arrow[r] \arrow[d, "\cong"] & 0 \\
 & & 0 & H^1(G, H^1(R, A)) \arrow[r, dashed] \arrow[d] & H^3(G, A) \arrow[d] & \\
 & & & 0 & 0 & .
\end{tikzcd}$$

However, the corestriction $H^1(G, A') \longrightarrow H^1(F, A')$ as well as the transgression $H^1(R, A')^G \longrightarrow H^2(G, A')$ are isomorphisms. Therefore, the commutativity of the diagram above shows that $H^1(G, H^1(R, A)) \cong H^3(G, A)$, whence the result. □

Using this, we can now establish a characterization of pro-p-groups G of $\operatorname{cd} G \leq 2$.

Theorem 2.2.4. *Let*

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

be a presentation of the pro-p-group G. The following are equivalent.

(i) $\operatorname{cd} G \leq 2$*;*

(ii) $H^1(R, \mathbb{F}_p)$ *is an induced G-module.*

Proof. (ii) ⇒ (i): If $H^1(R, \mathbb{F}_p)$ acts trivially on G, then $H^1(G, H^1(R, \mathbb{F}_p)) = 0$. However, by Theorem 2.2.3, $H^1(G, H^1(R, \mathbb{F}_p)) = H^3(G, \mathbb{F}_p)$, and thus $H^3(G, \mathbb{F}_p) = 0$, meaning that $\operatorname{cd} G = \operatorname{cd}_p G \leq 2$.

(i) ⇒ (ii): We will actually show something stronger, namely that $H^1(R, \mathbb{F}_p) \cong \operatorname{Ind}_G \coprod_i \mathbb{F}_p$. Consider a minimal relator system $\{r_i : i \in I\}$ of G and define a homomorphism

$$f : H^1(R, \mathbb{F}_p) \longrightarrow \operatorname{Ind}_G \coprod_I \mathbb{F}_p,$$

by

$$(f\alpha)g = \sum_{i \in I} \alpha(\hat{g}^{-1} r_i \hat{g}),$$

where $\alpha \in H^1(R, \mathbb{F}_p)$, $g \in G$, and $\hat{g}$ is a lift of g in F. By condition (ii) of the definition of a relator system, we get that $\alpha(\hat{g}^{-1} r_i \hat{g})$ vanishes almost everywhere, and so the map f is well defined.

By continuity of α, there is an open normal subgroup U of F, for which α depends only on the cosets of R modulo $R \cap U$. But then $f\alpha$ only depends on the cosets of F/U, and is thus continuous. Finally, it is easy to see that f is an injective homomorphism.

This yields the exact sequence

$$0 \longrightarrow H^1(R, \mathbb{F}_p) \xrightarrow{f} \operatorname{Ind}_G \coprod_I \mathbb{F}_p \longrightarrow C \longrightarrow 0.$$

Taking cohomology, gives

$$0 \longrightarrow H^1(R, \mathbb{F}_p)^G \xrightarrow{f^*} (\operatorname{Ind}_G \coprod_I \mathbb{F}_p)^G \longrightarrow C^G \longrightarrow H^1(G, H^1(R, \mathbb{F}_p)).$$

But $\operatorname{cd} G \leq 2$, and thus $H^1(G, H^1(R, \mathbb{F}_p)) \cong H^3(G, \mathbb{F}_p) = 0$ by Theorem 2.2.3.

Now, denote by R_i the subgroup of R generated by r_i. Since $\{r_i : i \in I\}$ is minimal, we have an isomorphism

$$H^1(R, \mathbb{F}_p)^G \overset{\cong}{\to} \coprod_{i \in I} H^1(R_i, \mathbb{F}_p).$$

Therefore, for every index $i \in I$, there exists a class $\alpha \in H^1(R, \mathbb{F}_p)^G$, such that $\alpha(r_i) = \delta_{ij}$ in $\mathbb{F}_p$ for some index $j \in I$. So the map f^* is surjective, meaning that $C^G = 0$. Since C is p-primary, we deduce that $C = 0$, and conclude that f is an isomorphism. □

2.3 Demushkin groups

We shall close this chapter by presenting the work of S. Demushkin, J.-P. Serre and J. Labute on the classification of Demushkin groups. S. Demushkin and J.-P. Serre initiated the study of such groups, and J. Labute completed it and classified all different types of Demushkin groups. The proofs are completely omitted, as the techniques go beyond of the scope of our work.

A pro-p-group G is called a *Demushkin group* if its Galois cohomology satisfies Poincaré duality in dimension 2, i.e.

(i) $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) < \infty$,

(ii) $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$, and

(iii) the cup product

$$H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \overset{\cup}{\to} H^2(G, \mathbb{F}_p)$$

is a nondegenerate bilinear form.

A natural question is any finite Demushkin groups exist. The answer, provided by Demushkin, is states as follows.

Theorem 2.3.1 (Demushkin)**.** *The cyclic group C_2 of order 2 is the only finite Demushkin group.*

Let G be a pro-p-group, such that $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = n < \infty$ and $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$. Then we see that

$$G^{\text{ab}} \cong \mathbb{Z}_p^n \text{ or } G^{\text{ab}} \cong \mathbb{Z}_p/q \times \mathbb{Z}_p^{n-1}.$$

The number q is a power of p and is an invariant of the group G. Note, moreover, that we can view the first case as G having invariant $q = 0$. Stating this, S. Demushkin gave the first description of a type of Demushkin groups. Below we present Labute's reinterpretation of it.

Theorem 2.3.2 (Demushkin). *Let G be a pro-p-group, with $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = n < \infty$, $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$ and with invariant $q \neq 2$. Then G is a Demushkin group if and only if it is isomorphic to the pro-p-group defined by n topological generators $x_1, \dots, x_n$, subject to the relation*

$$x_1^q[x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n].$$

Note that in this case, Demushkin showed that n has to be necessarily even. However, Demushkin's work is limited to the case that the invariant $q \neq 2$.

The situation when considering the case $q = 2$ is rather complicated. Serre described such groups G whose rank is odd. This was first studied by Serre and is demonstrated in the following Theorem, were again we provide Labute's interpretation

Theorem 2.3.3 (Serre). *Let G be a pro-p-group, such that $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = n < \infty$, with n odd, $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$ and with invariant $q = 2$. Then there exists a basis of topological generators $x_1, \dots, x_n$ for F, such that $G = F/(r)$, where*

$$r = x_1^2 x_2^{2^f}[x_2, x_3] \cdots [x_{n-1}, x_n],$$

where f is an integer ≥ 2 or $f = \infty$. Furthermore, for any relation of the above form with n odd, the group $G = F/(r)$ is a Demushkin group.

The last barrier toward a complete classification was to consider such groups when their rank is even. Even further core needs to be taken in order to present the statement. For any Demushkin group G, there exists a continuous homomorphism $\chi : G \longrightarrow \mathbb{U}_p$, where $\mathbb{U}_p$ denotes the group of units of $\mathbb{Z}_p$. Then the invariant q is the highest power of p, for which $\operatorname{im} \chi \subset 1 + q\mathbb{Z}_p$. Moreover, the index $(\operatorname{im} \chi : \operatorname{im}^2 \chi)$ plays an important role in the description of such Demushkin groups. In this regard, a complete answer was given by J. Labute in the following

Theorem 2.3.4 (Labute). *Let F be a free pro-p-group of rank $2n$, let r be an element of F and let $G = F/(r)$. Assume that G is Demushkin with* *invariant $q = 2$. Then there exists a basis $x_1, \ldots, x_{2n}$ of F, such that either*

$$r = x_1^{2+2^f}[x_1, x_2][x_3, x_4]\cdots[x_{2n-1}, x_{2n}], \text{ if } (\operatorname{im}\chi : \operatorname{im}^2\chi) = 2,$$

where f is an integer ≥ 2 or ∞, or

$$r = x_1^2[x_1, x_2]x_3^{2^f}[x_3, x_4][x_5, x_6]\cdots[x_{2n-1}, x_{2n}], \text{ if } (\operatorname{im}\chi : \operatorname{im}^2\chi) = 4,$$

where f is an integer ≥ 2.

Moreover, for any relations of the above forms, the group $G = F/(r)$ is a Demushkin group.

Putting these amazing results together gives us a complete classification of all Demushkin groups and furthermore shows that two Demushkin groups with the same rank and the same $\operatorname{im}\chi$ are isomorphic.

Theorem 2.3.5 (Labute). *Let $r, r' \in F^p[F, F]$, for a free pro-p-group F. Let $G = F/(r)$ and $G' = F/(r')$. If G and G' are Demushkin groups with $\operatorname{im}\chi = \operatorname{im}\chi'$, then there exists an automorphism mapping r to r'.*

In particular, if $(r) = (r')$ and $F/(r)$ is Demushkin, then there is an automorphism of F that sends r to r'.

Chapter 3

Koszulity

Quadratic algebras are graded algebras whose generators lie in degree 1 and with homogeneous quadratic generating relations. Among quadratic algebras, we single out the family of Koszul algebras. These are algebras whose cohomology has an extremely nice behavior. Namely, if an algebra is Koszul, then its cohomology is nothing but its quadratic dual algebra. This offers a relatively easy way to provide a complete description of the cohomology ring of such an algebra, and as a consequence, a presentation of it in terms of generators and relations. Koszul algebras were first introduced by S. Priddy in [Pri70] and have since been studied extensively in many contexts: Galois cohomology, commutative algebra, algebraic geometry, representation theory and quantum groups to name a few.

In this chapter, we present the basic vocabulary around quadratic and Koszul algebras and demonstrate some key properties, as well as fundamental examples of such algebras. A complete exposition of Koszulity can be found in [PP05] and in [LV12].

3.1 Quadratic algebras and Quadratic duals

Let $\Bbbk$ be a field. A $\Bbbk$-algebra A is *graded* if it admits a $\Bbbk$-vector space decomposition $A = \oplus_{n\in\mathbb{Z}} A_n$, such that $A_n A_m \subseteq A_{n+m}$. Similarly, a left A-module M is called *graded* if it admits a $\Bbbk$-vector space decomposition $M = \oplus_{n\in\mathbb{Z}} M_n$, such that $A_n M_m \subseteq M_{n+m}$.

We henceforth assume that any graded algebra A is *connected*, i.e. $A_0 = \Bbbk \cdot 1_A \cong \Bbbk$ and $A_n = 0$ for $n < 0$, and of *finite type*, that is $\dim_{\Bbbk} A_n < \infty$ for each $n \geq 0$.

In addition to identifying A_0 with $\mathbb{k} \cong 1_A \otimes \mathbb{k}$, we moreover assume that A_1 can be identified with a $\mathbb{k}$-vector space V of generators. Graded algebras for which A_1 is isomorphic to some vector space V of generators, are called *one-generated*. Hence, we get a decomposition of a one-generated algebra A as

$$A = \mathbb{k} \oplus V \oplus \left(\oplus_{n\geq 2} A_n\right).$$

We denote $A_+ = \oplus_{n=1}^{\infty} A_n$ and call it the *augmentation ideal* of A.

The *tensor algebra* over a finite-dimensional $\mathbb{k}$-vector space V is the graded algebra defined as

$$\mathbb{T}(V) = \bigoplus_{n\in\mathbb{N}} V^{\otimes n},$$

with $V^{\otimes 0} \cong \mathbb{k}$. Under the assumption that V has a basis $\{x_1, \ldots, x_d\}$ we can then identify $\mathbb{T}(V)$ with $\mathbb{k}\langle x_1, \ldots, x_d\rangle$, the $\mathbb{k}$-algebra freely generated over variables $x_1, \ldots, x_d$.

It is a well known fact that, for any graded algebra A, there always exists a natural map

$$p : \mathbb{T}(V) \longrightarrow A.$$

And A is one-generated if and only if the map p is surjective. Now, identifying $\mathbb{T}(V)$ with $\mathbb{k}\langle x_1, \ldots, x_d\rangle$, we see that p is surjective if and only if all generators of A belong to V. Denote the kernel of p by $I := \ker p$. Then the surjectivity of p implies that

$$\mathbb{T}(V)/I \cong A.$$

Definition 3.1.1. A one-generated algebra A is called *quadratic*, if I is generated as a two-sided ideal in $\mathbb{T}(V)$ by its subspace

$$R := I \cap \mathbb{T}_2(V) \subseteq V^{\otimes 2}.$$

In other words, every quadratic algebra A can be expressed as a quotient of the tensor algebra $\mathbb{T}(V)$ by some two-sided ideal (R) of homogeneous quadratic relators. This means that a quadratic algebra A is completely determined by a $\mathbb{k}$-vector space V of generators and a subspace $R \subseteq V^{\otimes 2}$ of homogeneous quadratic relators. We therefore denote such an algebra by $A = \{V, R\}$.

The fact that all relators in R are homogeneous means that A naturally inherits a grading from the grading on $\mathbb{T}(V)$.

Definition 3.1.2. Let $A = \{V, R\}$ be a quadratic algebra. We define the *quadratic dual algebra* $A^!$ of A as the quadratic algebra constructed by

$$A^! = \{V^*, R^\perp\},$$

where V^* is the dual vector space of V and $R^\perp \subseteq (V^*)^{\otimes 2}$ is the complement to R, defined as

$$R^\perp = \{\alpha \in (V^{\otimes 2})^* : \alpha(r) = 0 \text{ for all } r \in R\}$$

with respect to the pairing

$$\langle v_1 \otimes v_2, v_1^* \otimes v_2^* \rangle = \langle v_1, v_1^* \rangle \cdot \langle v_2 \otimes v_2^* \rangle .$$

Since V is a finite-dimensional $\Bbbk$-vector space, we get that $(V^*)^* = V$ and $(R^\perp)^\perp = R$. Therefore $(A^!)^! = A$.

Examples.
Below we present the most fundamental examples of quadratic algebras, together with their quadratic duals.

1. **Tensor algebras:** Consider the graded $\Bbbk$-algebra $A = \mathbb{T}(V)$, where V is a finite-dimensional $\Bbbk$-vector space. Since $\mathbb{T}(V) = \mathbb{T}(V)/(0)$, A is quadratic and can be expressed as

   $$A = \{V, 0\}.$$

   We now have that $A^! = \{V^*, 0^\perp\}$. An easy calculation shows that $A_0^* = \Bbbk^* = \Bbbk$, $A_1^! = V^*$, $R^\perp = 0^\perp = (V^*)^{\otimes 2}$. Thus

   $$A^! = \mathbb{T}(V)^! = \Bbbk \oplus V^* = \{V^*, (V^*)^{\otimes 2}\}.$$

2. **Symmetric algebras:** Let $A = \mathrm{Sym}(V)$ be the symmetric algebra over a finite-dimensional $\Bbbk$-vector space V. Since

   $$\mathrm{Sym}(V) = \mathbb{T}(V)/(\langle a \otimes b - b \otimes a \rangle : a, b \in V),$$

   we have that $\mathrm{Sym}(V)$ is a quadratic algebra and thus can be written as $\mathrm{Sym}(V) = \{V, R\}$, with R being generated as

   $$(R) = \langle a \otimes b - b \otimes a : a, b \in V \rangle .$$

We next determine $A^! = \mathrm{Sym}(V)^! = \{V^*, R^\perp\}$. It is not hard to see that, $R^\perp = \bigwedge$, the relation generated by all elements of the form

$$\bigwedge = \langle a \otimes b + b \otimes a : a, b \in V \rangle .$$

This yields

$$A^! = \{V^*, \bigwedge\}.$$

Or, in other words, the quadratic dual to the symmetric algebra is the exterior algebra with dual space of generators.

3. **Galois cohomology:** Let p be a prime number, assume that $\mathbb{F}$ is a field that contains a primitive p-th root of unity ζ_p and denote by $\mathbb{F}_s$ a separable closure of $\mathbb{F}$ and by $G_{\mathbb{F}} = \mathrm{Gal}(\mathbb{F}_s/\mathbb{F})$ the absolute Galois group of $\mathbb{F}$. We denote the Galois cohomology groups of $G_{\mathbb{F}}$ with coefficients in $\mathbb{F}_p$ on degree $n \in \mathbb{N}$ by $H^n(\mathbb{F}, \mathbb{F}_p)$ and the Galois cohomology algebra of $G_{\mathbb{F}}$ by $H^\bullet(\mathbb{F}, \mathbb{F}_p) = \oplus_n H^n(\mathbb{F}, \mathbb{F}_p)$.

   Consider now the Milnor K-theory of the field $\mathbb{F}$, $K^M_\bullet \mathbb{F}$, defined as

   $$K^M_\bullet \mathbb{F} = \mathbb{T}(\mathbb{F}^\times)/(a \otimes (1-a) : 1 \neq a \in \mathbb{F}^\times).$$

   Since the ideal $(\langle a \otimes (1-a), 1 \neq a \in \mathbb{F}^\times \rangle)$ is homogeneous quadratic homogeneous, the Milnor K-theory is a quadratic algebra. The Bloch-Kato Conjecture asserts that there is a natural isomorphism $H^n(\mathbb{F}, \mathbb{F}_p) \cong K^M_n \mathbb{F}/p$ for each $n \in \mathbb{N}$. Thus the graded $\mathbb{F}_p$-algebra $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is also a quadratic algebra.

4. Consider the polynomial algebra $\mathbb{Q}[x]/(x^p + a)$, where p is an odd prime number and $a > 0$ is not a p-th power. By Eisenstein's theorem, the polynomial $x^p + a$ is irreducible in $\mathbb{Q}[x]$, thus for any quadratic polynomial $f(x)$ with rational coefficients, we have that $x^p + a \notin \mathbb{Q}[x]f(x)\mathbb{Q}[x]$. This means that the relation $x^p + a$ cannot be expressed in terms of a quadratic relation, and thus the algebra $\mathbb{Q}[x]/(x^p + a)$ is not a quadratic algebra.

Constructing new quadratic algebras from old

The next natural thing is to ask what are the operations we can do with such algebras. For this, let $A = \{V_A, R_A\}$ and $B = \{V_B, R_B\}$ be two quadratic algebras.

Free product: The *free product* of A and B is denoted by $A \sqcup B$ and is defined as

$$A \sqcup B = \mathbb{T}(V_A \oplus V_B)/(R),$$

where $R = R_A \oplus R_B$.

Direct sum: The *direct sum* $A \sqcap B$ of A and B is defined as

$$A \sqcap B = \mathbb{T}(V_A \oplus V_B)/(R),$$

where $R = R_A \oplus R_B \oplus (A_1 \otimes B_1) \oplus (B_1 \otimes A_1)$.

Symmetric tensor product: The *symmetric tensor product* $A \otimes^1 B$ of A and B is given by

$$A \otimes^1 B = \mathbb{T}(V_A \oplus V_B)/(R),$$

where $R = R_A \oplus R_B \oplus \langle a \otimes b - b \otimes a : a \in A_1, b \in B_1 \rangle$.

Skew-symmetric tensor product: We finally define the *skew-symmetric tensor product* of A and B, denoted by $A \otimes^{-1} B$ as

$$A \otimes^{-1} B = \mathbb{T}(V_A \oplus V_B)/(R),$$

with $R = R_A \oplus R_B \oplus \langle a \otimes b + b \otimes a : a \in A_1, b \in B_1 \rangle$.

In all of the above cases, the new algebras constructed are quadratic. To see this, it is enough to note that the direct sum of homogeneous quadratic ideals is also homogeneous quadratic.

3.2 Koszul algebras

In theory, in order to compute the cohomology of an algebra, it is enough to use the bar construction and construct the normalized cobar complex. However, in practice, this is an extremely hard task. To this extent, we have to define more "refined" complexes, that are easier to construct, but also in a way so that the necessary algebra information is not compromised.

This, of course, sounds nothing but a utopia. Nevertheless, for any quadratic $\Bbbk$-algebra, we can always construct a special kind of complexes of free graded A-modules, called linear complexes, that possess all desired properties so that they could resolve the ground field $\Bbbk$. Such complexes are relatively easier to construct by hand, however, it turns out that more often than not they are not exact.

And here comes the motivation for Koszul algebras. They are a class of quadratic algebras, for which the aforementioned linear complex is a resolution of $\Bbbk$. In other words, Koszul algebras are quadratic algebras whose cohomology ring can be computed in a more combinatorial way; and moreover, as we shall see, the typical loss of information when passing from an algebraic/topological object to its cohomology is nonexistent here.

Definition 3.2.1. Let A be a quadratic $\Bbbk$-algebra and let M be a graded A-module. A graded resolution

$$\cdots \longrightarrow P_2 \overset{d_2}{\to} P_1 \overset{d_1}{\to} P_0 \overset{d_0}{\to} M,$$

where each P_n is a graded left A-module, is called *linear*, if for each n,

$$\mathrm{id} \otimes d_n : \Bbbk \otimes_A P_n \longrightarrow \Bbbk \otimes_A P_{n-1}$$

is zero and P_n is generated in degree n, or equivalently, $P_n = A(P_n)_n$.

Linear resolutions are easier to construct, since each component differs by one degree from the previous one. But, deciding whether we are able to find such a resolution is often too hard. This is why S. Priddy distinguished the Koszul algebras, as a special family of quadratic algebras, whose cohomology groups can be computed via a linear resolution.

Definition 3.2.2. A graded $\Bbbk$-algebra A is called *Koszul* if the trivial A-module $\Bbbk$ admits a linear resolution.

In particular,

Proposition 3.2.3. *A Koszul algebra is a quadratic algebra.*

Proof. See [PP05, Chapter 1, Corollary 5.3]. □

Following this definition, to show that a graded $\Bbbk$-algebra A is Koszul, we need to find a linear resolution for the trivial A-module $\Bbbk$. However, in practice, there is a plethora of linear complexes that can be constructed for $\Bbbk$ and finding which is the correct one and whether any of them is a resolution is hopeless. It was Priddy who overcame this problem as well, by finding a natural candidate, called the Koszul complex.

The Koszul complex associated to a quadratic $\Bbbk$-algebra is a complex of graded A-modules whose initial term is $\Bbbk$. By construction, a Koszul complex consists of free A-modules and is linear, so it is the ideal complex to test Koszulity. Another advantage of Koszul complexes is that one has a building "recipe" for each of their terms and differentials.

We denote the Koszul complex of quadratic algebra A by $\mathcal{K}_\bullet(A)$. It is the complex, whose degree n component is given by the graded A-module

$$\mathcal{K}_n(A) = A \otimes (A^!_n)^*,$$

for each $n \in \mathbb{N}$.

Now, to present the differentials $d_n : \mathcal{K}_n(A) \longrightarrow \mathcal{K}_{n-1}(A)$, we proceed as follows. First, we make A into a right A-module via the algebra multiplication. We then view $(A^!)^*$ as a right $A^!$-module via the action

$$({}^b\phi)c = \phi(bc),$$

where $b \in A^!$ acts on $\phi \in (A^!)^*$ and the action is evaluated at $c \in (A^!)$. Taking into account both actions, the $\Bbbk$-vector space $\mathcal{K}_n(A) = A \otimes (A^!_n)^*$ is made into a right $(A \otimes A^!)$-module. Let $\{x_1, \dots, x_d\}$ be a fixed basis of V and denote the dual basis of V^* by $\{x_1^*, \dots, x_d^*\}$. Then for each $n \in \mathbb{N}$, the differential d_n is given as

$$d_n : \mathcal{K}_n(A) \longrightarrow \mathcal{K}_{n-1}(A)$$

$$a \otimes \phi \mapsto d_n(a \otimes \phi) = \sum_i ax_i \otimes {}^{x_i^*}\phi.$$

Definition 3.2.4. The *Koszul complex* $(\mathcal{K}_\bullet(A), d_\bullet)$ of a quadratic algebra $A = \{V, R\}$, where $V = \operatorname{span}\{x_1, \dots, x_d\}$, is the complex whose degree n component is defined as

$$\mathcal{K}_n(A) = A \otimes (A^!_n)^*$$

and with differentials given by

$$d_n : \mathcal{K}_n(A) \longrightarrow \mathcal{K}_{n-1}(A)$$

$$a \otimes \phi \mapsto d_n(a \otimes \phi) = \sum_i ax_i \otimes {}^{x_i^*}\phi,$$

$a \in A, \phi \in (A^!_n)^*$, as constructed above.

Proposition 3.2.5. *The maps d_n are differentials.*

Proof. To verify this, we have to show that $d_n \circ d_{n+1} = 0$ for all $n \in \mathbb{N}$. Since all $\Bbbk$-vector spaces are assumed to be finite-dimensional, we have natural isomorphisms

$$(V \otimes V^!)^{\otimes 2} \cong V^{\otimes 2} \otimes V^{!\otimes 2} \cong V^{\otimes 2} \otimes (V^{\otimes 2})^*.$$

Moreover, for any finite-dimensional $\Bbbk$-vector space U, there is a natural bijective map

$$U \otimes U^* \longrightarrow \mathrm{Hom}_{\Bbbk}(U, U),$$

given by sending

$$u_1 \otimes f(-) \mapsto f(-)u_1.$$

Therefore, taking U to be V, we have a natural isomorphism

$$(V \otimes V^!)^{\otimes 2} \cong \mathrm{Hom}_{\Bbbk}(V^{\otimes 2}, V^{\otimes 2}).$$

Similarly for $A_2 = \frac{V^{\otimes 2}}{R}$, we have

$$\begin{aligned} A_2 \otimes A_2^! = & \quad \frac{V^{\otimes 2}}{R} \otimes \frac{V^{*\otimes 2}}{R^{\perp}} \\ \cong & \quad \frac{V^{\otimes 2}}{R} \otimes R^* \\ \cong & \quad \mathrm{Hom}_{\Bbbk}\left(R, \frac{V^{\otimes 2}}{R}\right). \end{aligned}$$

The algebra $A \otimes A^!$ comes equipped with a multiplication map

$$\mu : (A \otimes A^!)^{\otimes 2} \longrightarrow A \otimes A^!.$$

Then restricting $\mu_{|V \otimes V^!} = \mu_{|V \otimes V^*}$, we obtain a new map

$$\mu_{|V \otimes V^*} : (V \otimes V^*)^{\otimes 2} \longrightarrow A_2 \otimes A_2^!.$$

Note, however, that $(V \otimes V^*)^{\otimes 2} \cong \mathrm{Hom}_{\Bbbk}(V^{\otimes 2}, V^{\otimes 2})$ and $A_2 \otimes A_2^! \cong \mathrm{Hom}_{\Bbbk}\left(R, \frac{V^{\otimes 2}}{R}\right)$. Therefore, we can rewrite the map $\mu_{|V \otimes V^*}$ as

$$m : \mathrm{Hom}_{\Bbbk}(V^{\otimes 2}, V^{\otimes 2}) \longrightarrow \mathrm{Hom}_{\Bbbk}\left(R, \frac{V^{\otimes 2}}{R}\right).$$

Notice that m restricts $V^{\otimes 2}$ to R, and then it composes it with the canonical projection from $V^{\otimes 2}$ to $\frac{V^{\otimes 2}}{R}$. This translates into the commutative diagram

$$\begin{tikzcd}
(V \otimes V^*)^{\otimes 2} \arrow[r, "\cong"] \arrow[d, "\mu"] & \mathrm{Hom}_{\Bbbk}(V^{\otimes 2}, V^{\otimes 2}) \arrow[d, "m"] \\
(A_2 \otimes A_2^!)^{\otimes 2} \arrow[r, "\cong"'] & \mathrm{Hom}_{\Bbbk}(R, \frac{V^{\otimes 2}}{R}).
\end{tikzcd}$$

By the diagram above, showing that the composition of two consecutive differentials is the zero map is equivalent to showing that two composed actions are zero. However, from the identification of $V \otimes V^*$ with $\mathrm{Hom}_{\Bbbk}(V^{\otimes 2}, V^{\otimes 2})$, we can identify $\sum_i x_i \otimes x_i^*$ with $\mathrm{id}_{V^{\otimes 2}}$. Applying the map m to the latter element, we get that $m(\mathrm{id}_{V^{\otimes 2}})$ is a homomorphism that sends an element from R to $V^{\otimes 2}$ modulo R, and hence is zero, i.e. $m(\mathrm{id}_{V^{\otimes 2}}) = 0$. This implies that

$$\mu((\sum_i x_i \otimes x_i^*)^{\otimes 2}) = 0.$$

And since the maps d_n were defined exactly by this action, we deduce that the composition of two consecutive d_n's is the zero map. Thus the maps d_n's are differentials, as we wanted. □

We shall now try to decipher the Koszul complex a little further. First, each of the elements $(A_n^!)^*$ is defined as a $\Bbbk$-vector space, and is free by definition. However, to make sure that we turn the Koszul complex into a complex of A-modules, we tensor on the left with A. In this way, for each $n \in \mathbb{N}$, $\mathcal{K}_n(A) = A \otimes (A_n^!)^*$ is made into a A-module, and since both components are free A- and $\Bbbk$-modules respectively, by definition, $\mathcal{K}_n(A)$ is free as well. Thus, in order to provide a better description of $\mathcal{K}_n(A)$, it suffices to provide a more concrete description of $(A_n^!)^*$. To this extent, we have

$$\begin{aligned}
(A^!_n)^* &= \operatorname{Hom}^n_{\Bbbk}(A^!, \Bbbk)\\
&= \operatorname{Hom}_{\Bbbk}(A^!_n, \Bbbk)\\
&= \operatorname{Hom}_{\Bbbk}\left(\frac{(V^*)^{\otimes n}}{\sum_{i=0}^{n-2}(V^*)^{\otimes i}\otimes R^{\perp}\otimes (V^*)^{\otimes n-i-2}}, \Bbbk\right)\\
&= \operatorname{Hom}_{\Bbbk}\left(\left(\sum_{i=0}^{n-2}(V^*)^{\otimes i}\otimes R^{\perp}\otimes (V^*)^{\otimes n-i-2}\right)^c, \Bbbk\right)\\
&= \operatorname{Hom}_{\Bbbk}\left(\left(\bigcap_{i=0}^{n-2}(V^*)^{\otimes i}\otimes R^{\perp}\otimes (V^*)^{\otimes n-i-2}\right)^c, \Bbbk\right)\\
&= \operatorname{Hom}_{\Bbbk}\left(\bigcap_{i=0}^{n-2}(V^*)^{\otimes i}\otimes (R^{\perp})^c\otimes (V^*)^{\otimes n-i-2}, \Bbbk\right)\\
&= \bigcap_{i=0}^{n-2} V^{\otimes i}\otimes R\otimes V^{\otimes n-i-2},
\end{aligned}$$

as V is a finite-dimensional $\Bbbk$-vector space and where $-^c$ denotes the complement of $-$.

So, the Koszul complex starts as follows.

$$\cdots \longrightarrow A\otimes(R\otimes V\cap V\otimes R)\longrightarrow A\otimes R\longrightarrow A\otimes V\longrightarrow A\longrightarrow \Bbbk\longrightarrow 0.$$

The strongest motivation for studying Koszul complexes lies in the following Theorem by Priddy.

Theorem 3.2.6 (Priddy)**.** *Let $A = \{V, R\}$ be a quadratic algebra with associated Koszul complex $\mathcal{K}_\bullet(A)$. Then A is Koszul if and only if $\mathcal{K}_\bullet(A)$ is a resolution.*

Proof. See [PP05, Chapter 2, Corollary 3.2]. □

Example.
Let $A = \Bbbk\langle a, b, c : ab - bc, bc - ca\rangle$. Then A is Koszul, since the associated Koszul complex is acyclic. Since $(A^!_n)^* = \cap_{i=0}^{n-2} V^{\otimes i}\otimes R\otimes V^{\otimes n-i-2}$ and it is not hard to see that $R\otimes V\cap V\otimes R = 0$, the Koszul complex of a A is of the form

$$0\longrightarrow A\otimes R\xrightarrow{d_2} A\otimes V\xrightarrow{d_1} A\otimes\Bbbk\overset{\varepsilon=d_0}{\twoheadrightarrow}\Bbbk.$$

The maps send the leftmost element of the right hand side to the rightmost element of the left hand side of the tensor product. Denote the element $1\cdot a$ by $\underline{a}$. Then a basis of $A\otimes\Bbbk$ is simply $\{\underline{1}\}$; a basis for $A\otimes V$ is $\{\underline{a}, \underline{b}, \underline{c}\}$ and the basis for $A\otimes R$ is $\{\underline{ab} - \underline{bc}, \underline{bc} - \underline{ca}\}$.

The differentials look as follows.

$$\begin{aligned}
d_2(\underline{ab} - \underline{bc}) = & \quad d_2((1 \cdot a)(1 \cdot b) - (1 \cdot b)(1 \cdot c)) \\
= & \quad a(1 \cdot b) - b(1 \cdot c) \\
= & \quad a\underline{b} - b\underline{c}, \\
d_2(\underline{bc} - \underline{ca}) = & \quad b\underline{c} - c\underline{a},
\end{aligned}$$

and in the same fashion, we see that

$$\begin{aligned}
d_1(\underline{a}) = & \quad a\underline{1}, \\
d_2(\underline{b}) = & \quad b\underline{1}, \\
d_1(\underline{c}) = & \quad c\underline{1}.
\end{aligned}$$

To check that the above complex of $\Bbbk$ is exact, all we need to show is that its homology on each degree is trivial.

In degree 0, $\operatorname{im} d_1 = A_+$ and so is $\ker \varepsilon$, thus $H_0(\mathcal{K}_\bullet(A)) = 0$.

In degree 1,

$$\begin{aligned}
\ker d_1 = & \quad \{0\} \cup \{v \in A^3 \backslash \{0\} : v \cdot (a, b, c) = 0\} \\
= & \quad \{0\} \cup \{v \in A^3 \backslash \{0\} : v_1 a + v_2 b + v_3 c = 0\}.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\operatorname{im} d_2 = & \quad \langle d_2(\underline{ab} - \underline{bc}), d_2(\underline{bc} - \underline{ca}) \rangle \\
= & \quad \langle a\underline{b} - b\underline{c}, b\underline{c} - c\underline{a} \rangle \\
= & \quad \langle (0, a, -b), (-c, 0, b) \rangle .
\end{aligned}$$

It is easy to see that, since the complex is a chain complex, $\operatorname{im} d_2 \subseteq \ker d_1$. However, since the algebra A is a quadratic algebra, nothing else can go to zero, so $\operatorname{im} d_2 = \ker d_1$, which gives us that $H_1(\mathcal{K}_\bullet(A)) = 0$.

In degree 2,

$$\ker d_2 = \quad \{0\} \cup \{v \in A^2 \backslash \{0\} : (-v_2 c, v_1 a, -v_1 b + v_2 b) = (0, 0, 0)\}.$$

This of course gives us the system

$$\begin{cases} -v_2 c = 0 \\ v_1 a = 0 \\ -v_1 b + v_2 b = 0. \end{cases}$$

Now, $-v_2c = 0$ if and only if $v_2c = 0$ if and only if $(0, 0, v_2) \in \ker d_1 = \operatorname{im} d_2$, However, since $\operatorname{im} d_2$ is generated by $(0, a, -b)$ and $(-c, 0, b)$, it is clear that $(0, 0, v_2)$ belongs to $\operatorname{im} d_2$ if and only if $v_2 = 0$. Hence the above system reduces to

$$\begin{cases} v_2 = 0 \\ v_1 a = 0 \\ v_1 b = 0. \end{cases}$$

Reasoning along these lines, we find that $v_1 = 0$ as well. Therefore,

$$\ker d_2 = \{0\} \cup \{v \in A^2 \backslash \{0\}\} = \{0\} \cup \emptyset = \{0\}.$$

And $\operatorname{im} d_3 = 0$ implies $H_2(\mathcal{K}_\bullet(A)) = 0$.

For $n \geq 3$, the homology $H_n(\mathcal{K}_\bullet(A))$ is trivially zero, as the complex on these degrees is zero. Hence the homology of $\mathcal{K}_\bullet(A)$ is trivial and thus the Koszul complex is exact, as we wanted.

Theorem 3.2.7. *A quadratic algebra is Koszul if and only if its quadratic dual is Koszul.*

Proof. Since $(A^!)^! \cong A$, it is enough to show one direction. Consider the Koszul complex

$$\cdots \longrightarrow A \otimes_{\Bbbk} (A^!_n)^* \longrightarrow \cdots \longrightarrow A \otimes_{\Bbbk} (A^!_2)^* \longrightarrow A \otimes_{\Bbbk} V \longrightarrow A$$

associated to A. Since A is Koszul, the above complex is a resolution of $\Bbbk$. Recall now that if

$$\cdots \longrightarrow S_{n+1} \longrightarrow S_n \longrightarrow \cdots$$

is an exact sequence of finite-dimensional $\Bbbk$-vector spaces, then the dual sequence

$$\cdots \longleftarrow S^*_{n+1} \longleftarrow S^*_n \longleftarrow \cdots$$

is also exact. Therefore, the dual to the Koszul complex

$$\cdots \longrightarrow A^! \otimes_{\Bbbk} (A_{m-n})^* \longrightarrow \cdots \longrightarrow A^! \otimes_{\Bbbk} (A_2)^* \longrightarrow A^! \otimes_{\Bbbk} V^* \longrightarrow A^!$$

is also exact. But this is nothing but the Koszul complex of $A^!$. Therefore, $A^!$ is Koszul. □

Examples.

1. Consider the polynomial ring $\Bbbk[x] = \oplus_{n\geq 0}\Bbbk[x]_n$, where $\Bbbk[x]_n$ is the $\Bbbk$-vector space of polynomials of degree n with coefficients in $\Bbbk$. Consider the shifted module $\Bbbk[x][-1]_n = \Bbbk[x]_{n-1}$. We then have a complex over $\Bbbk$, given by
$$0 \longrightarrow \Bbbk[x][-1] \overset{\cdot x}{\to} \Bbbk[x] \overset{x\mapsto 0}{\to} \Bbbk \longrightarrow 0,$$
where on each component n of the grading of $\Bbbk[x]$, the map
$$\Bbbk[x][-1]_n \overset{\cdot x}{\to} \Bbbk[x]_n$$
$$a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \mapsto a_{n-1}x^n + \ldots + a_1 x^2 + a_0 x$$
denotes multiplication by x and the map
$$\Bbbk[x]_n \longrightarrow \Bbbk$$
$$a_n x^n + \ldots + a_1 x + a_0 \mapsto a_0$$
sends x to 0.

It is easy to see that $\ker(\cdot x) = \oplus \ker(\cdot x)_n = \{0\}$, hence the sequence is exact on the leftmost part.

For the next arrow,
$$\begin{aligned} \operatorname{im}(\cdot x)_n = & \{(a_{n-1}x^{n-1} + \ldots + a_0)\cdot x : a_{n-1}x^{n-1} + \ldots + a_0 \in \Bbbk[x](-1)_n\} \\ = & \{a_{n-1}x^n + \ldots + a_0 x : a_{n-1}, \ldots, a_0 \in \Bbbk\} = \Bbbk[x]_n/\Bbbk. \end{aligned}$$
Thus, $\operatorname{im}(\cdot x) = \Bbbk[x]_+$. Now,
$$\begin{aligned} \ker(x\mapsto 0)_n = & \{a_n x^n + \ldots + a_1 x + a_0 \in \Bbbk[x]_n : a_n 0^n + \ldots + a_1 0 + a_0 = 0\} \\ = & \{a_n x^n + \ldots + a_1 x + a_0 \in \Bbbk[x]_n : a_0 = 0\} \\ = & \{a_n x^n + \ldots + a_1 x \in \Bbbk[x]_n\} = \Bbbk[x]_n/\Bbbk. \end{aligned}$$
Thus, $\ker(x \mapsto 0) = \Bbbk[x]_+$. Therefore the complex is exact at the middle term as well.

Finally,
$$\begin{aligned} \operatorname{im}(x\mapsto 0) = & \{a_n 0^n + \ldots + a_1 0 + a_0 : a_n, \ldots, a_0 \in \Bbbk\} \\ = & \{a_0 : a_0 \in \Bbbk\} = \Bbbk, \end{aligned}$$
therefore the above complex is a resolution of $\Bbbk$ and thus, the algebra $\Bbbk[x]$ is a Koszul algebra.

2. Let $\{x_1, \dots x_n\}$ be a fixed basis of a $\Bbbk$-vector space V and consider the symmetric algebra

$$\mathrm{Sym}(V) = \Bbbk \langle x_1, \dots, x_n \rangle / (x_i x_j - x_j x_i).$$

Recall that the quadratic dual of $\mathrm{Sym}(V)$ is the exterior algebra $\bigwedge(V^*)$. To construct the Koszul complex associated to $\mathrm{Sym}(V)$, we have

$$(\mathrm{Sym}(V)^!_0)^* = (\bigwedge_0(V^*))^* = (V^*)^{\otimes 0} \cong \Bbbk,$$

$$(\mathrm{Sym}(V)^!_1)^* = (\bigwedge_1(V^*))^* = ((V)^*)^* = V,$$

$$(\mathrm{Sym}(V)^!_2)^* = (\bigwedge_2(V^*))^* = (\Bbbk \langle x_1, \dots, x_n \rangle / (x_i x_j + x_j x_i))^*,$$

for $i, j \in \{1, \dots, n\},\ i < j$, that is,

$$(\mathrm{Sym}(V)^!_2)^* = (V)^{\otimes 0} \otimes (x_i x_j - x_j x_i) \otimes V^{\otimes 0} = (x_i x_j - x_j x_i),$$

for $i, j \in \{1, \dots, n\},\ i < j$, and continuing in this manner,

$$(\mathrm{Sym}(V)^!_n)^* = (\sum_{\sigma \in S_n} \mathrm{sgn} \sigma x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}),$$

$$(\mathrm{Sym}(V)^!_{\geq n+1})^* = (0)^* = 0.$$

Therefore, the Koszul complex associated to $\mathrm{Sym}(V)$ is

$$\cdots \longrightarrow \mathrm{Sym}(V) \otimes V = \mathrm{Sym}(V)[-1] \longrightarrow \mathrm{Sym}(V) \otimes \Bbbk \longrightarrow \Bbbk \longrightarrow 0.$$

It is not hard to see that the above complex is exact and therefore the symmetric algebra in n variables is also Koszul.

3. Theorem 3.2.7 asserts that a quadratic algebra is Koszul if and only if its quadratic dual algebra is also Koszul. Since symmetric algebras are Koszul, exterior algebras are Koszul as well.

4. Let p be a prime number. A pro-p-group is called *uniform* if it is finitely generated, torsion-free and powerful. Let G be a uniform pro-p-group and consider the completed group algebra $\mathbb{F}_p[[G]]$ of G with coefficients in $\mathbb{F}_p$. By a Theorem of Lazard, we know that $\mathbb{F}_p[[G]]^!$ can be identified with $\bigwedge H^1(G, \mathbb{F}_p)$, so $\mathbb{F}_p[[G]]$ is Koszul.

Theorem 3.2.8 (Priddy)**.** *Assume that A is a quadratic $\Bbbk$-algebra. If A is Koszul, then its cohomology ring coincides with its quadratic dual, $A^!$.*

Proof. For a proof we refer to [PP05, Chapter 1, Proposition 3.1]. □

Chapter 4

Determining Koszulity

Unfortunately, it is an extremely hard task to show that a quadratic algebra is Koszul, using either the definition of Koszulity or the Koszul complex. Here, we demonstrate some alternative methods to determine whether an algebra is Koszul, such as writing its Hilbert-Poincaré series or finding a PBW basis.

The Hilbert-Poincaré series of a quadratic algebra is always easy to find, but it does not help to show that an algebra is Koszul. On the contrary, we use the Hilbert-Poincaré series to show that a quadratic algebra is not Koszul.

A PBW basis is constructed algorithmically, meaning that if a PBW basis exists, it can then be found in a painless way. In particular, one of the methods used to find whether a basis is a PBW basis for a quadratic algebra is via Bergman's Diamond Lemma. Quadratic algebras that possess a PBW basis are always Koszul. This gives us a nice combinatorial method for verifying Koszulity.

We follow the usual conventions, namely, every vector space V over a fixed field $\Bbbk$ is finite-dimensional, and we further assume that every graded algebra appearing throughout is a quadratic algebra of finite type.

For further details on the topics covered here, we suggest [PP05] and [Pio01] for a treatment of Hilbert-Poincaré series, [LV12] for PBW algebras, and [Ber78] for Bergman's Diamond Lemma.

4.1 Hilbert-Poincaré series

The material of this section is taken from [PP05].

Definition 4.1.1. We define the *Hilbert series* of a quadratic $\mathbb{k}$-algebra A as

$$h_A(z) = \sum_{n \in \mathbb{N}} \dim_{\mathbb{k}} A_n z^n.$$

The *Poincaré series* of A is defined as

$$p_A(u, z) = \sum_{n,m \in \mathbb{N}} \dim_{\mathbb{k}} \operatorname{Ext}_A^{n,m}(\mathbb{k}, \mathbb{k}) u^n z^m.$$

Proposition 4.1.2. *[PP05, Corollary 2.2] For any quadratic algebra A,*

$$h_A(z) p_A(-1, z) = 1.$$

In particular, if A is Koszul, then

$$h_A(z) h_{A^!}(-z) = 1.$$

Proof. Consider a minimal free graded resolution $(P_\bullet, d_\bullet)$ of $\mathbb{k}$. Then

$$\begin{aligned} h_{\operatorname{Ext}^n(\mathbb{k},\mathbb{k})}(z) h_A(z) = &\ \left(\textstyle\sum_{m \in \mathbb{N}} \dim_{\mathbb{k}} \operatorname{Ext}_A^{n,m}(\mathbb{k}, \mathbb{k})\right) \left(\textstyle\sum_{m \in \mathbb{N}} \dim_{\mathbb{k}} A_m\right) z^m \\ = &\ \textstyle\sum_{m \in \mathbb{N}} \left(\sum_{r=0}^m \dim_{\mathbb{k}} \operatorname{Ext}_A^{n,r}(\mathbb{k}, \mathbb{F}) \dim_{\mathbb{k}} A_{m-r}\right) z^m. \end{aligned}$$

Now we fix m and focus on the inner sum. We then have

$$\begin{aligned} &\sum_{r=0}^m \dim_{\mathbb{k}} \operatorname{Ext}_A^{n,r}(\mathbb{k}, \mathbb{k}) \dim_{\mathbb{k}} A_{m-r} \\ &\quad = \textstyle\sum_{r=0}^m \dim_{\mathbb{k}} \operatorname{Hom}_A^r(\mathbb{k} \otimes_A P_n, \mathbb{k}) \dim_{\mathbb{k}} A_{m-r} \\ &\quad = \textstyle\sum_{r=0}^m \dim_{\mathbb{k}} \operatorname{Hom}_A((\mathbb{k} \otimes_A P_n)_r, \mathbb{k}) \dim_{\mathbb{k}} A_{m-r} \\ &\quad = \textstyle\sum_{r=0}^m \dim_{\mathbb{k}} (\mathbb{k} \otimes_A P_n)_r \dim_{\mathbb{k}} A_{m-r} \\ &\quad = \dim_{\mathbb{k}} (A \otimes \mathbb{k} \otimes_A P_n)_m \\ &\quad = \dim_{\mathbb{k}} (P_n)_m. \end{aligned}$$

This implies that

$$\begin{aligned} h_{\operatorname{Ext}^n(\mathbb{k},\mathbb{k})}(z) h_A(z) = &\ \textstyle\sum_{m \in \mathbb{N}} \left(\sum_{r=0}^m \dim_{\mathbb{k}} \operatorname{Ext}_A^{n,r}(\mathbb{k}, \mathbb{k}) \dim_{\mathbb{k}} A_{m-r}\right) z^m \\ = &\ \textstyle\sum_{m \in \mathbb{N}} \dim_{\mathbb{k}} (P_n)_m z^m \\ = &\ h_{P_n}(z). \end{aligned}$$

Recall that the *Euler characteristic* of $(P_\bullet)_m$ is defined as

$$\chi_{\Bbbk}(P_\bullet)_m = \sum_{n\in\mathbb{N}}(-1)^n \dim_{\Bbbk}(P_n)_m.$$

Therefore,

$$\begin{array}{rcl}\displaystyle\sum_{m\in\mathbb{N}}\chi_{\Bbbk}(P_\bullet)_m z^m & = & \sum_{m\in\mathbb{N}}\left(\sum_{n\in\mathbb{N}}(-1)^n \dim_{\Bbbk}(P_n)_m\right) z^m \\ & = & \sum_{m\in\mathbb{N}}\left(\sum_{n\in\mathbb{N}}(-1)^n \left(\sum_{r=0}^m \dim_{\Bbbk}\operatorname{Ext}_A^{n,r}(\Bbbk,\Bbbk)\dim A_{m-r}\right)\right) z^m \\ & = & \sum_{m\in\mathbb{N}}\left(\sum_{r=0}^m \left(\sum_{n\in\mathbb{N}}(-1)^n \dim_{\Bbbk}\operatorname{Ext}_A^{n,r}(\Bbbk,\Bbbk)\dim_{\Bbbk} A_{m-r}\right)\right) z^m \\ & = & \left(\sum_{m\in\mathbb{N}}\sum_{n\in\mathbb{N}}(-1)^n \dim_{\Bbbk}\operatorname{Ext}_A^{n,m}(\Bbbk,\Bbbk) z^m\right)\left(\sum_{m\in\mathbb{N}}\dim_{\Bbbk} A_m z^m\right) \\ & = & p_A(-1,z)_m h_A(z).\end{array}$$

However, an equivalent way to formulate the Euler characteristic is

$$\chi_{\Bbbk}(P_\bullet)_m = \sum_{n\in\mathbb{N}}(-1)^n \dim_{\Bbbk} H_n(P_\bullet).$$

Since the homology of $\Bbbk$ is concentrated in degree 0, we obtain

$$\chi_{\Bbbk}(P_\bullet)_m = \dim_{\Bbbk} H_0(P_\bullet)_0 = \dim_{\Bbbk}\Bbbk_m = \begin{cases}1 & \text{if } m=0\\ 0 & \text{if } m\neq 0\end{cases}.$$

Therefore,

$$\sum_{m\in\mathbb{N}}\chi_{\Bbbk}(P_\bullet)_m z^m = 1.$$

We thus conclude that

$$p_A(-1,z)h_A(z) = 1.$$

Assume now that A is a Koszul algebra. Then we know by Theorem 3.2.8 that

$$H^\bullet(A) = \operatorname{Ext}_A^\bullet(\Bbbk,\Bbbk) \cong A^!.$$

As a result, we have

$$\begin{array}{rcl}p_A(u,z) & = & \sum_{n,m\in\mathbb{N}}\dim_{\Bbbk}\operatorname{Ext}_A^{n,m}(\Bbbk,\Bbbk)u^n z^m \\ & = & \sum_{n\in\mathbb{N}}\dim_{\Bbbk}\operatorname{Ext}_A^{n}(\Bbbk,\Bbbk)u^n z^n \\ & = & \sum_{n\in\mathbb{N}}\dim_{\Bbbk}(A^!)_n (uz)^n \\ & = & h_{A^!}(uz).\end{array}$$

Thus, $p_A(-1,z) = h_{A^!}(-z)$. And since $p_A(-1,z)h_A(z) = 1$, we get the desired conclusion. □

For many years it was believed that if the equality $h_A(z)h_{A^!}(-z) = 1$ of Proposition 4.1.2 holds, then the algebras A and $A^!$ are Koszul. This was open until J.-E. Roos (see [Roo95]) and L. Positselski (see [Pos95]) independently found the first counterexamples, and later D. Piontkovskii (see [Pio01]) gave an argument outlining why we cannot in general conclude whether A is a Koszul algebra by looking at the Hilbert series of A and $A^!$.

However, when the Hilbert series of a quadratic algebra is of a certain form, the equality $h_A(z)h_{A^!}(-z) = 1$ does, in fact, imply that A is Koszul. For a real power series $f(z) \in \mathbb{R}[[z]]$, denote by $|f(z)|$ the series obtained from $f(z)$ by deleting all the terms after the first negative coefficient. If $f(z), g(z) \in \mathbb{R}[[z]]$ are real power series, we then write $f(z) \geq g(z)$ to mean that the coefficients of f are greater that or equal to the coefficients of g in the respective terms.

Proposition 4.1.3. *[PP05, Proposition 2.3] Assume that A is a quadratic algebra with d generators and r relations. If*

$$h_A(z) = \frac{1}{1 - dz + rz^2},$$

then A is Koszul.

Proof. Recall that $A[d]_k = A_{d+k}$ and consider the graded exact sequence

$$R \otimes A[-2] \longrightarrow V \otimes A[-1] \longrightarrow A \longrightarrow \Bbbk \longrightarrow 0.$$

Note that, by definition, this sequence is linear. The Hilbert series associated with $R \otimes A[-2]$ is $rz^2 h_A(z)$, with $V \otimes A[-1]$ is $dzh_A(z)$, with A is $h_A(z)$ and with $\Bbbk$ is 1. Translating the above in these terms,

$$rz^2 h_A(z) - dzh_A(z) + rz^2 h_A(z) - 1 \geq 0,$$

or, equivalently,

$$h_A(z) \geq \left| \frac{1}{1 - dz + rz^2} \right|.$$

Now, assume that $h_A(z) = \frac{1}{1-dz+rz^2}$. This means that the above sequence is also left exact, so we get a free resolution of $\Bbbk$:

$$0 \longrightarrow R \otimes A[-2] \longrightarrow V \otimes A[-1] \longrightarrow A \longrightarrow \Bbbk \longrightarrow 0.$$

Then by definition, the algebra A is Koszul. □

Corollary 4.1.4. *[PP05, Corollary 2.4] Assume for the quadratic algebra A that $A_3 = 0$ or $A^!_3 = 0$ and assume that $h_A(z)h_{A^!}(-z) = 1$. Then A is Koszul.*

Proof. Assume without loss of generality that $A_3 = 0$. Then the exact sequence

$$0 \longrightarrow R \otimes A[-2] \longrightarrow V \otimes A[-1] \longrightarrow A \longrightarrow \Bbbk \longrightarrow 0$$

is a linear resolution of $\Bbbk$, and so A is Koszul. □

Examples.

1. Let $\mathbb{F}$ be a totally imaginary field. Then $\operatorname{cd} G_{\mathbb{F}} = 2$, and $H^{\geq 3}(\mathbb{F}, \mathbb{F}_p) = 0$. Therefore, by Corollary 4.1.4, $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is Koszul.

2. Assume that G is Demushkin group with $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = d < \infty$. The Hilbert series associated to $A = H^\bullet(G, \mathbb{F}_p)$ is

$$\begin{aligned} h_A(z) = & \textstyle\sum_{n=0}^{2}(-1)^n \dim_{\mathbb{F}_p} H^n(G, \mathbb{F}_p) z^n \\ = & \dim_{\mathbb{F}_p} H^0(G, \mathbb{F}_p) - \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) z + \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) z^2 \\ = & 1 - dz + z^2. \end{aligned}$$

   Therefore, from the relation $h_A(z)p_A(-1, z) = 1$, we get that

$$p_A(-1, z) = \frac{1}{1 - dz + z^2}.$$

   Hence $H^\bullet(G, \mathbb{F}_p)^!$ is Koszul. Since A and $A^!$ are simultaneously Koszul, we conclude that $h^\bullet(G, \mathbb{F}_p)$ is Koszul.

3. In fact, the $\operatorname{mod} p$-cohomology ring $H^\bullet(G, \mathbb{F}_p)$ of any profinite group G of cohomological dimension $\operatorname{cd} G \leq 2$ is Koszul, since for such groups the assumption $H^3(G, \mathbb{F}_p) = 0$ is trivially satisfied by Corollary 4.1.4.

4.2 PBW algebras and Koszulity

Poincaré-Birkhoff-Witt bases, hereafter abbreviated as PBW bases, are the noncommutative analog of Gröbner bases and are of significant importance in studying Koszulity. The importance in the existence of such bases arises due to the fact that a quadratic algebra $A = \{V, R\}$ whose space of topological generators V admits a PBW basis is a Koszul algebra.

Let $\{x_1, \ldots, x_d\}$ be a fixed basis of a $\Bbbk$-vector space V and write $V = V_1 \oplus \cdots \oplus V_d$, where $V_i = \operatorname{span}\{x_i\}$, $i = 1, \ldots, d$. Then for each $n \in \mathbb{N}$, we can identify $V^{\otimes n}$ with

$$V = \sum_{i_1, \ldots, i_n \in \{1, \ldots, d\}} V_{i_1} \otimes \cdots \otimes V_{i_n}.$$

For a multiindex $\alpha = (i_1, \ldots, i_n)$, where $i_1, \ldots, i_n \in \{1, \ldots, d\}$, we denote by x_α the monomial $x_{i_1} x_{i_2} \cdots x_{i_n}$ and by V_α the space $V_{i_1} \otimes \cdots \otimes V_{i_n} \subseteq V^{\otimes n}$. Under the convention that $\alpha_\emptyset = 1$, we build a set of indices $\mathcal{I} = \coprod_{n \in \mathbb{N}} \{1, \ldots, d\}^n$, that identifies every monomial in $\mathbb{T}(V)$.

We put a degree-lexicographic order on $\mathcal{I}$. For two multiindices $\alpha = (i_1, \ldots, i_n)$ and $\beta = (j_1, \ldots, j_m)$, we set

$$\alpha < \beta \text{ if and only if } \begin{cases} n < m & \text{or} \\ n = m & \text{and there exists } k : i_{<k} = j_{<k} \text{ and } i_k < j_k. \end{cases}$$

A PBW basis is constructed algorithmically and the first step towards that is the following

Lemma 4.2.1. *Let U be a vector space that admits an ordered basis $\{u_\alpha : \alpha \in \mathcal{I}_U\}$ and let W be a subspace of U. Consider the subset $\mathcal{I}_W \subset \mathcal{I}_U$ consisting of all $\alpha \in \mathcal{I}_U$, such that u_α cannot be presented as a linear combination of u_β with $\beta < \alpha \bmod W$. Then the images of the elements u_α with $\alpha \in \mathcal{I}_W$ form a basis of U/W. Moreover, the subset $\mathcal{I}_W$ is uniquely characterized by the property that there is a basis of W of the form*

$$w_\beta = u_\beta - \sum_{\alpha < \beta} c_{\beta\alpha} u_\alpha, \text{ where } \beta \in \mathcal{I}_U \backslash \mathcal{I}_W.$$

Finally, there exists a unique basis of W of this form with the additional property that for all $\alpha \notin \mathcal{I}_W$, $c_{\beta\alpha} = 0$.

Proof. See [PP05, Chapter 4, Lemma 1.1]. □

We will use the preceding Lemma to break down the relator set of a quadratic algebra $A = \{V, R\}$. Consider the space $V^{\otimes 2}$; since V is equipped with an ordered basis $\{x_1, \ldots, x_d\}$, we get that $V^{\otimes 2}$ admits a basis of monomials $x_{i_1} x_{i_2}$ where $(i_1, i_2) \in \{1, \ldots, d\}^2$. Applying Lemma 4.2.1 with $U = V^{\otimes 2}$ and $W = R \subset V^{\otimes 2}$, we obtain a set of pairs of indices $S \subset \{1, \ldots, d\}^2$, that consists of all pairs (n, m) for which the class $x_n x_m$ does not belong to the span of the classes $x_i x_j$ for $(i, j) < (n, m)$. Therefore, by the Lemma above, if $r \in R$ is a relator of A which can be written in the form $x_n x_m - \sum_{(i,j)<(n,m)} c_{nm}^{i,j} x_i x_j$, with $(i, j) \in S$, then we can express r as

$$x_n x_m = \sum_{(i,j)<(n,m),(i,j)\in S} c_{n,m}^{i,j} x_i x_j, \text{ where } (n, m) \in \{1, \dots, d\}^2 \backslash S.$$

Inductively, we consider similar sets of indices to S, constructed in the following way. Set $S^{(0)} = \emptyset$ and $S^{(1)} = \{1, \dots, d\}$. For $n \geq 2$, we construct the set of multiindices

$$S^{(n)} = \{(i_1, \dots, i_n) : (i_k, i_{k+1}) \in S, k = 1, \dots, n-1\}.$$

Now, for each $n \in \mathbb{N}$, we consider the sets of monomials $\{x_{i_1} \cdots x_{i_n} : (i_1, \dots, i_n) \in S^{(n)}\}$. Since each of these monomials cannot be written as a linear combination of lexicographically smaller monomials, it is easy to see that for each $n \in \mathbb{N}$, the collection $\{x_{i_1} \cdots x_{i_n} : (i_1, \dots, i_n) \in S^{(n)}\}$ linearly spans A_n as a $\Bbbk$-vector space. Indeed, consider the monomial $x_{i_1} \cdots x_{i_n}$ and assume that $(i_k, i_{k+1}) \notin S = S^{(2)}$ for some $k \in \{1, \dots, n-1\}$. Then $x_{i_1} \cdots x_{i_n}$ can be expressed as a linear combination of monomials of smaller degree modulo (R_n), where

$$R_n = \sum_k \mathbb{T}^n(V) \cap V^{\otimes k-1} \otimes R \otimes V^{\otimes n-k-1}.$$

We now consider the projection

$$\mathrm{pr} : V^{\otimes 2} \longrightarrow \left\langle x_n x_m : (n, m) \in S = S^{(2)} \right\rangle \oplus R \subseteq V^{\otimes 2},$$

defined by

$$x_n x_m \mapsto \mathrm{pr}(x_n x_m) = \begin{cases} x_n x_m & \text{if } (n, m) \in S \\ \sum_{S \ni (i,j)<(n,m)} c_{n,m}^{i,j} x_i x_j & \text{if } (n, m) \in \{1, \dots, d\}^2 \backslash S \end{cases}.$$

In particular, modulo (R_2), the projection sends an element in $\mathbb{T}_2(V)$ to an element of $\left\langle x_{i_1} x_{i_2}, (i_1, i_2) \in S^{(2)} \right\rangle$, and thus maps $\mathbb{T}_2(V)$ to $\left\langle x_{i_1} x_{i_2} : (i_1, i_2) \in S^{(2)} \right\rangle$.

In the same fashion we can extend these projections to indices of arbitrary length n. To do so, for each $k \in \{1, \dots, n-1\}$, consider the projections

$$\mathrm{pr}_{k,k+1} : \mathbb{T}_n(V) \longrightarrow \mathbb{T}_n(V)$$

defined by

$$\mathrm{pr}_{k,k+1} = \mathrm{id}^{\otimes k-1} \otimes \mathrm{pr} \otimes \mathrm{id}^{\otimes n-k-1}.$$

In other words, we define by $\mathrm{pr}_{k,k+1}$ the map that projects the element $x_{i_k}x_{i_{k+1}}$ of $x_{i_1}\cdots x_{i_n} \in \mathbb{T}_n(V)$, while it fixes the rest of the monomial. Notice that on the $(k, k+1)$-pair of indices, the projection is defined as the one introduced earlier for elements of $\mathbb{T}_2(V)$. Furthermore, applying iterated projections to the monomial $x_{i_1}\cdots x_{i_n}$, we obtain a more refined word, as we replace the product $x_k x_{k+1}$ with a sum of simpler equivalent expressions from R.

It is not hard to see that any element $x \in \mathbb{T}_n(V)$ satisfies

$$x \equiv \cdots \mathrm{pr}_{1,2}\mathrm{pr}_{2,3}\mathrm{pr}_{3,4}\cdots \mathrm{pr}_{n-1,n}\mathrm{pr}_{1,2}\mathrm{pr}_{2,3}\cdots \mathrm{pr}_{n-1,n} x \bmod (R).$$

This means that after we apply an (arbitrary and possibly infinite) amount of projections to $x \in \mathbb{T}_n(V)$, this monomial breaks down to a part inside the set spanned by $\left\langle x_{i_1}\cdots x_{i_n} : (i_1, \ldots, i_n) \in S^{(n)}\right\rangle$ and a part absorbed by the relations on degree n. This product is well defined, because the projections decrease the order. Moreover, we can also consider an infinite composition

$$\cdots \mathrm{pr}^{i_3,i_3+1}\mathrm{pr}^{i_2,i_2+1}\mathrm{pr}^{i_1,i_1+1}$$

associated to any sequence $(i_1, i_2, i_3, \ldots)$ that contain every index $1, \ldots, n-1$ infinitely many times. So, for any degree n, the set of monomials $\{x_{i_1}\cdots x_{i_n} : (i_1, \ldots, i_n) \in S^{(n)}\}$ span $\mathbb{T}^n(V)$ modulo R_n, and so, the set of monomials $\{x_{i_1}\cdots x_{i_n} : (i_1, \ldots, i_n) \in \cup_{n\geq 0} S^{(n)}\}$ linearly span A.

Definition 4.2.2. Let $\{x_1, \ldots, x_d\}$ be a fixed basis for V. The elements $x_1, \ldots, x_d$ are called *PBW-generators* of the quadratic algebra $A = \{V, R\}$ if the monomials $\{x_{i_1}\cdots x_{i_n} : (i_1, \ldots, i_n) \in \cup_{n\geq 0} S^{(n)}\}$ form a basis of A. In this case, the basis $\{x_{i_1}\cdots x_{i_n} : (i_1, \ldots, i_n) \in \cup_{n\geq 0} S^{(n)}\}$ is called a *PBW-basis of* A. Finally, a quadratic algebra A that admits a PBW-basis is called a *PBW algebra.*

We have already seen that the set $\{x_{i_1}\cdots x_{i_n} : (i_1 \cdots i_n) \in \cup_{n\geq 0} S^{(n)}\}$ linearly spans the algebra A, so in order to determine whether A is PBW, we only need to check whether they form a basis.

Note that an algebra A admits a PBW basis if and only if all above products of projections are equal to one another.

The next result, known as Diamond Lemma, asserts that it is enough to check linear independence up to degree 3.

Theorem 4.2.3 (Diamond Lemma). *Let A be a quadratic algebra and consider the set of cubic monomials $\{x_{i_1}x_{i_2}x_{i_3} : (i_1, i_2, i_3) \in S^{(3)}\}$. If these monomials are linearly independent in A_3, then any set $\{x_{i_1} \cdots x_{i_n} : (i_1, \ldots, i_n) \in S^{(n)}\}$ consists of linearly independent monomials for any degree n. Therefore, in this case, the elements $x_1, \ldots, x_d$ are PBW generators of A.*

Equivalently, the elements $\{x_1, \ldots, x_d\}$ are PBW generators of A if and only if

$$\cdots \mathrm{pr}_{1,2}\mathrm{pr}_{2,3}\mathrm{pr}_{1,2} = \cdots \mathrm{pr}_{2,3}\mathrm{pr}_{1,2}\mathrm{pr}_{2,3}.$$

Thus, constructing a PBW basis for an algebra gives us a hassle free way to determine Koszulity, without having to compute the homology groups of the associated Koszul complex.

Proof. Consider a sequence $(i_1, i_2, i_3, \ldots)$ and denote by π the corresponding product of projections

$$\pi = \cdots \mathrm{pr}_{i_3,i_3+1}\mathrm{pr}_{i_2,i_2+1}\mathrm{pr}_{i_1,i_1+1} = \pi'\mathrm{pr}_{i_1,i_1+1}.$$

To show that any two products are equal to each other, it is enough to show that for any j,

$$\pi\mathrm{pr}_{j,j+1} = \pi.$$

We shall do this by induction on the length of multiindex $(i_1, \ldots, i_n)$. For a monomial of length 0 there is nothing to prove and for a monomial of length 1, x_i, $i \in \{1, \ldots, d\}$, it is true that for any j, $\pi\mathrm{pr}_{j,j+1}x_i = \pi x_i$.

Now, assume that for all multiindices $(i_1, \ldots, i_k)$ with $k < n$, the statement holds. If $\mathrm{pr}_{j,j+1}x_{i_1} \cdots x_{i_n} = x_{i_1} \cdots x_{i_n}$, then there is nothing to prove again, so we can assume without loss of generality that $\mathrm{pr}_{j,j+1}x_{i_1} \cdots x_{i_n} \in \mathbb{T}_n(V)_{<(i_1,\ldots,i_n)} := \langle x_{i_1} \cdots x_{i_k} : (i_1, \ldots, i_k) < (i_1, \ldots, i_n)\rangle$. Then by the induction hypothesis

$$\mathrm{pr}_{i_1,i_1+1}\mathrm{pr}_{j,j+1}x_{i_1} \cdots x_{i_n} = \mathrm{pr}_{j,j+1}x_{i_1} \cdots x_{i_n}.$$

Now, we have that

$$\begin{aligned} \pi\mathrm{pr}_{j,j+1}x_{i_1} \cdots x_{i_n} = & \quad \pi'\mathrm{pr}_{i_1,i_1+1}\mathrm{pr}_{j,j+1}x_{i_1} \cdots x_{i_n} \\ = & \qquad \pi'\mathrm{pr}_{j,j+1}x_{i_1} \cdots x_{i_n}, \end{aligned}$$

by the induction hypothesis. So, we can assume that $\mathrm{pr}_{i_1,i_1+1}x_{i_1} \cdots x_{i_n} \in \mathbb{T}_n(V)_{<(i_1,\ldots,i_n)}$. Otherwise, $\mathrm{pr}_{i_1,i_1+1}x_{i_1} \cdots x_{i_n} = x_{i_1} \cdots x_{i_n}$ and we deduce that

$$\pi x_{i_1} \cdots x_{i_n} = \pi' x_{i_1} \cdots x_{i_n}.$$

So, assume that $\mathrm{pr}_{i_1,i_1+1}x_{i_1}\cdots x_{i_n} \in \mathbb{T}_n(V)_{<(i_1,\ldots,i_n)}$. In the same way we decomposed π to $\pi'\mathrm{pr}_{i_1,i_1+1}$, we can continue decomposing π' to $\pi''\mathrm{pr}_{i_2,i_2+1}$ and so on, until we obtain an index i_s, such that $i_s = j$.

By induction hypothesis, we obtain

$$\cdots \mathrm{pr}_{j,j+1}\mathrm{pr}_{i_1,i_1+1}\mathrm{pr}_{j,j+1}x_{i_1}\cdots x_{i_n} = \cdots \mathrm{pr}_{i_1,i_1+1}\mathrm{pr}_{j,j+1}\mathrm{pr}_{i_1,i_1+1}x_{i_1}\cdots x_{i_n}.$$

Applying π on both sides, the left hand side becomes

$$\begin{aligned}\pi\left(\cdots \mathrm{pr}_{j,j+1}, \mathrm{pr}_{i_1,i_1+1}\mathrm{pr}_{j,j+1}x_{i_1}\cdots x_{i_n}\right)&\\ &= \left(\pi\cdots \mathrm{pr}_{j,j+1}\mathrm{pr}_{i_1,i_1+1}\right)\mathrm{pr}_{j,j+1}x_{i_1}\cdots x_{i_n}\\ &= \mathrm{pr}_{j,j+1}x_{i_1}\cdots x_{i_n}\end{aligned}$$

by induction. Similarly for the right hand side,

$$\begin{aligned}\pi\left(\cdots \mathrm{pr}_{i_1,i_1+1}\mathrm{pr}_{j,j+1}\mathrm{pr}_{i_1,i_1+1}x_{i_1}\cdots x_{i_n}\right)&\\ &= \left(\pi\cdots \mathrm{pr}_{i_1,i_1+1}\mathrm{pr}_{j,j+1}\right)\mathrm{pr}_{i_1,i_1+1}x_{i_1}\cdots x_{i_n}\\ &= \pi\mathrm{pr}_{i_1,i_1+1}x_{i_1}\cdots x_{i_n}.\end{aligned}$$

Combining these, gives us the following

$$\pi\mathrm{pr}_{j,j+1}x_{i_1}\cdots x_{i_n} = \pi\mathrm{pr}_{i_1,i_1+1}x_{i_1}\cdots x_{i_n}.$$

However, by induction, $\pi\mathrm{pr}_{i_1,i_1+1}x_{i_1}\cdots x_{i_n} = \pi x_{i_1}\cdots x_{i_n}$. Therefore, the preceding equality becomes

$$\pi\mathrm{pr}_{j,j+1}x_{i_1}\cdots x_{i_n} = \pi x_{i_1}\cdots x_{i_n},$$

as we wanted. We have thus shown that if the cubic monomials $x_{i_1}x_{i_2}x_{i_3}$ with $(i_1, i_2, i_3) \in S^{(3)}$ are all linearly independent, then so are the monomials $x_{i_1}\cdots x_{i_n}$ of any degree n, hence the algebra A is a PBW-algebra. □

For a quadratic $\mathbb{k}$-algebra A, admitting a PBW basis is stronger than being Koszul. This is demonstrated in the following

Theorem 4.2.4 (Priddy)**.** *A PBW algebra is Koszul.*

Proof. See [PP05, Chapter 4, Theorem 3.1] . □

Examples.

1. Consider the quadratic algebra $A = \{V, R\}$, where V admits a basis $\{x_1, x_2\}$ of generators and $R = \langle x_1^2 - x_1x_2 \rangle$. Considering the degree-lexicographic order defined in the beginning of the section

$$1 < 2 < (1,1) < (1,2) < (2,1) < (2,2) < (1,1,1) < \cdots .$$

   The relation $x_1^2 = x_1x_2$ implies that

$$\begin{array}{rc} S^{(1)} = & \{1,2\} \\ S^{(2)} = & \{(1,1),(1,2),(2,1),(2,2)\}\backslash\{(1,2)\} \\ = & \{(1,1),(2,1),(2,2)\} \\ S^{(3)} = & \{(1,1,1),(1,1,2),\ldots,(2,2,1),(2,2,2)\}\backslash\{(-,1,2),(1,2,-)\} \\ = & \{(1,1,1),(2,1,1),(2,2,1),(2,2,2)\}. \end{array}$$

   It is an easy task to check that the monomials x_1^3, $x_2x_1^2$, $x_2^2x_1$ and x_2^3 are linearly independent in A. Therefore, by the Diamond Lemma Theorem 4.2.3, we deduce that for any $n \geq 4$, any set of monomials

$$\{x_{i_1}x_{i_2}\cdots x_{i_n} : (i_1,\ldots,i_n) \in S^{(n)}\}$$

   is also linearly independent, where

$$S^{(n)} = \{(1,1,\ldots,1),(2,1,\ldots,1,1),\ldots,(2,2,\ldots,2,1),(2,2,\ldots,2)\}.$$

   So, the algebra $A = \mathbb{T}(V)/(x_1^2 - x_1x_2)$ is a PBW and hence a Koszul algebra.

2. Assume that $A = \{V_A, R_A\}$ and $B = \{V_B, R_B\}$ are PBW algebras. Recall that the free product $A \sqcup B$ of A and B is defined as the quadratic algebra

$$A \sqcup B = \mathbb{T}(V_A \oplus V_B)/(R),$$

   where $R = R_A \oplus R_B$. Then a set of PBW generators of $A \sqcup B$ is simply the union of the PBW generators of A and of B. Therefore, $A \sqcup B$ is a PBW algebra. Similarly, the direct sum $A \sqcap B$, symmetric tensor product $A \otimes^1 B$ and skew symmetric tensor product $A \otimes^{-1} B$ of two PBW algebras is a PBW algebra.

4.3 Bergman's Diamond Lemma

To utilize PBW bases more efficiently, we have to adopt a way to check whether all monomials appearing in the span of each graded component of a given algebra are linearly independent or not. For this, it is desirable to have the ability to distinguish between monomials that certainly do not arise as a consequence of operations on other monomials, and monomials that are consequence of other ones. In this direction G.M. Bergman created another Diamond Lemma, which we refer to as Bergman's Diamond Lemma, that mimics the idea of the previous one, stated in Theorem 4.2.3, although this time it only contains terms of "ambiguous" nature.

Assume that the tensor algebra $\mathbb{T}(V)$ admits a weight associated with an order $\leq$. Then every element $x \in \mathbb{T}(V)$ can be written as

$$x = x_{i_{\text{lead}}} - \sum_{j<i_{\text{lead}}} x_j .$$

Or, in other words, $x_{i_{\text{lead}}}$ puts together all the summands of x of maximal weight and separates them from all the rest summands.

Definition 4.3.1. For an element $x \in \mathbb{T}(V)$ which can be written in the form $x = x_{i_{\text{lead}}} - \sum_{j<i_{\text{lead}}} x_j$, the term $x_{i_{\text{lead}}}$ is called the *leading term of* x and the term $\sum_{j<i_{\text{lead}}} x_j$ is called the *lower term.*

We can apply the above decomposition to the space of relations R for a quadratic algebra $A = \{V, R\}$. We can choose a basis $\mathcal{B}$ of R, such that:

(i) The coefficient of the leading term of each $r \in \mathcal{B}$ is 1; and

(ii) The leading term of each $r \in \mathcal{B}$ does not appear in any other element of $\mathcal{B}$; this means that it appears neither a leading nor as a lower term.

(Note that in order to achieve a decomposition described in (ii), we perform the equivalent of the Gram-Schmidt process in linear algebra.)

Definition 4.3.2. A basis $\mathcal{B}$ of R given as above is called a *normalized basis.* If $\mathcal{B}$ is a normalized basis, we denote by R_{lead} the linear span of the leading terms of $\mathcal{B}$.

Firstly, we put a filtration on $\mathbb{T}(V)$. Recall that $\mathcal{I} = \coprod_{n\in\mathbb{N}}\{1,\dots,d\}^n$ identifies every monomial on $\mathbb{T}(V)$ and there is a degree-lexicographic order on $\mathcal{I}$. Since $\mathcal{I}$ is countable, there exists a bijective map

$$f : \mathcal{I} \longrightarrow \mathbb{N}$$

$$\alpha \mapsto f(\alpha).$$

Therefore, the degree-lexicographic order on $\mathcal{I}$ is mapped bijectively to the (natural) order on $\mathbb{N}$. Thus, for two multiindices α, β, we can say that $\alpha < \beta$ if and only if $f(\alpha) < f(\beta)$. This induces a filtration on $\mathbb{T}(V)$ given by

$$F_n\mathbb{T}(V) = \oplus_{\alpha\in\mathcal{I}:\alpha\leq f^{-1}(n)} V_\alpha,$$

which is increasing and exhaustive. Now, set

$$\mathrm{gr}_n\mathbb{T}(V) = F_n\mathbb{T}(V)/F_{n-1}\mathbb{T}(V).$$

We obtain a graded algebra

$$\mathrm{gr}_\bullet\mathbb{T}(V) = \oplus_{n\in\mathbb{N}}\mathrm{gr}_n\mathbb{T}(V).$$

The second grading of $\mathrm{gr}_\bullet\mathbb{T}(V)$ is the refinement, associated with the new filtration, which we call the *weight*. This is naturally inherited by a quadratic algebra $A = \{V, R\}$ via the natural projection $\mathbb{T}(V) \longrightarrow A$, allowing us to obtain a new graded object, $\mathrm{gr}_\bullet A$, which comes equipped with two gradings, the degree and the weight.

Let $R \ni x = 0$ be a defining relation in A. Decomposing x into the leading and lower terms, the relation in A assumes the form $x_{\text{lead}} = x_{\text{lower}}$. However, in $\mathrm{gr}_\bullet A$, this relation is reduced to $x_{\text{lead}} = 0$, because the lower terms have been killed by the filtration. Therefore, $\mathrm{gr}_\bullet A$ has a presentation

$$\mathrm{gr}_\bullet A = \langle V : R_{\text{lead}} \rangle\,,$$

which induces a commutative diagram

$$\begin{tikzcd}
\mathbb{T}(V) \arrow[d, two heads] \arrow[dr, two heads] & \\
\mathbb{T}(V)/R_{\text{lead}} \arrow[r, two heads, "\rho"'] & \mathrm{gr}_\bullet A,
\end{tikzcd}$$

where the maps from $\mathbb{T}(V)$ to $\mathbb{T}(V)/R_{\text{lead}}$ and $\mathrm{gr}_\bullet A$ are canonical projections.

The map ρ is an isomorphism in degrees $0, 1$ and 2, without this necessarily meaning that ρ is in general an isomorphism of graded algebras. Indeed, the algebra A might have an element $a \in A_{\leq 3}$ that could be written in various ways replacing leading terms with their associated sums of lower terms. For instance, assume that an element $a \in A$ can be written as $a_1 = 0$ and as $a_2 = 0$ with $a_1 \neq a_2$ and assume without loss of generality that the weight of a_1 is less than the weight of a_2. Assume further that both a_1 and a_2 cannot be decomposed any further in terms of lower terms. Then in A, we get the relation $a_1 = a_2$, as a consequence of the quadratic relations. However, the weight of a_1 being less than the weight of a_2 yields that $[a_2] = 0$ on the level of $\mathrm{gr}_\bullet A$, while this is not a quadratic relation, nor is a consequence of such. Before we examine the situation in which ρ is an isomorphism, we need to expand our vocabulary and introduce some new notions.

Definition 4.3.3. Assume that $A = \mathbb{T}(V)/(R)$ is a graded (not necessarily quadratic) algebra with homogeneous relator space. We say that a relator $r \in R$ is a *consequence* of the relators r_j for some j if r belongs to the two-sided ideal (r_j). A relator $r \in R$ is called an *essential relator in degree n* if $r \in A_n$ and the relation $r = 0$ is not a consequence of the relations in degrees smaller than n.

Roughly speaking, a relator that is not an essential relator has no actual impact to the algebra, as it is derived from relators in smaller degrees. In other words, we only need to take into account the essential relators, and disregard all the relators that arrive as consequences.

Example.
Let $\{x_1, x_2, x_3, x_4\}$ be a basis for the vector space V and consider the symmetric algebra $\mathrm{Sym}(V) = \mathbb{T}(V)/(x_jx_i - x_ix_j : \ 1 \leq i < j \leq 4)$. Then focusing on the generating relations, we can rewrite $\mathrm{Sym}(V)$ as

$$\mathrm{Sym}(V) = \langle x_1, x_2, x_3, x_4 : r_{21}, r_{31}, r_{41}, r_{32}, r_{42}, r_{43} \rangle ,$$

where $r_{ji} = x_jx_i - x_ix_j$, $1 \leq i < j \leq 4$.

Let $r \in R$ be a relator of $A = \mathbb{T}(V)/(R)$. Then it decomposes into leading and lower terms, and we see that a relation in A can be derived by substituting leading terms for sums of lower terms. Ideally, we would like to reduce every relation in A as far as possible and in order to do so, it is enough to reduce all elements of a fixed set S of generators of R. So, for each element $r \in S$, we denote the substitution rule by $r_{\text{lead}} \mapsto r_{\text{lower}}$. This mapping can be represented by an oriented graph $\mathcal{G}$ whose vertices are the elements of $\mathbb{T}(V)$ and an oriented edge starts from a and ends in b if b can be obtained from a by application of a single substitution $r_{\text{lead}} \mapsto r_{\text{lower}}$. Adjacent edges with coherent orientation are called *paths* of $\mathcal{G}$ and adjacent edges with omitted orientation are called *quasipaths*. We call the number of edges that constitute a path (quasipath) the *length of the path (quasipath)*. For instance, the mapping $a \longrightarrow b \longrightarrow c \longrightarrow d \longrightarrow e$ is a path of length 4 and $a \longrightarrow b \longleftarrow c \longleftarrow d \longrightarrow e \longrightarrow f$ is a quasipath of length 5.

In this fashion, we can obtain a descent of iterated substitutions from an element a into an element b, represented by an edge $a \longrightarrow b$ on $\mathcal{G}$. Since $\mathbb{T}(V)$ comes equipped with an order, any path has necessarily finite length. Furthermore, a vertex has no succeeding edges if and only if its edge does not contain any leading monomials anymore. Finally, since every element derived by substitution is an element consisting of more lower terms, the graph $\mathcal{G}$ satisfies the descending chain condition for paths. If a vertex has no succeeding edges, that is, if the vertex contains no leading monomials, then the corresponding element of $\mathbb{T}(V)$ is called a *R-reduced term*. In this case, if $a \longrightarrow b$ is a path and b is an R-reduced term, then we call b an *R-reduced form of a*.

Example.
Considering again the symmetric algebra

$$\mathrm{Sym}(V) = \langle x_1, x_2, x_3, x_4 : r_{21}, r_{31}, r_{41}, r_{32}, r_{42}, r_{43} \rangle$$

of the previous example, we obtain a graph

$$\begin{tikzcd}
 & x_4x_3x_2x_1 \arrow[dl, "x_4x_3r_{21}"'] \arrow[dr, "r_{43}x_2x_1"] & & . \\
x_4x_3x_1x_2 \arrow[d, "x_4r_{31}x_2"'] & & x_3x_4x_2x_1 \arrow[d, "x_3r_{42}x_1"] & \\
x_4x_1x_3x_2 \arrow[d, "r_{41}x_3x_2"'] & & x_3x_2x_4x_1 \arrow[d, "r_{32}x_4x_1"] & \\
x_1x_4x_3x_2 \arrow[d, "x_1x_4r_{32}"'] & & x_2x_3x_4x_1 \arrow[d, "x_2x_3r_{41}"] & \\
x_1x_4x_2x_3 \arrow[d, "x_1r_{42}x_3"'] & & x_2x_3x_1x_4 \arrow[d, "x_2r_{31}x_4"] & \\
x_1x_2x_4x_3 \arrow[dr, "x_1x_2r_{43}"'] & & x_2x_1x_3x_4 \arrow[dl, "r_{21}x_3x_4"] & \\
 & x_1x_2x_3x_4 & &
\end{tikzcd}$$

So, we see that in the path $x_4x_3x_2x_1 \longrightarrow x_1x_2x_3x_4$, the element $x_1x_2x_3x_4$ is an R-reduced form of the monomial $x_4x_3x_2x_1$.

However, as illustrated in the example above, the path $a \longrightarrow b$ might not be unique, that is, there might be more than one ways to derive b starting from a. In addition, it might be the case that on each level we have to make a choice on which reduction we should use and to which part of the give vertex. So, it is natural to wonder whether all of the procedures produce a unique irreducible form to an expression and of course, it is natural to wonder whether this is done in a canonical way, with no choices involved.

The answer to the above questions as well as an algorithmic procedure for reduction by substitution was given by Bergman in [Ber78].

Under the above identification, we are able to express relations in $\mathrm{gr}_\bullet A$ that are neither quadratic nor consequences of them. In this new language of graphs, such a relation occurs when there exists some non-confluent term.

Definition 4.3.4. A term $a \in \mathbb{T}(V)$ is called a *critical term* if it is the origin of at least two distinct edges. When we arrive to a critical term, we say that there is an *ambiguity* in rewriting systems.

A term a is called *confluent* if every pair of paths that starts from a ends in a common vertex. In this case, we say that the ambiguity is a *solvable ambiguity.*

Example.
In the preceding example, we saw that the term $x_4x_3x_2x_1$ is a critical term, as multiple paths produced ambiguity in rewriting terms. However, since any two paths that start from $x_4x_3x_2x_1$ end in the common vertex $x_1x_2x_3x_4$, the monomial $x_4x_3x_2x_1$ is confluent and the ambiguity is solvable.

Theorem 4.3.5 (Bergman's Diamond Lemma)**.** *Let S be a reduction system for a free associative algebra $\mathbb{T}(V)$ and assume that a basis of generators of V admits an order $\leq$ that is compatible with S and satisfies the descending chain condition. Then the following are equivalent.*

(i) All ambiguities of S are solvable;

(ii) All elements of $\mathbb{T}(V)$ are reduction unique under S;

(iii) A set of representatives in $\mathbb{T}(V)$ for the elements of the algebra $A = \mathbb{T}(V)/(R)$ determined by the generators V and the relations $r_{lead\sigma} = r_{lower\sigma}$, $\sigma \in S$ is given by the $\Bbbk$-submodule $\mathbb{T}(V)_{irr}$ spanned by the S-irreducible monomials of the free monoid $\langle V\rangle$ on a basis of V.

When one of these conditions hold, then A can be identified with the $\Bbbk$-module $\mathbb{T}(V)_{irr}$, viewed as an algebra by the multiplication $a \cdot b = r_s(ab)$, where $r_s(ab)$ is the unique reduction of the term ab.

Proof. For a proof, we refer to [Ber78, Theorem 1.2]. □

We represent the successive relations that are applied to elements in A_n by connected graphs. The associated terminal vertices are the linear combinations of monomials labeled by elements in $S^{(n)}$, as those vertices do not have any other leading terms of any relation. When a monomial descends to two different terminal vertices, these two have to be equal in A. So, the collection of monomials $\{x_{i_1} \cdots x_{i_n} : (i_1, \ldots, i_n) \in S^{(n)}\}$ consist of a PBW basis for A if and only if every connected graph has a unique terminal vertex, and the collection of the terminal vertices consists of the PBW basis of A.

Corollary 4.3.6. *Let $A = \{V, R\}$ be a quadratic algebra, and assume that $\mathbb{T}(V)$ is weight-graded. If the ambiguities coming from critical monomials are solvable, then the monomials $\{x_{i_1} \cdots x_{i_n} : (i_1, \ldots, i_n) \in S^{(n)}\}$ form a PBW basis for A and A is Koszul.*

Proof. By Theorem 4.2.3, it is enough to check that this holds for elements that do not belong to $\{x_{i_1}x_{i_2}x_{i_3} : (i_1, i_2, i_3) \in S^{(3)}\}$. So assume that there exists a nontrivial linear combination of elements labeled in $S^{(3)}$. Representing a relation $x = y$, where x and y are sums of elements labeled in $S^{(3)}$ with a graph, we arrive at a picture as follows:

$$x \longleftarrow - \longleftarrow - \longrightarrow - \longleftarrow \cdots \longleftarrow - \longrightarrow - \longrightarrow - \longrightarrow y.$$

However, since by assumption all ambiguities are solvable, we can find another path, such that the distance between x and the first vertex of the form $\longleftarrow - \rightarrow$ is strictly less than the distance of the original graph. Iterating this, we end up with a graph of the form

$$x \longleftarrow - \longrightarrow - \longrightarrow - \longrightarrow \cdots \longrightarrow y.$$

Finally, for the part $x \longleftarrow -$, since the ambiguities are solvable, we cannot find an edge leading to x. This means that all monomials $\{x_{i_1} \cdots x_{i_3} : (i_1, \ldots, i_3) \in S^{(3)}\}$ have a unique reduced form, and these reduced forms consist of a basis for A_3. By Diamond Lemma Theorem 4.2.3, the algebra A is a PBW algebra, and thus Koszul. □

To use Bergman's Diamond Lemma and show that we have a PBW basis, it suffices to check the graphs arising by elements that do not belong to the set $\{x_{i_1}x_{i_2}x_{i_3} : (i_1, i_2, i_3) \in S^{(3)}\}$ have a terminal vertex.

Example.
Consider the algebra $A = \{V, R\}$, where V has a basis $\{x_1, x_2\}$ and R is the relator $r = x_1^2 - x_2^2$. We will show that A is not a PBW algebra, by showing that x_2^3 has two different decompositions.

$$\begin{tikzcd}
& x_2^3 \arrow[ld, "rx_2"'] \arrow[rd, "x_2r"] & \\
x_1^2x_2 & & x_2x_1^2
\end{tikzcd}.$$

Indeed, since the reduction is not unique, A is not PBW.

Example.
Consider the symmetric algebra $A = \mathrm{Sym}(V)$, where V admits a basis of generators $\{x_1, x_2, x_3\}$ and R consists of the relators $r_{ji} = x_jx_i - x_ix_j$, for $1 \leq i < j \leq 3$. The only critical monomials of length 3 are $x_2^2x_1$, $x_3x_2x_1$, $x_3^2x_1$ and $x_3^2x_2$. We shall make a graph of reductions for each of them, to show that they are all confluent.
For $x_2^2x_1$, we have

$$\begin{tikzcd}
x_2^2x_1 \arrow[d, "x_2r_{21}"'] \\
x_2x_1x_2 \arrow[d, "r_{21}x_2"'] \\
x_1x_2^2,
\end{tikzcd}$$

therefore the critical monomial $x_2^2x_1$ is confluent. Similarly we see that

$$\begin{tikzcd}
& x_3x_2x_1 \arrow[ld, "r_{32}x_1"'] \arrow[rd, "x_3r_{21}"] & \\
x_2x_3x_1 \arrow[d, "x_2r_{31}"'] & & x_3x_1x_2 \arrow[d, "r_{31}x_2"] \\
x_2x_1x_3 \arrow[rd, "r_{21}x_3"'] & & x_1x_3x_2 \arrow[ld, "x_1r_{32}"] \\
& x_1x_2x_3 &
\end{tikzcd}.$$

$$\begin{tikzcd}
x_3^2x_1 \arrow[d, "x_3r_{31}"'] \\
x_3x_1x_3 \arrow[d, "r_{31}x_3"'] \\
x_1x_3^2,
\end{tikzcd}$$

and

$$\begin{tikzcd}
x_3^2x_2 \arrow[d, "x_3r_{32}"'] \\
x_3x_2x_3 \arrow[d, "r_{32}x_3"'] \\
x_2x_3^2.
\end{tikzcd}$$

Since all ambiguities are solvable, we conclude that A is PBW. $\square$

Chapter 5

Forms of Enhanced Koszulity

Galois theory has been playing a central role in mathematical research for the past two centuries; yet many questions remain unanswered and many objects of study rather mysterious. Among the deepest problems is to classify which profinite groups are realizable as Galois groups. To this extent, very few things are yet known, so we turn to the study of Galois cohomology for answers.

The most significant result in this direction is the proof of the Bloch-Kato Conjecture, by V. Voevodsky, with the contributions of M. Rost et al, now known as the Voevodsky-Rost Theorem. The Voevodsky-Rost Theorem allows us to obtain some understanding of Galois cohomology, however it does not let us see the shape of absolute Galois groups directly.

Assume that $\mathbb{F}$ contains a primitive p-th root of unity. As demonstrated in Section 3.1, the Galois cohomology algebra $H^{\bullet}(\mathbb{F}, \mathbb{F}_p) = \oplus_n H^n(\mathbb{F}, \mathbb{F}_p)$ is a quadratic $\mathbb{F}_p$-algebra, which means that all its generators lie in $H^1(\mathbb{F}, \mathbb{F}_p)$, while all the relations are consequences of the ones generated in $H^2(\mathbb{F}, \mathbb{F}_p)$. This puts some serious restrictions on the description of the absolute Galois group of $\mathbb{F}$.

On the other hand, showing that Galois cohomology is Koszul, gives us a full understanding of how higher relations are connected to one another. Moreover, Koszulity of Galois cohomology, along with the bijectivity of the norm-residue homomorphism in degree 2 and its injectivity in degree 3 imply a more natural and elementary proof of the Bloch-Kato Conjecture (see [Pos05, Theorem 1.3]). However, it was demonstrated in Chapter 4 that Koszulity is not always easy to determine, while properties that imply Koszulity, such as the existence of a PBW basis, are easier to show.

Throughout this Chapter, we introduce notions that are stronger than an algebra being PBW, and hence Koszul. Namely, the case of strongly Koszul and universally Koszul algebras, as well as algebras with Koszul filtrations.

The notion of strong Koszulity, the strongest property of all and directly implying Koszulity, made its first appearance in the paper [HHR00] of Herzog, Hibi and Restuccia. Here, we adopt their definition, without however assuming that the objects of study are ordered. Strong Koszulity provides with a direct way to construct a linear resolution to **any** linear A-module. Taking into account that Koszulity asks for a linear resolution of the trivial A-module $\Bbbk$, the extremely powerful implications of strong Koszulity are impossible to miss.

However, strong Koszulity is often "too good to be true". This is why the concept of Koszul filtration in the commutative setting was introduced in [CTV01], as a more flexible version of strong Koszulity. What is magic about Koszul filtration is that it encodes precisely the properties needed to imply the Koszulity, but in a coordinate-free way, which allows us for more options in the choice of ideals. The definition of Koszul filtration, which we present here, is taken from [Pio05].

If a Koszul filtration for a quadratic algebra exists, then we can choose ideals of any number of generators. Thus, algebras with Koszul filtrations have many Koszul cyclic modules. On the other hand, one would like the filtration to be as big as possible, namely asking that all ideals generated in degree 1 are Koszul. This is precisely the definition of universal Koszulity, given in the commutative setting in [Con00]. Here, we extend this definition to a general setting.

First, we recall the formulation of the Bloch-Kato Conjecture. We then introduce the forms of enhanced Koszulity mentioned above and discuss some fundamental properties of each.

Further, we give a small exposition on the family of Elementary Type pro-p-groups, and we finally define the twisted extension of a quadratic algebra by a set.

The material presented in this Chapter should be treated as the base of the next Chapters of this writing. For further reading, suggested references are [HHR00], [Pio05], [Con00], [MPQT] for more details on Elementary Type pro-p-groups and [Wad83] for the definition of a twisted extension.

5.1 The Bloch-Kato Conjecture

Let $\mathbb{F}$ be a field. For $n > 1$, we define the *n-th Milnor K-group* $K_n^M\mathbb{F}$ to be the quotient of the n-fold tensor product $\mathbb{F}^\times \otimes_\mathbb{Z} \cdots \otimes_\mathbb{Z} \mathbb{F}^\times$ by the subgroup generated by those elements satisfying $a_1 \otimes \cdots \otimes a_n$ with $a_i + a_j = 1$ for some $1 \leq i < j \leq n$. The latter relation is usually called the *Steinberg relation.* We define $K_0^M\mathbb{F} = \mathbb{Z}$ and $K_1^M\mathbb{F} = \mathbb{F}^\times$. For elements $a_1, \ldots, a_n \in \mathbb{F}^\times$, we denote the class of $a_1 \otimes \cdots \otimes a_n$ in $K_n^M\mathbb{F}$ by $\{a_1, \ldots, a_n\}$ and we call it a *symbol.*

Now, let p be a prime number such that $\operatorname{char}\mathbb{F} \neq p$. The *Kummer isomorphism*

$$\mathbb{F}^\times/\mathbb{F}^{\times p} \overset{\cong}{\to} H^1(\mathbb{F}, \mu_p)$$

extends to the *norm residue homomorphism*

$$h_n : K_n^M\mathbb{F}/p \longrightarrow H^n(\mathbb{F}, \mu_p^{\otimes n}),$$

sending $\{a_1, \ldots, a_n\}$ to $(a_1) \cup \ldots \cup (a_n)$ and Milnor asked whether this map is an isomorphism for $p = 2$. The same question was formulated by K. Kato for p being odd in [Kat80], and is known as the Bloch-Kato Conjecture. In other words, the *Bloch-Kato Conjecture* asserts that

$$K_n^M\mathbb{F}/p \overset{\cong}{\to} H^n(\mathbb{F}, \mu_p^{\otimes n}),$$

for all $n \geq 0$, for all fields $\mathbb{F}$ and all p that are prime to $\operatorname{char}\mathbb{F}$.

For $n = 0$, the statement is trivial. For $n = 1$, it is Kummer theory. For global fields and $n = 2$, it was solved by J. Tate in [Tat76]. For $n = 2 = p$, it was proved by A. Merkurjev in [Mer81]. For $n = 2$ and all p that are invertible in $\mathbb{F}$ it was proved by A. Merkurjev and A. Suslin in [MeSu82]. For $n = 3$ and $p = 2$ it was proved by A. Merkurjev and A. Suslin in [MeSu90] and independently by M. Rost in [Ros86]. In particular, for $p = 2$, the Bloch-Kato Conjecture is known as the *Milnor Conjecture* and was proven by V. Voevodsky in 1996 (cf. [Voe03]). Finally, the proof of the general case, was given by V. Voevodsky in [Voe11], with majors contributions of M. Rost and various other important mathematicians.

These results provide a description of Galois cohomology in terms of generators and relations. However, usually there is a relation between relations, a relation between relations between relations and so on and so forth. Driven by that and in attempt to understand Galois cohomology better, L. Positselski in [Pos05] stated the following

Conjecture(Positselski). Let $\mathbb{F}$ be a field containing a primitive p-th root of unity. Then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is Koszul.

Note that we have already seen that $K^M_\bullet\mathbb{F}/p$, and hence, $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is a quadratic $\mathbb{F}_p$-algebra. Its Koszulity then would imply a resolution of all higher Steinberg relations, which would then results a complete description of $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ an would hence put some serious restrictions on the silhouette of the absolute Galois group $G_\mathbb{F}$.

Moreover, in [PV95] it was shown that the Koszulity of the small Milnor K-theory, together with the fact that the norm residue homomorphism is bijective in degree 2 and injective in degree 3 would not only imply a stronger version of the Bloch-Kato Conjecture, but also a more natural proof.

Throughout this chapter, we introduce richer forms of Koszulity. As the name suggests, each of the different notions implies Koszulity, but in a more insightful way concerning the enigmatic world of profinite and pro-p Galois groups.

5.2 Enhanced Koszulity

Let $\mathbb{k}$ be a field and recall that all quadratic $\mathbb{k}$-algebras are assumed to be of finite type. In particular, every such algebra A is equipped with the *augmentation map*

$$\varepsilon\colon A \to \mathbb{k}$$

that is the projection onto A_0. Its kernel is the *augmentation ideal*

$$A_+ = \bigoplus_{n\geq 1} A_n.$$

The augmentation map induces a canonical structure of $\mathbb{k}$ as a graded A-module concentrated in degree 0, via the action $a \cdot f = \varepsilon(a)f$.

Definition 5.2.1. A graded module M over a quadratic algebra A is *generated in grade n* if and only if the natural map

$$\varpi : A \otimes M_n \longrightarrow M$$

induced by the module structure is surjective.

M is called *quadratic* if, for some $n \in \mathbb{Z}$, M is generated in degree n and $\ker \varpi$ is generated, as an A-submodule, by $\ker \varpi \cap (A_1 \otimes M_n)$.

Informally, this means that M has a presentation with degree n generators and degree $n+1$ relators.

Recall from Definition 3.2.2 that a quadratic $\mathbb{k}$-algebra A is called *Koszul* if the trivial A-module $\mathbb{k}$ admits a linear resolution, that is, it has a graded free resolution $(P_\bullet, d_\bullet)$ with each P_i generated in degree i, i.e. $P_i = A \cdot (P_i)_i$.

In similar flavor, we make the following

Definition 5.2.2. A graded module M generated in degree n over a quadratic algebra A is said to be *Koszul* if it has a linear resolution, that is, a graded free resolution $(P_\bullet, d_\bullet)$ with each P_i generated in degree $i+n$, that is, $P_i = A \cdot (P_i)_{i+n}$.

A free resolution of $\mathbb{k}$ can be contracted to a free resolution of A_+ and reversely, a free resolution of A_+ can be extended to a free resolution of $\mathbb{k}$, which leads to the equivalence of the following

1. A is Koszul;

2. $\mathbb{k}$ is a Koszul module;

3. A_+ is a Koszul module.

Note that the trivial A-module $\mathbb{k}$ is generated in degree 0. Therefore, Definition 5.2.2 of Koszul module is nothing but a generalization of Definition 3.2.2 of Koszul algebra. Further, since all objects treated here are assumed to be of finite type, linear resolutions have also a homological interpretation. Namely, a graded A-module M generated in degree n is Koszul if and only if $H_i(M)_j = 0$ for all $i \geq 0$ and $j \neq i+n$. This implies that a Koszul module is quadratic.

Let A be a quadratic $\mathbb{k}$-algebra.

Definition 5.2.3. Let $X = \{a_1, \dots, a_d\}$ be an minimal system of homogeneous generators of the augmentation ideal A_+ of A. A graded A-module M is called *linear* if it admits a system of generators $\{g_1, \dots, g_m\}$ of the same degree, such that for each $j \in \{1, \dots, m\}$ the colon ideal of A

$$(Ag_1 + \cdots + Ag_{j-1}) \colon g_j = \{a \in A : ag_j \in Ag_1 + \cdots + Ag_{j-1}\}$$

is generated by a subset of X. Note that for $j = 1$, the corresponding colon ideal is $(0) : g_1$. Such a system is called a *set of linear generators* of M.

In other words, a linear A-module can gradually be made up by adding one element at a time. This makes the construction of resolutions for these modules significantly easier.

Definition 5.2.4. A quadratic algebra A is called *strongly Koszul* if its augmentation ideal A_+ admits a system of homogeneous generators $X = \{a_1, \ldots, a_d\}$, such that for every subset $Y = \{a_{i_1}, \ldots, a_{i_m}\} \subseteq X$ and for every $j = 1, \ldots, m$ the colon ideal

$$(a_{i_1}, \ldots, a_{i_{j-1}})\colon a_{i_j} = \{a \in A : aa_{i_j} \in (a_{i_1}, \ldots, a_{i_{j-1}})\}$$

is generated by a subset of X.

Keeping the same notation, by Definition 5.2.3, we get that A is strongly Koszul if and only if all the ideals $(a_{i_1}, \ldots, a_{i_m})$ are linear A-modules.

In [HHR00], where the definition was first given, it was assumed that the system of homogeneous linear generators is ordered. However, this assumption was made due to the fact that their objects of study were already ordered. We therefore adopt the definition, but without assuming an ordering in the set of generators, following [CDR13], for instance.

In the same paper, it was shown that the name “strongly Koszul” is justified, as is demonstrated in the following

Theorem 5.2.5 (Herzog, Hibi, Restuccia)**.** *Let A be a strongly Koszul $\Bbbk$-algebra with respect to the system of homogeneous generators $X = \{a_1, \ldots, a_d\}$. Then any linear A-module has a linear resolution.*

Proof. We first claim that any graded module admits a set of homogeneous generating relations. To see this, assume that the sum of some elements is zero. Since the homogeneous components of a module are inside a direct sum, this means that each subsum of elements that belong to the same homogeneous component is zero. In other words, a nonhomogeneous relation is always a consequence of homogeneous ones, and we can always assume that the generating relations are homogeneous.

The first step is to show that any linear A-module M has linear generating relations. For this, let $\{g_1, \ldots, g_m\}$ be a system of linear generators of M. Let $c_1 g_1 + \ldots + c_m g_m$ be a (homogeneous) generating relation of M and let c_j be its last nonzero coefficient.

Then c_j is a generator of the colon ideal $(c_1 g_1 + \ldots + c_{j-1} g_{j-1}) : g_j$. Indeed, it obviously belongs to it, and it is a generator, as it comes from a generating relation of M. Since M is linear by assumption, the colon ideal $(c_1 g_1 + \ldots + c_{j-1} g_{j-1}) : g_j$ is generated by a subset of X, all of whose elements have degree 1. Then any set of generators of it has to be made of all degree 1 elements, so c_j has degree 1. And since the relations are homogeneous, we deduce that the degree of all c_i, $i = 1, \ldots, j-1$ is also 1, and thus the generating relation is linear.

On the second step, we show that the syzygy module of a linear module is linear by induction on the number of generators of M. Let $F_\bullet$ be a minimal free graded resolution of M and let $\Omega^1(M)$ denote the first syzygy module of M.

Assume first that $M = Ag_1$. Then $F_0 = A\underline{g_1}$, where $\underline{g_1}$ is the unique generator of degree 0. By definition,

$$\Omega^1(M) = \operatorname{ann}_A(g_1)\underline{g_1} = \{a \in A : ag_1 = 0\}\underline{g_1} = ((0) : g_1)\,\underline{g_1}.$$

Since M is linear by assumption, the colon ideal $(0) : g_1$ is generated by a subset of X. And since all elements of X are of degree 1, we obtain that $(0) : g_1$ is linear.

Now consider the homomorphism

$$\cdot\underline{g_1} : (0) : g_1 \longrightarrow \Omega^1(M) = ((0) : g_1)\,\underline{g_1}.$$

It is not hard to see that this is a graded isomorphism, and since $(0) : g_1$ is linear, we get that $\Omega^1(M)$ is also linear.

Assume now that $\{g_1, \ldots, g_m\}$ is a system of linear generators of M. Then there exists a A-submodule N of M with system of linear generators $\{g_1, \ldots, g_{m-1}\}$. By the induction hypothesis, $\Omega^1(N)$ is then linear with respect to, say, $\{h_1, \ldots, h_k\}$.

Moreover, M/N is cyclic, so by the first step of induction hypothesis, $\Omega^1(M/N)$ is linear with respect to $\{a_{i_1}\underline{g_m}, \ldots, a_{i_l}\underline{g_m}\}$, with $a_{i_1}, \ldots, a_{i_l} \in X$.

We now claim that there is a short exact sequence

$$0 \longrightarrow \Omega^1(N) \xrightarrow{\alpha} \Omega^1(M) \xrightarrow{\beta} \Omega^1(M/N) \longrightarrow 0.$$

This is just the beginning of the proof of the horseshoe Lemma ([Wei95, Lemma 2.2.8]): given two free resolutions, $P_\bullet$ of N and $Q_\bullet$ of M/N, the diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker\epsilon \arrow[r] \arrow[d, "\alpha"] & P_0 \arrow[r, "\epsilon"] \arrow[d, "\iota_0"] & N \arrow[r] \arrow[d, "\iota"] & 0 \\
0 \arrow[r] & \ker(\iota\epsilon+\widetilde{\delta}) \arrow[r] \arrow[d, "\beta"] & P_0 \oplus Q_0 \arrow[r, "\iota\epsilon+\widetilde{\delta}"] \arrow[d, "\pi_0"] & M \arrow[r] \arrow[d, "\pi"] & 0 \\
0 \arrow[r] & \ker\delta \arrow[r] \arrow[d] & Q_0 \arrow[r, "\delta"] \arrow[d] & M/N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

has commutative squares, its rows are exact, its right two columns are exact, ι, ι_0 are the inclusions, π, π_0 are the canonical projections, $\widetilde{\delta} : Q_0 \longrightarrow M$ is a lift of δ and α and β are the restrictions of ι_0 and π_0 respectively. A diagram chase (or the snake Lemma) ensures that the left column is also exact. But that column is the claimed short exact sequence of modules.

We can say that in the above diagram P_0 is the free A module $\bigoplus_{i=1}^{m-1} A\underline{g_i}$, ϵ is the A-linear extension of the map

$$\underline{g_i} \mapsto g_i,$$

and similarly $Q_0 = A\underline{g_m}$ with

$$\delta : \underline{g_m} = [g_m]_N = g_m + N.$$

Then

$$\iota\epsilon + \widetilde{\delta} : \bigoplus_{i=1}^{d} A\underline{g_i} \longrightarrow M, \iota\epsilon + \widetilde{\delta}(\underline{g_i}) = g_i.$$

All $\underline{g_i}$ are given degree 0.

We will construct a system of linear generators of $\Omega^1(M)$ using the systems of linear generators of $\Omega^1(N)$ and $\Omega^1(M/N)$, together with the above short exact sequence. The set of linear generators $\{t_1, \ldots, t_{k+l}\}$ of $\Omega^1(M)$ is then constructed in the following way. For $i = 1, \ldots, k$,

$$t_i = \alpha(h_i).$$

And for $j = 1, \ldots, l$,

$$t_{k+j} = a_{i_j}\underline{g_m} + n_j,$$

for a suitable element n_j of $\Omega^1(N)$. We therefore conclude that $\Omega^1(M)$ is linear. For the construction of the whole resolution of M, it suffices to note that $\Omega^n(M) = \Omega^1\left(\Omega^{n-1}(M)\right)$. □

Due to its combinatorial complexity, strong Koszulity fails to become useful in many ways. So we would like to have other properties which imply Koszulity, but are less combinatorially involved.

One of the instant implications of strong Koszulity is the more relaxed property of the existence of a Koszul filtration.

Definition 5.2.6. A collection $\mathcal{F}$ of ideals of a quadratic algebra A is a *Koszul filtration* if

1. the zero ideal and the augmentation ideal A_+ belong to $\mathcal{F}$;

2. each ideal $I \in \mathcal{F}$ is generated by elements of A_1;

3. for each $(0) \neq I \in \mathcal{F}$, there exist $I \neq J \in \mathcal{F}$ and $x \in A_1$, such that $I = J + (x)$ and the colon ideal $J\colon I = \{a \in A : xa \in J\}$ lies in $\mathcal{F}$.

Property 3. can also be seen as $I = J + (x)$ and $J\colon x \in \mathcal{F}$.

Note that strong Koszulity implies immediately properties 2. and 3. of the Definition of Koszul filtration above, while property 1. is obvious. To see this, note that if A is strongly Koszul, then the collection $\mathcal{F} = \{(Y) : Y \subseteq X\}$ is a Koszul filtration.

In fact, the existence of a Koszul filtration immediately implies that the given algebra is Koszul, but in a coordinate-free way, which gives us a bigger pool of options for the chosen collection of ideals than strong Koszulity. The general proof that each ideal of a Koszul filtration is a Koszul module first appeared in [Pio05].

Algebras admitting a Koszul filtration have sufficiently many Koszul cyclic modules. At the extreme, one may ask the algebra to have a Koszul filtration as big as possible, so that all ideals generated in degree 1, or equivalently all cyclic modules, are Koszul. In the commutative setting, this property has been introduced in [Con00] under the name of *universal Koszulity.* We extend the definition to the possibly noncommutative setting.

Definition 5.2.7. A quadratic algebra A is called *universally Koszul* if every ideal generated in degree 1 has a linear resolution.

As in the commutative setting in [Con00], we define

$$\mathcal{L}(A) = \{I \trianglelefteq A : I = AI_1\}$$

to be the set of all ideals of A generated in degree 1 and we have the following characterization of universally Koszul algebras.

Proposition 5.2.8. *For a quadratic algebra A, the following are equivalent.*

(i) *A is universally Koszul;*

(ii) *for every $I \in \mathcal{L}(A)$ and every $x \in A_1 \setminus I$ one has $I : (x) \in \mathcal{L}(A)$;*

(iii) *$\mathcal{L}(A)$ is a Koszul filtration.*

Schematically, all known implications are presented below.

$$\begin{tikzcd}
& \text{Universally Koszul} \arrow[dr, Rightarrow] & & \text{Strongly Koszul} \arrow[dl, Rightarrow] \\
\text{PBW} \arrow[dr, Rightarrow] & & \text{Koszul filtration} \arrow[dl, Rightarrow] & \\
& \text{Koszul} & &
\end{tikzcd}$$

In this work, a new implication is added to the above, namely that Universal Koszulity does not imply Strong Koszulity, adding the arrow

$$\begin{tikzcd}
\text{Universally Koszul} \arrow[r, Rightarrow, "/" marking] & \text{Strongly Koszul}
\end{tikzcd}$$

to the above scheme.

5.3 Elementary Type pro-p-groups

The family of elementary type pro-p-groups is one of the most prominent families in field theory. The reason for this is that every known case where the maximal pro-p-quotient $G_{\mathbb{F}}(p)$ of $G_{\mathbb{F}}$ is finitely generated, this group is of elementary type. And generally, it is believed and conjectured that every finitely generated pro-p-group is of elementary type which their study under the spotlight.

Definition 5.3.1. The class $\mathcal{E}_p$ of *elementary type* cyclotomic pairs is the smallest class of cyclotomic pairs, such that

(a) any pair (G, χ), with G a finitely generated free pro-p-group and χ an arbitrary cyclotomic character, is in $\mathcal{E}_p$; the pair $(1, 1)$ consisting of the trivial group and the trivial character is not excluded;

(b) any pair (G, χ), with G a Demushkin group and χ its unique cyclotomic character, provided $\operatorname{im} \chi \subseteq 1 + p\mathbb{Z}_p$, is in $\mathcal{E}_p$;

(c) if $(G_1, \chi_1), (G_2, \chi_2) \in \mathcal{E}_p$, then also the free product $(G_1 *_p G_2, \chi_1 *_p \chi_2)$ is in $\mathcal{E}_p$;

(d) if $(G, \chi) \in \mathcal{E}_p$, then for any positive integer m also the cyclotomic semidirect product $(\mathbb{Z}_p^m \rtimes G, \chi \circ \pi)$ is in $\mathcal{E}_p$.

An *elementary type* pro-p-group is a group G appearing in a pair from $\mathcal{E}_p$.

In other words, the family of elementary type pro-p-groups is the family constructed inductively starting with finitely generated free and Demushkin pro-p-groups as basis and applying the elementary operations of free pro-p-products and cyclotomic semidirect products.

Recall the construction of the direct sum of two quadratic algebras given in Section 3.1. If $A = \{V_A, R_A\}$ and $B = \{V_B, R_B\}$ are two quadratic algebras, then the *direct sum* of A and B is the quadratic algebra

$$A \sqcap B = \frac{\mathbb{T}(A_1 \oplus B_1)}{(R)}, \quad \text{with } R = R_A \oplus R_B \oplus (A_1 \otimes B_1) \oplus (B_1 \otimes A_1).$$

Theorem 5.3.2 ([NSW08, Theorem 4.1.4])**.** *Let G_1 and G_2 be elementary type pro-p-groups. Then $H^\bullet(G_1 *_p G_2, \mathbb{F}_p) \cong H^\bullet(G_1, \mathbb{F}_p) \sqcap H^\bullet(G_2, \mathbb{F}_p)$.*

Therefore, the cohomology algebra of the free product of two elementary type pro-p-groups coincides with the direct sum of their cohomology algebras.

Definition 5.3.3. Let A be a graded-commutative quadratic $\mathbb{F}_p$-algebra, with space of generators $V = \operatorname{span}_{\mathbb{F}_p}\{t, a_1, \ldots, a_d\}$, space of relators R and a distinguished element t, such that $t + t = 0$. Let $\{x_1, \ldots, x_m\}$ be a set of distinct symbols not belonging to A. The *twisted extension* of A by $\{x_1, \ldots, x_m\}$ is the quadratic $\mathbb{F}_p$-algebra $A(t; x_1, \ldots, x_m)$ with space of generators

$$\operatorname{span}_{\mathbb{F}_p}\{t, a_1, \ldots, a_d, x_1, \ldots, x_m\}$$

and space of relators

$$\mathrm{span}_{\mathbb{F}_p}\left(R \cup \{x_i x_j + x_j x_i, x_j t + t x_j, x_j a_k + a_k x_j, x_j^2 - t x_j\}\right),$$

for i, j each running through $\{1, \ldots, m\}$ and $k = 1, \ldots, d$.

Now, recall from section 3.1 that the *skew-symmetric tensor product* of two quadratic algebras $A = \{V_A, R_A\}$ and $B = \{V_B, R_B\}$ is the quadratic algebra given by

$$A \otimes^{-1} B = \frac{\mathbb{T}(A_1 \oplus B_1)}{(R)}, \quad \text{with } R = R_A \oplus R_B \oplus \langle ab + ba : a \in A_1, b \in B_1 \rangle .$$

Therefore, a twisted extension $A(0; x_1, \ldots, x_m)$ with $t = 0$ is the same as the skew-symmetric tensor product of A with the exterior algebra on a set of variables $\{x_1, \ldots, x_m\}$.

We further wish to make one more remark, namely, that the twisted extension $A(0; x_1, \ldots, x_m)$ admits an additional $\oplus_{i=1}^m (\mathbb{Z}/2\mathbb{Z})$-grading, characterized by

$$A(0; x_1, \ldots, x_m)_{(\varepsilon_1 + 2\mathbb{Z}, \ldots, \varepsilon_m + 2\mathbb{Z})} = \mathrm{span}_{\mathbb{F}_p}\{a x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m} : a \in A\}. \qquad (\heartsuit)$$

In particular, $A(0; x)$ has the additional $\mathbb{Z}/2\mathbb{Z}$-grading

$$A(0; x)_{0+2\mathbb{Z}} = A, \; A(0; x)_{1+2\mathbb{Z}} = Ax.$$

A twisted extension of the Galois cohomology algebra of an elementary type pro-p-group can be extracted from the cohomology of the group itself as shown in

Theorem 5.3.4. *[MPQT] Let G be an elementary type pro-p-group. Then $H^\bullet(\mathbb{Z}_p^m \rtimes G, \mathbb{F}_p) \cong H^\bullet(G, \mathbb{F}_p)(0; x_1, \ldots, x_m)$.*

And this means that the semidirect product above is nothing but the twisted extension of $H^\bullet(G, \mathbb{F}_p)$.

The last notions that we would like to recall, as they will be proven useful later are the extension and contraction of ideals. Let $A \subseteq B$ be two algebras and recall that given an ideal I of A, we define its *extension* to B to be the intersection I^e of all ideals of B that contain I. In other words, I^e is the ideal of B generated by the same generators of I as an ideal of A. Given an ideal J of B, we define its *contraction* to A to be the ideal $J^c = J \cap A$ of A. In case A_1, A_2 are two subalgebras of B, we will use the notation $J^c_{A_1}$ or $J^c_{A_2}$ to differentiate between the contractions of J to either subalgebra.

Chapter 6

Groups that satisfy strong Koszulity

In Section 5 we discussed the various forms of enhanced Koszulity. This part is devoted to pro-p-groups whose Galois cohomology is strongly Koszul. Applied to Galois theory, we obtain explicit description of the Galois cohomology of various families of absolute Galois groups.

As a consequence of this work, we show that the Galois cohomology of certain elementary type pro-p-groups is strongly Koszul. We do this by proving the statement for each class of groups inside the family $\mathcal{E}_p$. Namely, we first show that if the maximal pro-p-quotient of the absolute Galois group over a field is a finitely generated free or a Demushkin group, then the Galois cohomology algebra satisfies strong Koszulity. After having established these, we then show that the direct sum of two strongly Koszul algebras is again a strongly Koszul algebra. Combining this with Theorem 5.3.2, we deduce that the cohomology of the free product of two elementary type pro-p-groups is strongly Koszul. And finally, we show that the twisted extension of a strongly Koszul algebra is strongly Koszul. Putting this together with Theorem 5.3.4, gives us the full statement.

Notice that for $p = 2$, the assumption $\sqrt{-1} \in \mathbb{F}$ had to be taken. This hints that strong Koszulity depends heavily on the behavior of the ground field, which dictates the cohomological complexity of the absolute Galois group, so it is doomed to fail at some point.

Nonetheless, it is a miraculous fact that big families of groups fall under the category of groups whose algebras do satisfy strong Koszulity.

Let $\mathbb{F}$ be a field containing a primitive p-th root of unity and for $p = 2$

assume that $\mathbb{F}$ contains $\sqrt{-1}$. We further assume that $\dim_{\mathbb{F}_p} \mathbb{F}^\times/\mathbb{F}^{\times p} = n < \infty$. Under this assumption, by Voevodsky's proof of the Bloch-Kato Conjecture ([Voe11]), we have that

$$H^\bullet(\mathbb{F},\mathbb{F}_p) \cong \mathbb{T}(\mathbb{F}^\times)/p \left\langle a \otimes (1-a) : 1 \neq a \in \mathbb{F}^\times \right\rangle .$$

In particular, two spectacular implications arose from the Voevodsky-Rost Theorem. First, that $H^\bullet(\mathbb{F},\mathbb{F}_p)$ is a commutative quadratic $\mathbb{F}_p$-algebra. And second, that the inflation map

$$H^\bullet(\mathbb{F}(p),\mathbb{F}_p) \xrightarrow{\text{inf}} H^\bullet(\mathbb{F},\mathbb{F}_p)$$

is an isomorphism, meaning that we can effectively study the cohomology of maximal pro-p-quotients instead of absolute Galois groups, without any loss of information.

By studying pro-p-groups, we conclude that in certain cases, Galois cohomology is strongly Koszul, hence Koszul.

6.1 Free pro-p-groups

The first instance of strong Koszulity appears in the Galois cohomology of free groups.

Proposition 6.1.1. *Suppose that G is a free pro-p-group on n generators. Then $H^\bullet(G,\mathbb{F}_p)$ is strongly Koszul.*

Proof. We know by Proposition 2.2.1 that the cohomology is concentrated in degrees 0 and 1, that is, $R = \langle u_1,\ldots,u_m\rangle$, where each of the $u_1,\ldots,u_m$ is a quadratic monomial. Now, if $H^\bullet(G,\mathbb{F}_p) = \mathbb{F}_p[x_1,\ldots,x_n]/(R)$, let $\bar{x_i}$ denote the residue class of x_i, $i = 1,\ldots,n$. To show that $H^\bullet(G,\mathbb{F}_p)$ is strongly Koszul, we need to show that for any sequence of elements $\bar{x_{i_1}},\ldots,\bar{x_{i_k}}$, the colon ideal $(\bar{x_{i_1}},\ldots,\bar{x_{i_{k-1}}})\colon \bar{x_{i_k}}$ is generated by a subset of $\bar{x_1},\ldots,\bar{x_n}$.

Note that

$$(\bar{x_{i_1}},\ldots,\bar{x_{i_{k-1}}})\colon \bar{x_{i_k}} = \big((R, x_{i_1},\ldots,x_{i_{k-1}})\colon x_{i_k}\big)/R. \qquad (*)$$

Now, we have

$$(R, x_{i_1},\ldots,x_{i_{k-1}})\colon x_{i_k} = (u_{j_1},\ldots,u_{j_r}, x_{i_1},\ldots,x_{i_{k-1}}),$$

where none of the monomials appearing on the right hand side is divisible by any of the $x_{i_1}, \ldots, x_{i_{k-1}}$. Passing to the definition of the colon ideal, we obtain that

$$(R, x_{i_1}, \ldots, x_{i_{k-1}})\colon x_{i_k} = \left(\frac{u_{j_1}}{\gcd(u_{j_1}, x_{i_k})}, \frac{u_{j_2}}{\gcd(u_{j_2}, x_{i_k})}, \ldots, \frac{u_{j_r}}{\gcd(u_{j_r}, x_{i_k})}, x_{i_1}, \ldots, x_{i_{k-1}} \right).$$

Now, if x_{i_k} divides the quadratic monomial u_{j_s} for some $s \in \{1, \ldots, r\}$, then the fraction $\frac{u_{j_s}}{\gcd(u_{j_s}, x_{i_k})}$ is a variable. And if x_{i_k} does not divide u_{j_s}, then $\frac{u_{j_s}}{\gcd(u_{j_s}, x_{i_k})} = u_{j_s}$.

So in either case, $(R, x_{i_1}, \ldots, x_{i_{k-1}})\colon x_{i_k}$ is generated by a subset of u_{j_s}'s and some of $x_1, \ldots, x_n$. Quotieting with R, however, kills all the u_{j_s}'s and thus $(\bar{x_{i_1}}, \ldots, \bar{x_{i_{k-1}}})\colon \bar{x_{i_k}}$ is generated by a subset of $\bar{x_1}$, …, $\bar{x_n}$. □

Corollary 6.1.2. *Suppose that $G_{\mathbb{F}}(p)$ is a free pro-p-group on n generators. Then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is strongly Koszul.*

Proof. The proof is identical to that of the preceding proposition. □

6.2 Demushkin groups

Passing to the next higher cohomological dimension, recall that the pro-p-groups of cohomological dimension 2 satisfying Poincaré duality, are called Demushkin groups and were classified by Demushkin in [Dem61] and [Dem63].

We show that if $G_{\mathbb{F}}(p)$ is Demushkin, the its cohomology algebra is strongly Koszul. Recall from 2.3 that the presentation of a Demushkin group depends on whether the invariant q is 2 and on the the square class of the image its character. We therefore have to take into account each of the different cases, and show that for each individual one, the Galois cohomology algebra $H^\bullet(\mathbb{F}(p), \mathbb{F}_p)$ is strongly Koszul. In this sense, the result is independent of the presentation of the group.

Proposition 6.2.1. *Let G be a Demushkin group on d generators and assume that $q \neq 2$. Then $H^\bullet(G, \mathbb{F}_p)$ is strongly Koszul.*

Proof. Since $q \neq 2$, we know that the number d of generators of $H^\bullet(G, \mathbb{F}_p)$ is necessarily even, say $d = 2k$. Moreover, it was shown in [Lab67, Proposition

4] that there exists a symplectic basis $X = \{a_1, \dots, a_{2k}\}$ of $H^1(G, \mathbb{F}_p)$, such that

$$\begin{array}{l} a_1 \cup a_2 = a_3 \cup a_4 = \cdots = a_{2k-1} \cup a_{2k} = 1, \\ a_2 \cup a_1 = a_4 \cup a_3 = \cdots = a_{2k} \cup a_{2k-1} = -1, \ . \\ a_i \cup a_j = 0 \text{ otherwise} \end{array}$$

In order to show that $H^\bullet(G, \mathbb{F}_p)$ is strongly Koszul we distinguish two cases.

1. The subset $Y \subseteq X$ is a singleton $\{a_i\}$.
   Then the only colon ideal involved is $(0)\colon a_i$, and in fact
   $$(0)\colon a_i = \begin{cases} (\{a_j : j \neq i-1\}) & \text{for } i \text{ even} \\ (\{a_j : j \neq i+1\}) & \text{for } i \text{ odd.} \end{cases}$$
   So, $(0)\colon a_i$ is generated by a subset of X.
2. The subset $Y \subseteq X$ contains at least 2 elements.
   Then besides a colon ideal of the preceding type, the colon ideals of the form $(a_{i_1}, \dots, a_{i_{j-1}})\colon a_{i_j}$, for $j > 1$, are involved. But each of these ideals is just the whole (X). So in this case, Y is generated by a subset of X as well. So $H^\bullet(G, \mathbb{F}_p)$ is strongly Koszul. □

Corollary 6.2.2. *Suppose that $G_{\mathbb{F}}(p)$ is a Demushkin group on d generators and that if $p = 2$, then $\sqrt{-1} \in \mathbb{F}$. Then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is strongly Koszul.*

Assume now that $q = 2$.

Proposition 6.2.3. *Let G be a Demushkin group on $d = 2k+1$ generators, where k is a positive integer. Then $H^\bullet(G, \mathbb{F}_p)$ is strongly Koszul.*

Proof. Again, by the work of Labute [Lab67, Proposition 4], we know that there is a basis $X = \{a_1, \dots, a_{2k+1}\}$ of $H^1(G, \mathbb{F}_p)$ such that

$$\begin{array}{l} a_1 \cup a_1 = a_2 \cup a_3 = a_4 \cup a_5 = \cdots = a_{2k} \cup a_{2k+1} = 1, \\ a_3 \cup a_2 = a_5 \cup a_4 = \cdots = a_{2k+1} \cup a_{2k} = 1, \qquad\qquad . \\ a_i \cup a_j = 0 \text{ for all other } i, j \end{array}$$

Imitating the proof of the preceding proposition, we distinguish again the same two cases, namely

1. The subset $Y \subseteq X$ is a singleton $\{a_i\}$.
   Then the only colon ideal involved is

$$(0)\colon a_i = \begin{cases} (\{a_j : j \neq 1\}) & \text{for } i = 1 \\ (\{a_j : j \neq i+1\}) & \text{for } i \text{ even} \\ (\{a_j : j \neq i-1\}) & \text{for } i \neq 1 \text{ odd.} \end{cases}$$

   Therefore, the colon ideal $(0) : a_i$ is generated by a subset of X, implying that $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is strongly Koszul.

2. The subset $Y \subseteq X$ contains at least 2 elements.
   Identical to Proposition 6.2.1. □

Corollary 6.2.4. *Let $G_{\mathbb{F}}(p)$ be a Demushkin group on $d = 2k+1$ generators, $k \in \mathbb{N} \setminus \{0\}$. Then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is strongly Koszul.*

Finally, we need to deal with the case $q = 2$ and G is generated by an even number of generators. These Demushkin groups were classified in [Lab67]. The result remains the same, and the proof follows mutatis mutandis the previous ones, after a suitable base change.

Proposition 6.2.5. *Let G be a Demushkin group with invariant $q = 2$ and $d = 2k$ generators. Then $H^\bullet(G, \mathbb{F}_p)$ is strongly Koszul.*

Proof. By [Lab67, Proposition 4] we know that there is a basis $X = \{a_1, \ldots, a_{2k}\}$ of $H^1(G, \mathbb{F}_p)$, such that

$$\begin{array}{l} a_1 \cup a_1 = a_1 \cup a_2 = a_3 \cup a_4 = \cdots = a_{2k-1} \cup a_{2k} = 1, \\ a_2 \cup a_1 = a_4 \cup a_3 = \cdots = a_{2k} \cup a_{2k-1} = 1, \\ a_i \cup a_j = 0 \text{ otherwise} \end{array} .$$

The change of basis

$$b_1 = a_1, \quad b_2 = a_2 + a_1, \quad b_i = a_i \ (i = 3, \ldots, 2k).$$

implies that

$$\begin{cases} b_1 \cup b_1 = a_1 \cup a_1 = 1 \\ b_1 \cup b_2 = a_1 \cup (a_1 + a_2) = a_1 \cup a_1 + a_1 \cup a_2 = 0 \\ b_2 \cup b_2 = (a_1 + a_2) \cup (a_1 + a_2) = a_1 \cup a_1 + a_2 \cup a_2 = 1 \\ b_i \cup b_{i+1} = a_i \cup a_{i+1} = 1 \text{ for } i \geq 3 \\ b_i \cup b_j = 0 \text{ otherwise} \end{cases} .$$

Therefore, the new basis $\{b_1, \dots, b_{2k}\}$ of $H^1(G, \mathbb{F}_p)$ induces the following description of the relevant colon ideals.

1. The subset $Y \subseteq X$ is a singleton $\{b_i\}$.
   Then the only colon ideal involved is

$$(0)\colon b_i = \begin{cases} (\{b_j : j \neq 1\}) & i = 1 \\ (\{b_j : j \neq 2\}) & i = 2 \\ (\{b_j : j \neq i+1\}) & i > 1 \text{ odd} \\ (\{b_j : j \neq i-1\}) & i > 2 \text{ even.} \end{cases}$$

   And in the same way as previously, in all of the above, $(0) : b_i$ is generated by a subset of X.

2. The subset $Y \subseteq X$ contains at least 2 elements.
   Identical to Proposition 6.2.1. □

Corollary 6.2.6. *Suppose that $G_{\mathbb{F}}(p)$ is a Demushkin group on $d = 2k$ generators, $k \in \mathbb{N} \setminus \{0\}$ with invariant $q = 2$. Then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is strongly Koszul.*

6.3 Direct sum

The main goal here is to prove that the direct sum of two strongly Koszul algebras is also a strongly Koszul algebra.

Proposition 6.3.1. *Let A and B be strongly Koszul algebras with respect to the homogeneous systems $X_A = \{a_1, \dots, a_c\}$ and $X_B = \{b_1, \dots, b_d\}$ respectively. Then the direct sum $A \sqcap B$ is strongly Koszul with respect to the system $X_A \cup X_B$.*

Proof. The key idea is that every element $x \in A \sqcap B$ has a unique decomposition $x = x_A + x_B$ with $x_A \in A$ and $x_B \in B$, and that elements of A annihilate x_B and vice versa. We show the statement by distinguishing between the various types of colon ideals of $A \sqcap B$.

1. An ideal of $A \sqcap B$ of the shape $I = (a_{i_1}, \dots, a_{i_{k-1}}) : a_{i_k}$ coincides with $(I_A^c)^e + (B_+)^e$. By hypothesis, I_A^c is generated, as an ideal of A, by a subset Y_A of X_A, so $I = (Y_A \cup X_B)$. An analogous argument works for an ideal of $A \sqcap B$ of the shape $(b_{i_1}, \dots, b_{i_{k-1}}) : b_{i_k}$.

2. We now consider the case where a colon ideal of $A \sqcap B$ consists of elements from both ordered systems. Let I be an ideal of $A \sqcap B$ of the form $I = (a_{i_1}, \dots, a_{i_h}, b_{j_1}, \dots, b_{j_{k-1}}) : b_{j_k}$. Then I coincides with $(A_+)^e + (((b_{j_1}, \dots, b_{j_{k-1}}) : b_{j_k})^c_B)^e$. Since the ideal $((b_{j_1}, \dots, b_{j_{k-1}}) : b_{j_k})^c_B$ is generated by a subset Y_B of X_B, as an ideal of B, we deduce that $I = (X_A \cup Y_B)$. An analogous argument works for an ideal of $A \sqcap B$ of the shape $I = (a_{i_1}, \dots, a_{i_{h-1}}, b_{j_1}, \dots, b_{j_k}) : a_{i_h}$. □

Corollary 6.3.2. *Let G_1 and G_2 be finitely generated free or Demushkin pro-p-groups. Then $H^\bullet(G_1 * G_2, \mathbb{F}_p)$ is a strongly Koszul algebra.*

Proof. The claim follows easily by Theorem 5.3.4 and Propositions 6.1.1, 6.2.1, 6.2.3 and 6.2.5. □

6.4 Twisted extension

We lastly show that the twisted extension of a strongly Koszul algebra is again strongly Koszul.

Proposition 6.4.1. *Let A be a strongly Koszul algebra with respect to the system of homogeneous generators $X_A = \{a_1, \dots, a_d\}$ and let $\{x_1, \dots, x_m\}$, $m \in \mathbb{N}$, be a set of elements not in A. Then the twisted extension*

$$A(0; x_1, \dots, x_m) = A \otimes^{-1} \bigwedge(x_1, \dots, x_m)$$

is strongly Koszul with respect to the system $\{a_1, \dots, a_d, x_1, \dots, x_m\}$.

Proof. Since $A(0; x_1, \dots, x_m) = (((A(0; x_1))(0; x_2)) \dots)(0; x_m)$, it is enough to prove the claim for the algebra

$$A(0; x) = \frac{\mathbb{T}(\mathrm{span}_{\mathbb{F}_p}(X_A \cup \{x\})}{(R \cup \{x^2, x a_i + a_i x : a_i \in X_A\})},$$

where R denotes the relator system of A. The only relation between x and any element of A_+ is skew-commutativity. As a consequence, there are only two cases to be treated.

1. If in A $(a_{i_1}, \dots, a_{i_k}) : a_{i_{k+1}} = (a_{j_1}, \dots, a_{j_r})$, then in $A(0; x)$

$$(a_{i_1}, \dots, a_{i_k}, x) : a_{i_{k+1}} = (a_{j_1}, \dots, a_{j_r}, x).$$

2. $(a_{i_1}, \ldots, a_{i_k}, x) : x = (a_{i_1}, \ldots, a_{i_k}, x)$.

In fact, any element $b \in A(t; x)$ is a sum $p + xq$ with $p, q \in A$ and the summands p and xq are exactly the homogeneous components of b with respect to the additional grading ($\heartsuit$) before Theorem 5.3.4 in Section 5.3. Since the left hand side colon ideals are homogeneous with respect to the additional grading ($\heartsuit$), an element b belongs to one of these ideals if and only if both p and xq belong to that ideal. □

Corollary 6.4.2. *If G is a finitely generated free or a Demushkin pro-p-group, and $x_1, \ldots, x_m$ are not in $H^\bullet(G, \mathbb{F}_p)$, then $H^\bullet(G, \mathbb{F}_p)(0; x_1, \ldots, x_m)$ is strongly Koszul.*

Theorem 6.4.3. *If G is an elementary type pro-p-group that does not contain an element $a \neq 1$, such that $a^2 = 1$, then $H^\bullet(G, \mathbb{F}_p)$ is strongly Koszul.*

Proof. The statement follows by combining Propositions 6.1.1, 6.2.1, 6.2.3 and 6.2.5, Theorem 5.3.4 with Proposition 6.3.1, and Theorem 5.3.2 with Proposition 6.4.1. □

Corollary 6.4.4. *Let $\mathbb{F}$ be a field that contains a primitive p-th root of unity ζ_p, or $\sqrt{-1} \in \mathbb{F}$ for $p = 2$ and assume that $G_{\mathbb{F}}(p)$ is of elementary type. Then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is strongly Koszul.*

Chapter 7

Groups that satisfy universal Koszulity

In Chapter 6, an illustration of the powerful property of strong Koszulity and its implications to Galois theory was given. However, this was exactly because we were able to describe the basis of the space of topological generators of the given group, and it is not hard to imagine that this is not usually the case. So it is reasonable to look for a property that is more compatible with Galois cohomology and less dependent on the coordinates.

This is the notion of universal Koszulity, which is more natural in the context of Galois cohomology than strong Koszulity; it provides with a Koszul filtration, all of whose ideals are generated in degree 1, allowing us to study a quadratic algebra by "dividing" it in small parts in the most convenient way possible. On the other hand, however, universal Koszulity, due to its basis-free nature.

Similarly to Chapter 6, we show that cohomology of elementary type pro-p-groups is universally Koszul; this time without any further assumptions on the case that $p = 2$. We do this by demonstrating that the cohomology of finitely generated free and Demushkin pro-p-groups, as well as their direct sum and twisted extensions are universally Koszul.

7.1 Free pro-p-groups

The goal of this Section is to show that the Galois cohomology algebra of a free pro-p-group is universally Koszul. Note that since no Galois-theoretic information is needed here, we can assume that G is a free pro-p-group, for any prime p.

Proposition 7.1.1. *Suppose that G is a finitely generated free pro-p-group. Then $H^\bullet(G, \mathbb{F}_p)$ is universally Koszul.*

Proof. Since the cohomology is concentrated in degrees 0 and 1, the product of any two elements of positive degree is 0. This means that if

$$I \neq H^\bullet(G, \mathbb{F}_p)_+ = H^1(G, \mathbb{F}_p),$$

for any arbitrary ideal $I \trianglelefteq H^\bullet(G, \mathbb{F}_p)$, then for all $x \in H^\bullet(G, \mathbb{F}_p)_1 \setminus I$, we get that

$$I : x = H^\bullet(G, \mathbb{F}_p)_+ = H^1(G, \mathbb{F}_p).$$

The result follows from condition (ii) of Proposition 5.2.8. □

7.2 Demushkin groups

Similarly to Section 6.2, we show that the cohomology algebra of a Demushkin group is universally Koszul. In addition to assuming the more generalized assumption that p is any prime number, another instance of the flexibility of universal against strong Koszulity is demonstrated here: the fact that we need not take into account the several forms of the presentation of a Demushkin group allows us to only distinguish between the cases where it is infinite or finite.

Proposition 7.2.1. *Suppose that G is an infinite Demushkin pro-p-group. Then $H^\bullet(G, \mathbb{F}_p)$ is universally Koszul.*

Proof. Let $I \in \mathcal{L}(H^\bullet(G, \mathbb{F}_p)) \setminus \{H^\bullet(G, \mathbb{F}_p)_+\}$ and let $x \in (H^\bullet(G, \mathbb{F}_p))_1 \setminus I$. Let us first address the case $I = (0)$. The ideal $(0) : x$ is made of all solutions to the equation $ax = 0$ in one variable $a \in H^\bullet(G, \mathbb{F}_p)$. This equation has a solution in $H^\bullet(G, \mathbb{F}_p)_1$ for any x, as can clearly be seen, for example, writing a and x as $H^\bullet(G, \mathbb{F}_p)$-linear combinations of an alternating basis of $H^\bullet(G, \mathbb{F}_p)_1$. So $(0) : x \neq (0)$, whence $H^\bullet(G, \mathbb{F}_p)_1((0) : x) \supseteq H^\bullet(G, \mathbb{F}_p)_2$. For a general ideal I, we have that $(0) : x \subseteq I : x$, so again $H^\bullet(G, \mathbb{F}_p)_1(I : x) \supseteq H^\bullet(G, \mathbb{F}_p)_2$.

But in general, for any graded algebra A generated in degree 1 and for any ideal $J \trianglelefteq A$ with $A_1 J \supseteq A_2$, we have that $J = AJ_1$. In fact, since A is generated in degree 1,

$$A_{n+1} = A_{n-1}A_2 \subseteq A_{n-1}A_1 J = A_n J,$$

for all $n \in \mathbb{N}$. Now, if a is a homogeneous element of J_{n+1} for some $n \in \mathbb{N}$, then $a \in A_{n+1} \subseteq A_n J$ and so, taking the degree of a into account, $a \in A_n J_1$.

This shows that condition (ii) of Proposition 5.2.8 is satisfied. □

Proposition 7.2.2. *The cohomology $H^\bullet(C_2, \mathbb{F}_2)$ of the cyclic group of order 2 is universally Koszul.*

Proof. In this case $H^\bullet(G, \mathbb{F}_2) = \mathbb{F}_2[t]$ is a free algebra on one generator. Therefore, for all $I \in \mathcal{L}(H^\bullet(G, \mathbb{F}_2)) \setminus \{H^\bullet(G, \mathbb{F}_2)_+\}$ and all $x \in H^\bullet(G, \mathbb{F}_2)_1 \setminus I$, $I : x = (0)$. The result follows from condition (ii) of Proposition 5.2.8. □

7.3 Direct sum

Proposition 7.3.1. *Let A and B be universally Koszul algebras. Then the direct sum $A \sqcap B$ is universally Koszul.*

Proof. The proof is almost verbatim the same as for the commutative case (cf. [Con00, Lemma 1.6(3)]). Consider an ideal $I \in \mathcal{L}(A \sqcap B) \setminus \{(A \sqcap B)_+\}$ and let $x \in (A \sqcap B)_1 = A_1 \oplus B_1$. We can then express I and x as

$$I = (a_1 + b_1, \dots, a_n + b_n), \text{ and } x = a + b,$$

with $a_i, a \in A_1$ and $b_i, b \in B_1$. Set $J_A = (a_1, \dots, a_n)$, $J_B = (b_1, \dots, b_n)$ and $J = J_A^e + J_B^e = J_A + J_B \trianglelefteq A \sqcap B$, since $J_A, J_B \trianglelefteq A \sqcap B$. Then $I \subseteq J$. Moreover, if $c \in J_i$ for $i \geq 2$, then $c \in I_i$, because A_+ annihilates B_+ and vice versa.

We claim that

$$I : (x) = (J : (x)) \cap (A \sqcap B)_+.$$

To see this, let $c \in A \sqcap B$ be such that $xc \in I$. Note that the latter implies that $x \in I$. Then $cx \in J$, as $I \subseteq J$, and so $c \in J : (x)$, and $c \in (A \sqcap B)_+$. This gives us the inclusion $I : (x) \subseteq (J : (x)) \cap (A \sqcap B)_+$. Reversely, $c \in J : (x)$ and $c \in (A \sqcap B)_+$ imply that

$$cx \in \oplus_{i \geq 2} J_i = \oplus_{i \geq 2} I_i,$$

so $c \in I : (x)$.

As a consequence, if $x \in J$, then $I : (x) = (A \sqcap B)_+ \in \mathcal{L}(A \sqcap B)$; otherwise, $I : (x) = J : (x)$ and there are three cases to consider.

1. If $a \notin J_A$ and $b \notin J_B$, then $J : (x) = (J_A :_A (a))^e + (J_B :_B (b))^e$. Indeed, if $c \in J : (x)$, then $cx \in J_A + J_B = J$. Writing $c = c_A + c_B$ with $c_A \in A$ and $c_B \in B$, we get that $cx = c_A a + c_B b$ and that $c_A a \in J_A$, $c_B b \in J_B$. Hence, $c \in (J_A :_A (a))^e + (J_B :_B (b))^e$. For the reverse, assume that $c = c_A + c_B \in (J_A :_A (a))^e + (J_B :_B (b))^e$; then $c_A a = ca \in J_A$ and $c_B b = cb \in J_B$. Therefore, $cx \in J_A + J_B$, or equivalently $c \in J : (x)$.

2. If $a \in J_A$ and $b \notin J_B$, then $J : x = (A_+)^e + (J_B :_B (b))^e$. In fact, if $c \in J : (x)$, then with the same notation as before, $cx = c_A a + c_B b \in J_A + J_B = J$. Surely, for all $c_A \in A_+$, $c_A a \in J_A$, hence $c_B b \in (J_A + J_B) \cap B = J_B$. This implies that $c \in (A_+)^e + (J_B :_B (b))^e$. The reverse inclusion is obvious.

3. If $a \notin J_A$ and $b \in J_B$, then $J : (x) = (J_A :_A (a))^e + (B_+)^e$. The proof is analogous to the previous case.

In all cases, $I : (x) = J : (x) \in \mathcal{L}(A \sqcap B)$, since $J_A :_A (a), A_+ \in \mathcal{L}(A)$ and $J_B :_B (b), B_+ \in \mathcal{L}(B)$ and the result follows from condition (ii) of Proposition 5.2.8. □

7.4 Twisted extensions

In fact, the preceding Proposition is a specific case of the following more general result.

Proposition 7.4.1. *If $A = \{V, R\}$ is a universally Koszul $\Bbbk$-algebra, then the twisted extension $A(t; x_1, \dots, x_m) = \frac{\mathbb{T}(V \oplus span_{\Bbbk}\{x_1,\dots,x_m\})}{R_A \cup \{x_i^2 = tx_i, x_i a + a x_i :\ 1 \leq i \leq m, a \in A_1\}}$ is universally Koszul.*

Proof. In the same fashion as before, by induction it is enough to prove the statement for the twisted extension $A(t; x)$. We will show that the collection $\mathcal{L}(A(t; x))$ of ideals of $A(t; x)$ generated in degree 1 is a Koszul filtration. Conditions (i) and (ii) of Definition 5.2.6 are satisfied, so it suffices to show that for any $(0) \neq I \in \mathcal{L}(A(t, x))$, there exist $I \neq J \in \mathcal{L}(A(t; x))$ and an element $* \in A(t; x)_1$, such that $I = J + *$ and $J : * \in \mathcal{L}(A(t; x))$. We shall distinguish two cases.

1. Assume that all generators of I lie in A_1.
   Then $I = I_A^e$ for some $(0) \neq I_A \in \mathcal{L}(A)$. Since A is universally Koszul,

there exist $J_a \in \mathcal{L}(A)$ and $a \in A_1 \backslash J$, such that $I_A = J_A + (a)$ and $J_A :_A (a) \in \mathcal{L}(A)$.

Set $J = J_A^e$; then $I = J + (a)_{A(t;x)}$. We claim that $I \neq J$. Indeed, assume that $I = J + (a)_{A(t;x)} = J$. Then, $I_A = J_A + (a)_A$ and so $a \in J_A$, which contradicts the fact that A is universally Koszul. Therefore $I \neq J$ and it only remains to show that $J : (a) \in \mathcal{L}(A(t;x))$. We will show something even stronger, namely that $J : (a) = (J_A :_A (a))^e$.

Let $p + qx \in J : (a)$ be in standard normal form. Then, $(p + qx)a \in J$. However, all elements in J can be uniquely expressed as $\sum_i p_i + q_i x \alpha_i$, where $\{\alpha_i\}$ are a set of generators of J_A, and since the same set generates J as an ideal of $A(t;x)$, $\{\alpha_i\}$ are a set of generators of J. We thus obtain that

$$\begin{array}{rc} (p+qx)a = & \sum_i (p_i + q_i x)\alpha_i \\ pa - qax = & \sum_i p_i\alpha_i - \sum_i q_i\alpha_i x, \end{array}$$

which implies that

$$\begin{cases} pa = \sum_i p_i\alpha_i \\ qa = \sum_i q_i\alpha_i \end{cases}$$

and thus $pa, qa \in J_A$, which means that $p, q \in J_A :_A (a)$. But then, $p + qx \in (J_A : A(a))^e$, which implies that $J : (a) \subseteq (J_A :_A (a))^e$. On the other hand, by construction, all generators of $(J_A : A(a))^e$ belong to $J : (a)$, so the reverse inclusion is straightforward. This deduces the equality $J : (a) = (J_A :_A (a))^e \in \mathcal{L}(A(t;x))$.

2. Assume that at least one generator of I does not belong to A.
We can then write I as

$$I = I_A^e + (x + l),$$

where $I_A \in \mathcal{L}(A)$ and $l \in A_1 \backslash I_A$. Assume that $l = 0$. Then, I takes the form

$$I = I_A^e + (x)$$

and set $J = J_A^e$. Then $I = J + (x)$, and by construction it is easy to see that $I = J + (x) \neq J$. So it only remains to show that $J : (x) \in \mathcal{L}(A(t;x))$. We will instead show that $J : (x) = J + (x + t)$. Then, since $J + (x + t) \in \mathcal{L}(A(t;x))$, we will have shown that $J : (x) \in \mathcal{L}(A(t;x))$.

Let $c = p + qx \in J : (x)$ be in standard normal form. Then, $cx = (p+qx)x \in J$. And since each element in J can be uniquely decomposed into a sum $\sum_i (p_i + q_i x)\alpha_i$, where $\{\alpha_i\}$ is a set of generators of J, $cx = (p + qx)x \in J$ implies

$$\begin{aligned} px + qx^2 = &\quad \textstyle\sum_i (p_i + q_i x)\alpha_i \\ px - qtx = &\textstyle\sum p_i\alpha_i - \sum_i q_i\alpha_i x, \end{aligned}$$

which then implies that $p - qt = \sum_i q_i\alpha_i$, and thus $p, q \in J$. So $p + qx \in J + (t + x)$, which gives us the inclusion $J : (x) \subseteq J + (x + t)$. On the other hand, again, all generators of $J + (x+t)$ belong to $J : (x)$, and thus $J : (x) = J + (x + t) \in \mathcal{L}(A(t; x))$.

If $l \neq 0$, we consider the automorphism of graded algebras

$$\mathscr{m} : A(t; x) \longrightarrow A(t; x)$$

defined as

$$\mathscr{m}(p + zx) = p + q(x - l).$$

Then, $\mathscr{m}$ sends an ideal J to $I^e + (x)$, so the problem reduces to the previous case. □

So, in any case, $J : (x) \in \mathcal{L}(A(t; x))$ and the twisted extension $A(t; x)$ is universally Koszul. □

Combining Propositions 7.1.1, 7.2.1, 7.2.2, 7.3.1 and 7.4.1 we obtain the following

Theorem 7.4.2. *If G is an elementary type pro-p-group, then $H^\bullet(G, \mathbb{F}_p)$ is universally Koszul.*

In particular, regarding to Positselski's Conjecture,

Corollary 7.4.3. *Let $\mathbb{F}$ be a field that contains a primitive p-th root of unity. If $G_{\mathbb{F}}(p)$ is of elementary type, then $H^\bullet(\mathbb{F}, \mathbb{F}_p)$ is universally Koszul.*

Chapter 8

Groups that do not satisfy strong Koszulity

One cannot help but wonder what happens if the assumption $\sqrt{-1} \in \mathbb{F}$ is removed while studying the property of strong Koszulity. As expected, strong Koszulity fails to hold. This Chapter is therefore devoted to groups whose Galois cohomology algebras are not strongly Koszul. Such groups include absolute Galois groups of superpythagorean fields and rigid fields of level two. What really works as a propagation of universal Koszulity is that these algebras are universally Koszul, which really clearly points at the direction of universal Koszulity, as a means of resolving the Steinberg relations.

8.1 Level of fields

Here we deal with fields that do not contain $\sqrt{-1}$. There is a plethora of such fields, however our focus restricts to fields where -1 can either never be written as a sum of squares, or it can be written as a sum of exactly two squares. As Proposition 8.2.3 below shows, dropping this assumption $\sqrt{-1} \in \mathbb{F}$, makes the building of strong Koszulity collapsing.

Definition 8.1.1. [Lam05] The *level* (*stufe*) of a field $\mathbb{F}$, denoted by $s(\mathbb{F})$, is the smallest positive integer k such that -1 is a sum of k squares in $\mathbb{F}$, provided such integer exists, and 0 otherwise. It will be denoted $s(\mathbb{F})$.

Before we proceed, there are some remarks on the level of a field we need to make.

1. If $\mathbb{F}$ is a field of characteristic $\operatorname{char}\mathbb{F} = 2$, then $s(\mathbb{F}) = 1$, as in this case -1 is itself a square.

2. If $\mathbb{F}$ is a field of characteristic $\operatorname{char}\mathbb{F} \neq 2$, then $s(\mathbb{F}) = 0$ if and only if $\mathbb{F}$ is a formally real field. Otherwise, it is a power of 2 (see [Lam05]).

3. The level of a field $\mathbb{F}$ is strongly connected to the value set of quadratic forms over $\mathbb{F}$. Recall from Section 1.4 that the *value set* of a quadratic form ϕ over $\mathbb{F}$ is defined as

$$D_{\mathbb{F}}(\phi) = \{[a] \in \mathbb{F}^\times/\mathbb{F}^{\times 2} : a \text{ is represented by } \phi\},$$

where $[a]$ denotes the image of $a \in \mathbb{F}^\times$ in $\mathbb{F}^\times/\mathbb{F}^{\times 2}$.

Definition 8.1.2. We say that a field $\mathbb{F}$ is 2*-rigid* if, for all $a \in \mathbb{F}$ such that $[a] \neq 1, [-1]$, the value set of the quadratic form $\langle 1, a\rangle = X^2 + aY^2$ is included in $\{[1], [a]\} \subseteq \mathbb{F}^\times/\mathbb{F}^{\times 2}$.

By [War78, Theorem 1.9, Proposition 1.1], the level of a 2-rigid field $\mathbb{F}$ is either 0, 1 or 2. The case $s(\mathbb{F}) = 1$ corresponds to the condition that $\sqrt{-1} \in \mathbb{F}$, while $s(\mathbb{F}) = 0$ is equivalent to $\mathbb{F}$ being superpythagorean.

8.2 Superpythagorean fields

Maximal pro-2-quotients of absolute Galois groups of superpythagorean fields form the first family of groups whose cohomology algebras are not strong Koszul, although still Koszul, as we shall see below.

Let $\mathbb{F}$ be a superpythagorean field with $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} = d < \infty$. Let $\{[-1], [a_2], \ldots, [a_d]\}$ be an $\mathbb{F}_2$-basis of $\mathbb{F}^\times/\mathbb{F}^{\times 2}$ and denote the maximal pro-2 quotient of $\mathbb{F}$ by $\mathbb{F}(2)$. Then by [Wad83], a presentation of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is given as

$$H^\bullet(\mathbb{F}(2), \mathbb{F}_2) = \mathbb{F}_2 \langle t, \alpha_2, \ldots, \alpha_d : \alpha_j\alpha_i = \alpha_i\alpha_j, \alpha_i t = t\alpha_i, \alpha_i\alpha_i = t\alpha_i\rangle,$$

where $t = \ell([-1])$ and $\alpha_i = \ell([a_i])$ and the product between two generators is the cup product.

For each $n \geq 1$, we set

$$B_n = \{t^{n-r}\alpha_{i_1} \cdots \alpha_{i_r} : 0 \leq r \leq d,\ i_1 < \ldots < i_r\}.$$

Then the set B_n forms a basis of $H^n(\mathbb{F}(2), \mathbb{F}_2)$ for each $n \geq 1$, by [EL72, Theorem 5.13(2)] and [Voe03, Corollary 7.5].

Proposition 8.2.1. *For a superpythagorean field $\mathbb{F}$ with $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} < \infty$, $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is PBW.*

Proof.

We are going to apply the Rewriting Method of Section 4.3. Consider the degree-lexicographic order on the monomials of $\mathbb{T}\langle t, \alpha_2, \dots, \alpha_d\rangle$ induced by the total order $t < \alpha_2 < \cdots < \alpha_d$. Then a normalized basis for the space of relations of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is

$$\{\alpha_j\alpha_i - \alpha_i\alpha_j : 2 \le i < j \le d\} \cup \{\alpha_i t - t\alpha_i : 2 \le i \le d\} \cup \{\alpha_i\alpha_i - t\alpha_i : 2 \le i \le d\}.$$

The corresponding critical monomials are

1. $\alpha_i\alpha_i\alpha_i$, with $2 \le i \le d$;
2. $\alpha_j\alpha_j\alpha_i$, with $2 \le i < j \le d$;
3. $\alpha_j\alpha_i\alpha_i$, with $2 \le i < j \le d$;
4. $\alpha_i\alpha_i t$, with $2 \le i \le d$;
5. $\alpha_k\alpha_j\alpha_i$, with $2 \le i < j < k \le d$; and
6. $\alpha_j\alpha_i t$, with $2 \le i < j \le d$.

We shall show that all the critical monomials above are confluent.

Type 1.

$$\begin{tikzcd}
 & \alpha_i\alpha_i\alpha_i \arrow[ddl] \arrow[dr] & \\
 & & \alpha_i t\alpha_i \arrow[dll] \\
t\alpha_i\alpha_i \arrow[d] & & \\
tt\alpha_i\ ; & &
\end{tikzcd}$$

Type 2.

$$\begin{tikzcd}
 & \alpha_j\alpha_j\alpha_i \arrow[dl] \arrow[dr] & \\
t\alpha_j\alpha_i \arrow[dddr] & & \alpha_j\alpha_i\alpha_j \arrow[d] \\
 & & \alpha_i\alpha_j\alpha_j \arrow[d] \\
 & & \alpha_i t\alpha_j \arrow[dl] \\
 & t\alpha_i\alpha_j & ;
\end{tikzcd}$$

Type 3.

$$\begin{tikzcd}
 & \alpha_j\alpha_i\alpha_i \arrow[dl] \arrow[dr] & \\
\alpha_i\alpha_j\alpha_i \arrow[d] & & \alpha_j t\alpha_i \arrow[d] \\
\alpha_i\alpha_i\alpha_j \arrow[dr] & & t\alpha_j\alpha_i \arrow[dl] \\
 & t\alpha_i\alpha_j & ;
\end{tikzcd}$$

Type 4.

$$\begin{tikzcd}
 & \alpha_i\alpha_i t \arrow[dl] \arrow[dr] & \\
t\alpha_i t \arrow[ddr] & & \alpha_i t\alpha_i \arrow[d] \\
 & & t\alpha_i\alpha_i \arrow[dl] \\
 & tt\alpha_i & ;
\end{tikzcd}$$

Type 5.

$$\begin{tikzcd}
 & \alpha_k\alpha_j\alpha_i \arrow[dl] \arrow[dr] & \\
\alpha_j\alpha_k\alpha_i \arrow[d] & & \alpha_k\alpha_i\alpha_j \arrow[d] \\
\alpha_j\alpha_i\alpha_k \arrow[dr] & & \alpha_i\alpha_k\alpha_j \arrow[dl] \\
 & \alpha_i\alpha_j\alpha_k & ;
\end{tikzcd}$$

Type 6.

$$\begin{tikzcd}
 & \alpha_j\alpha_i t \arrow[dl] \arrow[dr] & \\
\alpha_i\alpha_j t \arrow[d] & & \alpha_j t\alpha_i \arrow[d] \\
\alpha_i t\alpha_j \arrow[dr] & & t\alpha_j\alpha_i \arrow[dl] \\
 & t\alpha_i\alpha_j & .
\end{tikzcd}$$

Thus all the critical monomials of three terms are confluent. By Theorem 4.2.3 we obtain that all critical monomials of any number of terms are confluent and thus by Corollary 4.3.6 of Bergman's Diamond Lemma, we get that $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is PBW, as wanted. □

But, $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is even more than PBW.

But, this Galois cohomology has an even stronger property, namely, it is a universally Koszul algebra, as the result below shows.

Proposition 8.2.2. *If* $\mathbb{F}$ *is a superpythagorean field with* $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} < \infty$, *then* $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ *is universally Koszul.*

Proof. Note that $H^\bullet(\mathbb{F}(2), \mathbb{F}_2) = \mathbb{F}_2[t](t; \alpha_1, \ldots, \alpha_d)$. Since the algebra $\mathbb{F}_2[t]$ is universally Koszul, Proposition 7.4.1 implies that the twisted extension $\mathbb{F}_2[t](t; \alpha_1, \ldots, \alpha_d)$ is universally Koszul, and thus $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is universally Koszul. □

We conclude with the next

Proposition 8.2.3. *Let* $\mathbb{F}$ *be a superpythagorean field with* $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} = d \geq 3$. *Then* $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ *is not strongly Koszul.*

Proof.

First, we claim that for all $a \in F^\times$, with $[a] \neq [1], [-1]$, the colon ideal $(0)\colon \ell(a) = \langle \ell(-a) \rangle$. This has already been noted in the proof of Proposition 10.3.2 as Equation (♠) in the case $\ell([a]) = \alpha_i$. Since the system of generators $\{t, \alpha_1, \ldots, \alpha_d\}$ of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is arbitrary, it holds in complete generality. In fact, the inclusion $\langle \ell([-a]) \subseteq (0)\colon \ell([a]) \rangle$ is a direct consequence of the Steinberg relation. For the reverse, choose a $\mathbb{F}_2$-basis $\{[-1], [a_2], \ldots, [a_d]\}$ of $\mathbb{F}^\times/(\mathbb{F}^\times)^2$ with $[a_2] = [-a]$. Keeping the notation of Proposition 8.2.1, recall that $\ell([a]) = t + (\alpha_2)$ in $H^1(\mathbb{F}(2), \mathbb{F}_2)$. Therefore, for all $n \geq 1$, the cup product between $\ell([a])$ and a typical element of B_n is

$$\ell([a])\chi = t^{n-r+1}\alpha_{i_1} \ldots \alpha_{i_r} + (\alpha_2)t^{n-r}\alpha_{i_1} \ldots \alpha_{i_r}.$$

Thus, there is no way for an element not in $\langle \ell([-a]) \rangle$ to be annihilated by $\ell([a])$. An element $\chi \in H^n(\mathbb{F}(2), \mathbb{F}_2)$ belongs to $(0)\colon \ell([a])$ if and only if, in the decomposition of χ as linear combination of B_n, only the basis vectors containing the factor α_2 have a nonzero coefficient. But this is equivalent to the fact that $\chi \in \langle \ell([-a]) \rangle$. This proves the claim.

Since by assumption $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} = d \geq 3$, we obtain that any basis of $H^1(\mathbb{F}(2), \mathbb{F}_2)$ contains at least two elements, say $\ell([a]), \ell([b])$, such that $\ell([-1]), \ell([a]), \ell([b]), \ell([-a]), \ell([-b])$ are all distinct.

Assume that $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is strongly Koszul with respect to a minimal system of homogeneous generators $X = \{u_1, \ldots, u_n\} \supseteq \{\ell([a]), \ell([b])\}$. Applying the claim to the colon ideals $(0)\colon \ell([a])$ and $(0)\colon \ell([b])$, we get that

$$X \supseteq \{\ell([a]), \ell([b]), \ell([-a]), \ell([-b])\}.$$

But then the system X is not minimal, as

$$\ell([a]) + \ell([b]) + \ell([-a]) + \ell([-b]) = 0 \in H^1(\mathbb{F}(2), \mathbb{F}_2),$$

which is a contradiction. Thus $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is not strongly Koszul. □

8.3 Rigid fields of level two

Following the same techniques and methods as in Section 8.2, the aim is to show that the cohomology of a rigid field os level 2 is not strongly Koszul as well. In the same fashion as before, this cohomology algebra is PBW and admits a Koszul filtration, but strong Koszulity fails under the assumption that the square class of the field contains at least three representatives.

Therefore, assume that $\mathbb{F}$ is a 2-rigid field of level $s(\mathbb{F}) = 2$, and let $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} = d < \infty$. Let $\{[-1], [a_2], \ldots, [a_d]\}$ be a $\mathbb{F}_2$-basis of $\mathbb{F}^\times/\mathbb{F}^{\times 2}$. We follow the same notation as before, that is, $t = \ell([-1])$, $\alpha_i = \ell([a_i])$ and the cup product between two basis elements is omitted. Then a presentation of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is given by

$$H^\bullet(\mathbb{F}(2), \mathbb{F}_2) = \langle t, \alpha_2, \ldots, \alpha_d : \alpha_j\alpha_i = \alpha_i\alpha_j, \alpha_i t = t\alpha_i, \alpha_i\alpha_i = t\alpha_i, tt = 0\rangle .$$

This graded algebra is concentrated in all degrees between 0 and d. Similarly to superpythagorean fields, for all $n \leq d$, we set

$$B_n = \{t^\delta \alpha_{i_1} \ldots \alpha_{i_{n-\delta}} : \delta = 0, 1,\ i_1 < \cdots < i_n - \delta\}.$$

The set B_n forms a $\mathbb{F}_2$-basis of $H^n(\mathbb{F}(2), \mathbb{F}_2)$.

Proposition 8.3.1. *If $\mathbb{F}$ is a 2-rigid field of level $s(\mathbb{F}) = 2$ and $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} < \infty$, then $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is PBW.*

Proof. Similarly to the proof of Proposition 8.2.1, consider the degree-lexicographic order on the monomials of $\mathbb{T}\langle t, \alpha_2, \ldots, \alpha_d\rangle$ induced by the total order $t < \alpha_2 < \cdots < \alpha_d$. Then a normalized basis for the space of relations of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is

$$\{\alpha_j\alpha_i - \alpha_i\alpha_j,\ \alpha_i t - t\alpha_i,\ \alpha_i\alpha_i - t\alpha_i : 2 \leq i < j \leq d\} \cup \{tt\}.$$

It is not hard to see that the six types of monomials introduced in the proof of Proposition 8.2.1 are again critical monomials. In addition, there are two new types of them:

1'. ttt; and

3'. $\alpha_i tt$, with $2 \leq i \leq d$.

We will use the Rewriting Method of Section 4.3 to show that all these critical monomials are confluent.

Type 1.

$$\begin{tikzcd}
 & \alpha_i\alpha_i\alpha_i \arrow[ddl] \arrow[dr] & \\
 & & \alpha_i t\alpha_i \arrow[dll] \\
t\alpha_i\alpha_i \arrow[d] & & \\
tt\alpha_i \arrow[d] & & \\
0\,; & &
\end{tikzcd}$$

Type 1'.

$$\begin{tikzcd}
ttt \arrow[d, bend right] \arrow[d, bend left] & \\
0 & ;
\end{tikzcd}$$

Type 2.

$$\begin{tikzcd}
 & \alpha_j\alpha_j\alpha_i \arrow[dl] \arrow[dr] & \\
t\alpha_j\alpha_i \arrow[dddr] & & \alpha_j\alpha_i\alpha_j \arrow[d] \\
 & & \alpha_i\alpha_j\alpha_j \arrow[d] \\
 & & \alpha_i t\alpha_j \arrow[dl] \\
 & t\alpha_i\alpha_j & ;
\end{tikzcd}$$

Type 3.

$$\begin{tikzcd}
 & \alpha_j\alpha_i\alpha_i \arrow[dl] \arrow[dr] & \\
\alpha_i\alpha_j\alpha_i \arrow[d] & & \alpha_j t\alpha_i \arrow[d] \\
\alpha_i\alpha_i\alpha_j \arrow[dr] & & t\alpha_j\alpha_i \arrow[dl] \\
 & t\alpha_i\alpha_j & ;
\end{tikzcd}$$

Type 3'.

$$\begin{tikzcd}
 & \alpha_i tt \arrow[dl] \arrow[dddr] & \\
t\alpha_i t \arrow[d] & & \\
tt\alpha_i \arrow[drr] & & \\
 & & 0\,;
\end{tikzcd}$$

Type 4.

$$\begin{tikzcd}
 & \alpha_i\alpha_i t \arrow[dl] \arrow[dr] & \\
t\alpha_i t \arrow[ddr] & & \alpha_i t\alpha_i \arrow[d] \\
 & & t\alpha_i\alpha_i \arrow[dl] \\
 & tt\alpha_i \arrow[d] & \\
 & 0 & ;
\end{tikzcd}$$

Type 5.

$$\begin{tikzcd}
 & \alpha_k\alpha_j\alpha_i \arrow[dl] \arrow[dr] & \\
\alpha_j\alpha_k\alpha_i \arrow[d] & & \alpha_k\alpha_i\alpha_j \arrow[d] \\
\alpha_j\alpha_i\alpha_k \arrow[dr] & & \alpha_i\alpha_k\alpha_j \arrow[dl] \\
 & \alpha_i\alpha_j\alpha_k & ;
\end{tikzcd}$$

Type 6.

$$\begin{tikzcd}
 & \alpha_j\alpha_i t \arrow[dl] \arrow[dr] & \\
\alpha_i\alpha_j t \arrow[d] & & \alpha_j t\alpha_i \arrow[d] \\
\alpha_i t\alpha_j \arrow[dr] & & t\alpha_j\alpha_i \arrow[dl] \\
 & t\alpha_i\alpha_j & .
\end{tikzcd}$$

So every critical monomial with three terms is confluent. By Theorem 4.2.3, we obtain that every critical monomial in any number of terms is confluent. Thus, by Corollary 4.3.6 we get that $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is PBW. □

Moreover,

Proposition 8.3.2. *If $\mathbb{F}$ is a 2-rigid field of level $s(\mathbb{F}) = 2$, such that $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} < \infty$, then $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is universally Koszul.*

Proof. As before, we can identify $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ with the twisted extension $\bigwedge_{\mathbb{F}_2}(t)(t; \alpha_1, \dots, \alpha_d)$. Since the algebra $\bigwedge_{\mathbb{F}_2}(t)$ is universally Koszul, we conclude using Proposition 7.4.1 that $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is universally Koszul as well. □

We finally conclude with the following

Proposition 8.3.3. *Let* $\mathbb{F}$ *be a 2-rigid field of level* $s(\mathbb{F}) = 2$ *and assume that* $\dim_{\mathbb{F}_2} \mathbb{F}^\times/\mathbb{F}^{\times 2} = d \geq 3$. *Then* $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ *is not strongly Koszul.*

Proof. Virtually identical to that of Proposition 8.2.3. □

Chapter 9

Unconditional results

In Chapter 5 we presented the Bloch-Kato and the Milnor Conjecture and established the relationship between the small Milnor K-theory and Galois cohomology. Here, we take a look at another aspect. In particular, we focus on the relationship between the small Milnor K-theory and the graded Witt ring over a field.

Let $\mathbb{F}$ be a field of characteristic $\operatorname{char}\mathbb{F} \neq 2$ and as. In [Mil70], J. Milnor observed the connection between $K^M_\bullet\mathbb{F}/2$, $H^\bullet(\mathbb{F}, \mathbb{F}_2)$ and $\mathrm{gr}W\mathbb{F}$. These objects are related via the following graded homomorphisms

$$\begin{tikzcd}
& K^M_\bullet\mathbb{F}/2 \arrow[dl, "\nu_\bullet"'] \arrow[dr, "h_\bullet"] & \\
\mathrm{gr}W\mathbb{F} \arrow[rr, "e_\bullet"] & & H^\bullet(\mathbb{F}, \mathbb{F}_2).
\end{tikzcd}$$

Milnor proved the Milnor Conjectures under some special circumstances. The map $e_\bullet$ was shown to be was shown to be an isomorphism by the work of D. Orlov, A. Vishik and V. Voevodsky in [OVV07]. We can thus use our knowledge on the $K^M_\bullet\mathbb{F}/2$ to obtain a description of the graded Witt ring $\mathrm{gr}W\mathbb{F}$ over the field $\mathbb{F}$.

On the other hand, there have been several attempts to understand the structure of $W\mathbb{F}$ within its own terms. On this wise, the aim was to encode the abstract ring-theoretic properties of $W\mathbb{F}$ into a set of axioms. Having this in mind, M. Marshall in [Mar80] defined a unified class of rings that is flexible enough in order to describe several families of Witt rings, including the traditional Witt rings of quadratic forms over $\mathbb{F}$. This general class is called the class of abstract Witt rings.

We start by building the theory of this class. So, the first Section is devoted to the discussion of the most fundamental properties of abstract Witt rings. This exposition contains only the minimum material required, so it is far from thorough. Details on the definition of abstract Witt rings and further properties of them can be found in [Mar80]. For further reading on the decomposition of such rings and operations of two such objects, we refer to [Kul79] and [Kul85]. Finally, the Elementary Type Conjectures and the only partial results up to now can be found in [CM82] and [Mar80].

The little progress to a solution of the Elementary Type Conjectures amounts to the many factors that dictate its complexity, the square class number of the associated field and the number of quaternion algebras over it to name a few.

We have seen in Section 1.4 that passing from the Witt ring to the associated graded object usually clarifies the situation. Guided by this, we construct the graded abstract Witt ring. Once this has been established, we proceed to our goal, which is to prove the analogues of Theorems 5.3.2 and 5.3.4. This gives a new insight to the Elementary Type Conjectures.

9.1 Abstract Witt rings

The first step is to define the notion of an abstract Witt ring.

Definition 9.1.1. An *abstract Witt ring* is a pair $W = (R, G)$, such that

(a) R is a commutative ring with 1_R;

(b) G is a subgroup of the multiplicative group $R^\times$ that contains -1, has exponent 2, and generates R as additive group;

(c) the ideal $I_W \trianglelefteq R$, generated by $I_W = \langle a + b : a, b \in G\rangle$ satisfies

AP1 if $a \in G$, then $a \notin I_W$;

AP2 if $a, b \in G$ and $a + b \in I_W^2$, then $a + b = 0$;

WC if $a_1 + \ldots + a_n = b_1 + \ldots + b_n$, $a_i, b_i \in G$, $n \geq 3$, then there exist $a, b, c_3, \ldots, c_n \in G$, such that $a_2 + \ldots + a_n = a + c_3 \ldots + c_n$ and $a_1 + a = b_1 + b$.

We call the idea I_W the *fundamental ideal* of W.

Definition 9.1.2. Let $W_1 = (R_1, G_1)$ and $W_2 = (R_2, G_2)$ be abstract Witt rings. A *morphism of Witt rings* $W_1 \longrightarrow W_2$ is a ring homomorphism $\alpha : R_1 \longrightarrow R_2$, such that $\alpha(G_1) \subseteq \alpha(G_2)$.

Below we present the most basic examples of abstract Witt rings.

Examples.

1. Consider the field $\mathbb{C}$ of complex numbers. Then the trivial Witt ring $W\mathbb{C}$ is an abstract Witt ring, with all the associated elements being trivial.

2. If $\mathbb{F}$ is a local field, then $W\mathbb{F}$ is an abstract Witt ring.

3. In general, the classical Witt ring of quadratic forms over a field $\mathbb{F}$ of characteristic $\operatorname{char}\mathbb{F} \neq 2$ is an abstract Witt ring. To see this, note that $R = W\mathbb{F}$ is a commutative unital ring; G is the group $\mathbb{F}^\times/\mathbb{F}^{\times 2}$ of square classes; and I_W is the fundamental ideal I generated by even dimensional quadratic forms. The axioms AP1 and AP2 appearing in the definition above are nothing else but two specific instances of the *Arason-Pfister properties*

$$\text{APk}: \text{ if } a_1 + \ldots + a_n \in I^k \text{ and } n < 2^k, \text{ then } a_1 + \ldots + a_n = 0.$$

   At last, WC translates to the Witt Cancellation Theorem 1.4.1.

Our study concerns Galois-theoretic information. A question, therefore, arising in a natural way from this newly introduced vocabulary is whether it can be used as a means to achieving our goal. For this, we would like to distinguish between objects of the family of abstract Witt rings that come from the quadratic form theory and the more general objects.

Definition 9.1.3. An abstract Witt ring (R, G) is called *realizable* if there is a field $\mathbb{F}$ of characteristic $\operatorname{char}\mathbb{F} \neq 2$, such that $R \cong W\mathbb{F}$ as rings and $G \cong \mathbb{F}^\times/\mathbb{F}^{\times 2}$ as groups. We say that an abstract Witt ring (R, G) is *finitely generated* if $\#G < \infty$.

9.2 Elementary Operations on abstract Witt rings

In general, the product of two Witt rings is not well defined. The first advantage of the theory of abstract Witt rings is that we can actually speak about the product of two such objects.

Definition 9.2.1. The *direct product* of the abstract Witt rings $W_1 = (R_1, G_1)$ and $W_2 = (R_2, G_2)$, denoted by $W_1 \circledast W_2$, is the abstract Witt ring $W = (R, G)$ with $G = \langle G_1, G_2 \rangle$ as group and R the subring of the ring-theoretic direct product $R_1 \times R_2$ that is additively generated by G.

M. Kula, in [Kul79] and [Kul85], showed that the direct product of two realizable abstract Witt rings is realizable as well.

Theorem 9.2.2 (Kula). *If W_1 and W_2 are two realizable abstract Witt rings, then $W_1 \circledast W_2$ is realizable.*

$W_1 = (R_1, G_1)$ and $W_2 = (R_2, G_2)$ being realizable means that there exist fields $\mathbb{F}$ and $\mathbb{K}$ of characteristic $\operatorname{char}\mathbb{F}, \operatorname{char}\mathbb{K} \neq 2$, such that $R_1 = W\mathbb{F}$, with $G_1 = \mathbb{F}^\times/\mathbb{F}^{\times 2}$ and similarly, $R_2 = W\mathbb{K}$, with $G_2 = \mathbb{K}^\times/\mathbb{K}^{\times 2}$. Thus, the next task would be to describe the way that $W_1 \circledast W_2$ is realizable. From a Galois-theoretic perspective, the direct product of realizable abstract Witt rings corresponds to the free product $G_1 *_p G_2$ of pro-p-groups (cf. also [MPQT, Section 4.2]).

A second operation we can perform on an abstract Witt rings is its group extension, that is, the group ring with an elementary 2-group.

Definition 9.2.3. The *group ring* of an abstract Witt ring $W = (R, G)$ *over the group* $C_2 = \{1, x\}$ of order 2 is $W[x] = (R[C_2], G \times C_2)$.

Assume that W is realizable as the Witt ring over a field $\mathbb{F}$, then $W[x]$ is realizable as the Witt ring over the formal power series field $\mathbb{F}((x))$. From a Galois-theoretic viewpoint, the group ring construction of a realizable Witt ring is the equivalent of the cyclotomic semidirect product $\mathbb{Z}_p \rtimes G$, for a pro-p-group G(cf. [MPQT, Section 4.2]).

The operations direct product and group ring are called the *elementary operations* on abstract Witt rings. The motivation behind the name is justified as follows: given a list of basic abstract Witt rings, we should be able to construct a class of abstract Witt rings using only these two operations.

Example. It can be shown that all Witt rings of fields with square class number ≤ 8 can be obtained by elementary operations from the basic Witt rings $\mathbb{Z} = W\mathbb{R}$, $\mathbb{Z}/2 = W\mathbb{C}$, $\mathbb{Z}/4 = \mathbb{F}_3$ and $\mathbb{L} = W\mathbb{Q}_2$. It can further be shown that another family of basic Witt rings is the family $\mathbb{L}_n$ of degree-n extensions over $\mathbb{Q}_2$. However, the nature of n induces different Witt rings. This means that if $n = 2d$ is even, there are two Witt rings $\mathbb{L}_{2d,1}$ and $\mathbb{L}_{2d,2}$ corresponding to fields of levels 1 and 2 respectively. Therefore, the complete list of basic Witt rings of fields of square class number ≤ 8 is

$$\mathbb{Z},\ \mathbb{Z}/2,\ \mathbb{Z}/4,\ \mathbb{L}_{2k,1},\ \mathbb{L}_{2k,2},\ \mathbb{L}_{\text{odd}}.$$

Extending this idea to abstract Witt rings, we obtain the following

Definition 9.2.4. An abstract Witt ring is said to be of *elementary type* if it is obtained applying finitely many direct products and group ring constructions starting with the basic Witt rings $W\mathbb{C}$ and $W\mathbb{F}$, with $\mathbb{F}$ being a local field.

Weak Elementary Type Conjecture. Every realizable finitely generated abstract Witt ring is of elementary type.

Strong Elementary Type Conjecture. Every finitely generated abstract Witt ring is of elementary type, and hence realizable.

Very few things are known on the Elementary Type Conjectures. Notably,

Theorem 9.2.5. *[CM82] Strong Elementary Type Conjecture holds for abstract Witt rings* (R, G) *with* $\#G \leq 32$.

Theorem 9.2.6. *[Mar80] Weak Elementary Type Conjecture holds for torsion-free abstract Witt rings.*

Finally, in [Cor82], C.M. Cordes classified Witt rings of fields that contain at most four quaternions and showed that these Witt rings satisfy Strong Elementary Type Conjecture.

Theorem 9.2.7. *[Cor82] Strong Elementary Type Conjecture holds for abstract Witt rings* $W \cong W(\mathbb{F})$, $\operatorname{char}\mathbb{F} \neq 2$, *if the number of quaternion algebras supported by* $\mathbb{F}$ *does not exceed* 4.

9.3 Graded abstract Witt rings

The main goal is to form the graded abstract Witt ring and determine the shape of the elementary type operations on such objects. As shown below, the elementary operations extend to the graded objects in a natural manner. We therefore achieve an outlook that provides new insight into one of the most persistent problems in the algebraic theory of quadratic forms.

In the same fashion as the classical setting, to each abstract Witt ring, we can associate a graded object, defined by filtering the powers of fundamental ideas. We have

Definition 9.3.1. Let $W = (R, G)$ be an abstract Witt ring with fundamental ideal I_W. The associated *graded abstract Witt ring* is defined as

$$\mathrm{gr}W = \oplus_{i=0}^{\infty} I_W^i / I_W^{i+1},$$

where by convention $I_W^0 = R$. If $r \in I_W^n$, the corresponding image $\overline{r} = r + I_W^{n+1} \in I_W^n / I_W^{n+1}$ in $\mathrm{gr}W$ is called the *initial form* of r.

Because of the naturality of the grading on $W = (R, G)$, the product of W gives rise to a well-defined product on $\mathrm{gr}W$ as follows: if $r \in I_W^n$ and $s \in I_W^m$, then

$$\overline{r}\overline{s} = \overline{rs} = rs + I_W^{n+m+1} \in I_W^{n+m}/I_W^{n+m+1}.$$

The question that arises from the construction of graded abstract Witt rings is whether the elementary operations are respected by grading. Amazingly, the following results show that grading, viewed as a functor, is functorial.

Proposition 9.3.2. *If $W_1 = (R_1, G_1)$ and $W_2 = (R_2, G_2)$ are two abstract Witt rings, then $\mathrm{gr}(W_1 \circledast W_2) = \mathrm{gr}W_1 \sqcap \mathrm{gr}W_2$.*

Proof. From the direct product construction, we have that $I^n_{W_1 \circledast W_2} = I^n_{W_1} \oplus I^n_{W_2}$ for all $n \geq 1$. Now, for each $n \geq 1$, we consider the map

$$\Phi_n : I^n_{W_1}/I^{n+1}_{W_1} \oplus I^n_{W_2}/I^{n+1}_{W_2} \to (I^n_{W_1} \oplus I^n_{W_2})/(I^{n+1}_{W_1} \oplus I^{n+1}_{W_2}),$$

defined by

$$(a + I^{n+1}_{W_1}, b + I^{n+1}_{W_2}) \mapsto a + b + (I^{n+1}_{W_1} \oplus I^{n+1}_{W_2}).$$

We further define $\Phi_0 = \mathrm{id}_{\mathbb{F}_2}$. It is not hard to check that for Φ_n is an isomorphism of $\mathbb{F}_2$-vector spaces for each $n \geq 0$.

Next, notice that the diagram

$$\begin{tikzcd}
\left(\frac{I^n_{W_1}}{I^{n+1}_{W_1}} \oplus \frac{I^n_{W_2}}{I^{n+1}_{W_2}}\right) \arrow[d, "\Phi_n"] & \times & \left(\frac{I^m_{W_1}}{I^{m+1}_{W_1}} \oplus \frac{I^m_{W_2}}{I^{m+1}_{W_2}}\right) \arrow[d, "\Phi_m"] \arrow[r, "\text{product in } \mathrm{gr}W_1 \sqcap \mathrm{gr}W_2"] & \frac{I^{n+m}_{W_1}}{I^{n+m+1}_{W_1}} \oplus \frac{I^{n+m}_{W_2}}{I^{n+m+1}_{W_2}} \arrow[d, "\Phi_{n+m}"] \\
\frac{I^n_{W_1} \oplus I^n_{W_2}}{I^{n+1}_{W_1} \oplus I^{n+1}_{W_2}} & \times & \frac{I^m_{W_1} \oplus I^m_{W_2}}{I^{m+1}_{W_1} \oplus I^{m+1}_{W_2}} \arrow[r, "\text{product in } \mathrm{gr}(W_1 \circledast W_2)"] & \frac{I^{n+m}_{W_1} \oplus I^{n+m}_{W_2}}{I^{n+m+1}_{W_1} \oplus I^{n+m+1}_{W_2}}
\end{tikzcd}$$

commutes; thus the isomorphisms Φ_n are compatible with the product. Hence $\Phi = \oplus_{n=0}^{\infty} \Phi_n : \mathrm{gr}W_1 \sqcap \mathrm{gr}W_2 \to \mathrm{gr}(W_1 \circledast W_2)$ is an isomorphism of graded algebras. □

We finally show that the group ring operation is also compatible with the grading.

Proposition 9.3.3. *Let $W = (R, G)$ be an abstract Witt ring. Then* $\mathrm{gr}W[x] = (\mathrm{gr}W)(t; y)$*, where* $t = \overline{(1+1)} \in I_{W[x]}/I^2_{W[x]}$ *and* $y = \overline{(1+x)} \in I_{W[x]}/I^2_{W[x]}$.

Proof. First, notice that $1 + x \in I_{W[x]}$. Therefore, $I^n_{W[x]} = I^n_W \oplus (1+x)I^{n-1}_W$. For each $n \geq 1$, we consider the map

$$\Phi_n : I^n_W/I^{n+1}_W \oplus yI^{n-1}_W/I^n_W \to (I^n_W \oplus (1+x)I^{n-1}_W)/(I^{n+1}_W \oplus (1+x)I^n_W),$$

defined by sending

$$(a + I^{n+1}_W, y(b + I^n_W)) \mapsto a + (1+x)b + (I^{n+1}_W \oplus (1+x)I^n_W).$$

Similarly, $\Phi_0 = \mathrm{id}_{\mathbb{F}_2}$. It is not hard to see that for each $n \geq 0$, the map Φ_n is well-defined and an isomorphism of $\mathbb{F}_2$-vector spaces.

Moreover, x has by construction order 2 by construction (see Definition 9.2.3); so $(1+x)(1+x) = (1+1)(1+x)$ in $W[x]$, meaning that $y^2 = ty$ in $\mathrm{gr}W[x]$. This implies that the diagram

$$\begin{tikzcd}
\left(\frac{I^n_W}{I^{n+1}_W} \oplus y\frac{I^{n-1}_W}{I^n_W}\right) \arrow[d, "\Phi_n"'] & \times & \left(\frac{I^m_W}{I^{m+1}_W} \oplus y\frac{I^{m-1}_W}{I^m_W}\right) \arrow[d, "\Phi_m"'] \arrow[r, "\text{product in } \mathrm{gr}W(t;y)"] & \frac{I^{n+m}_W}{I^{n+m+1}_W} \oplus y\frac{I^{n+m-1}_W}{I^{n+m}_W} \arrow[d, "\Phi_{n+m}"'] \\
\frac{I^n_W \oplus (1+x)I^{n-1}_W}{I^{n+1}_W \oplus (1+x)I^n_W} & \times & \frac{I^m_W \oplus (1+x)I^{m-1}_W}{I^{m+1}_W \oplus (1+x)I^m_W} \arrow[r, "\text{product in } \mathrm{gr}W[x]"] & \frac{I^{n+m}_W \oplus (1+x)I^{n+m-1}_W}{I^{n+m+1}_W \oplus (1+x)I^{n+m}_W}
\end{tikzcd}$$

commutes and so, for each n, the maps Φ_n are compatible with the product. Hence $\Phi = \oplus_{n=0}^{\infty} \Phi_n : (\mathrm{gr}W)(t; y) \longrightarrow \mathrm{gr}W[x]$ is an isomorphism of graded algebras. □

Corollary 9.3.4. *Let W be realizable over a field $\mathbb{F}$ of characteristic* $\operatorname{char}\mathbb{F} \neq 2$. *Then* $\mathrm{gr}W[x]$ *is realizable as well.*

9.4 Unconditional results

Combining Theorem 9.2.5 with our results on Galois cohomology, we obtain the following

Proposition 9.4.1. *Let $\mathbb{F}$ be a field of characteristic* $\operatorname{char}\mathbb{F} \neq 2$ *and assume that* $\#\mathbb{F}^\times/\mathbb{F}^{\times 2} \leq 32$. *Then $H^\bullet(\mathbb{F}, \mathbb{F}_2)$ is universally Koszul.*

Theorem 9.2.7 together with our results in Koszulity for Galois cohomology imply that

Proposition 9.4.2. *If $\mathbb{F}$ is a field of characteristic* $\operatorname{char}\mathbb{F} \neq 2$ *that supports at most four quaternions, then $H^\bullet(\mathbb{F}, \mathbb{F}_2)$ is universally Koszul.*

Moreover, we know by Merkurjev's Theorem [Mer81] that the number of quaternion algebras over a field $\mathbb{F}$ of characteristic $\operatorname{char}\mathbb{F} \neq 2$ coincides with the cardinality $\#H^2(\mathbb{F}(2), \mathbb{F}_2)$. Hence, the assumption of Proposition 9.4.2 can be stated in the following equivalent way: $\operatorname{char}\mathbb{F} \neq 2$ and $\dim_{\mathbb{F}_2} H^2(\mathbb{F}(2), \mathbb{F}_2) \leq 2$. However, by 1, this is nothing but the minimal number of generating relations of $G_{\mathbb{F}}(2)$. Therefore, the preceding Proposition can be formulated in the following way.

Proposition 9.4.3. *Let $\mathbb{F}$ be a field of characteristic* $\operatorname{char}\mathbb{F} \neq 2$ *and assume that $G_{\mathbb{F}}(2)$ is finitely generated subject to at most two relations. Then $H^\bullet(\mathbb{F}, \mathbb{F}_2)$ is universally Koszul.*

Note that the Proposition above is a generalization of a result in [Qua].

From a different perspective, a case of the Elementary Type Conjecture has been shown for the $\mathcal{PFR}$ family of pythagorean formally real fields with finitely many square classes.

Definition 9.4.4. [Min86][Jac81][Bec74] Let $\mathbb{F}$ be a field of $\operatorname{char}\mathbb{F} \neq 2$. We say that $\mathbb{F}$ is *pythagorean* if $\mathbb{F}^2 + \mathbb{F}^2 = \mathbb{F}^2$. We say that $\mathbb{F}$ is *formally real* if -1 cannot be written as a sum of squares in $\mathbb{F}$.

Definition 9.4.5. The family $\mathcal{PFR}$ of pythagorean formally real fields is the family consisting of all fields $\mathbb{F}$ of characteristic $\operatorname{char}\mathbb{F} \neq 2$, such that $\mathbb{F}^{\times 2} + \mathbb{F}^{\times 2} = \mathbb{F}^{\times 2}$ and $\mathbb{F}^\times = \mathbb{F}^{\times 2} \cup -\mathbb{F}^{\times 2}$.

Theorem 9.4.6. *The family of maximal pro-2-quotients of absolute Galois groups of fields in the family $\mathcal{PFR}$ has an inductive description in the following way.*

(i) For any euclidean field $\mathbb{F} \in \mathcal{PFR}$, $G_{\mathbb{F}}(2) = C_2$.

(ii) For any two fields $\mathbb{K}_1, \mathbb{K}_2 \in \mathcal{PFR}$, there exists a field $\mathbb{F} \in \mathcal{PFR}$, such that

$$G_{\mathbb{K}_1}(2) *_2 G_{\mathbb{K}_2}(2) \cong G_{\mathbb{F}}(2).$$

(iii) For any field field $\mathbb{K} \in \mathcal{PFR}$ and any finite product $\mathbb{Z}_2^m$, there exists a field $\mathbb{F} \in \mathcal{PFR}$, such that $\mathbb{Z}_2^m \rtimes G_{\mathbb{K}}(2) \cong G_{\mathbb{F}}(2)$, where the action of $G_{\mathbb{K}}(2)$ on $\mathbb{Z}_2^m$ is given by

$$\sigma^{-1} z \sigma = z^{-1}, \textit{ for any } 1 \neq \sigma \in G_{\mathbb{K}}(2);\ \sigma^2 = 1 \textit{ and } z \in \mathbb{Z}_2^m.$$

Moreover, each maximal pro-2-quotient of the absolute Galois group of a $\mathcal{PFR}$ field can be obtained inductively from Galois groups of euclidean fields applying a finite number of operations described in (ii) and (iii).

By Theorem 5.3.2, for any two fields $\mathbb{F}, \mathbb{K} \in \mathcal{PFR}$, we have that

$$H^\bullet(\mathbb{F}(2) *_2 \mathbb{K}(2), \mathbb{F}_2) = H^\bullet(\mathbb{F}(2), \mathbb{F}_2) \sqcap H^\bullet(\mathbb{K}(2), \mathbb{F}_2).$$

Moreover, we know by Theorem 5.3.4 that for any $\mathbb{F} \in \mathcal{PFR}$,

$$H^\bullet(\mathbb{Z}_2^m * \mathbb{F}(2), \mathbb{F}_2) = H^\bullet(\mathbb{F}(2), \mathbb{F}_2)(t; x_1, \ldots, x_m),$$

where t corresponds to the square class of -1. In addition, since $H^\bullet(C_2, \mathbb{F}_2)$ is universally Koszul, we obtain the following

Proposition 9.4.7. *If $\mathbb{F} \in \mathcal{PFR}$ is such that $\#\mathbb{F}^\times/\mathbb{F}^{\times 2} < \infty$, then $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ is universally Koszul and thus Koszul.*

Chapter 10

Koszul filtrations

We have already seen that Galois cohomology of rigid fields is always universally Koszul, even if it is not strongly Koszul. Here we would like to show that these algebras have Koszul filtrations, and moreover, show that Koszul filtrations are preserved by direct sums and twisted extensions. Of course, this could easily follow from the fact that Universal Koszulity implies the existence of a Koszul filtration, However, these results can stand in their own terms, as outside of the context of Galois cohomology, there are very few examples of Universally Koszul algebras.

10.1 Direct sum

Proposition 10.1.1. *Let A and B be algebras with respective Koszul filtrations $\mathcal{F}$ and $\mathcal{G}$. Then the direct sum $A \sqcap B$ has the Koszul filtration $\mathcal{H} = \mathcal{F} \sqcap \mathcal{G} = \{I_A^e \cup I_B^e : I_A \in \mathcal{F},\ I_B \in \mathcal{G}\}$.*

Proof. Conditions 1. and 2. of Definition 5.2.6 for the family $\mathcal{H}$ stem immediately from the corresponding conditions on the Koszul filtrations $\mathcal{F}$ and $\mathcal{G}$.

For Condition 3., we consider two cases.

1. $I = I_A^e$, with $I_A \in \mathcal{F} \setminus \{(0)\}$.
   Since A_+ and B_+ annihilate each other, we get that $I = I_A \in \mathcal{F}$. By assumption, there exist an ideal $J \in \mathcal{F} \setminus \{I\}$ and an element $a \in A_1$, such that $I = J + (a)_A$ and $J :_A a \in \mathcal{F}$. But, viewing I and J as ideals of $A \sqcap B$, we deduce that $J = J^e \in \mathcal{H} \setminus \{I\}$ and $I = J + (a)_{A \sqcap B}$.

We claim that $J :_{A \sqcap B} a = (J :_A a)^e + B_+$. In fact, the inclusion $(J :_A a)^e + B_+ \subseteq J :_{A \sqcap B} a$ follows directly from the definition of direct sum. Conversely, a typical element of $A \sqcap B$ has the shape $x + y$ for some $x \in A, y \in B$, and without loss of generality we may assume $y \in B_+$. If $x + y \in J :_{A \sqcap B} a$, then $xa + ya = xa \in J = J \cap A$, whence $x \in (J :_A a)^e$. Therefore $x + y \in (J :_A a)^e + B_+$.

2. $I = I_A^e + I_B^e$, with $I_A \in \mathcal{F}$ and $I_B \in \mathcal{G} \setminus \{(0)\}$.
   As before, $I_A^e = I_A$ and $I_B^e = I_B$. Since $\mathcal{G}$ is a Koszul filtration, there exist $J_B \in \mathcal{G} \setminus \{I_B\}$ and $b \in B_1$, such that $I_B = J_B + (b)_B$ and $J_B :_B b \in \mathcal{G}$. Set $J = I_A^e + J_B^e$. Then $J + (b)_{A \sqcap B} = I$. The claim that $J :_{A \sqcap B} b = A_+ + (J_B :_B b)^e$ can be proved in an analogous way as before. □

10.2 Twisted extension

Similarly to the preceding Section, the aim is to show that the existence of Koszul filtrations is preserved by twisted extensions.

Proposition 10.2.1. *Let A be a quadratic algebra with a Koszul filtration $\mathcal{F}$. Suppose that $t \in A$ satisfies $t + t = 0$ and that $\mathcal{F}$ has the property*

$$J \in \mathcal{F} \Rightarrow J + (t) \in \mathcal{F}. \qquad (\diamondsuit)$$

Then any twisted extension $A(t; x_1, \ldots, x_m)$ has the Koszul filtration

$$\mathcal{H} = \{I^e + (Y) : I \in \mathcal{F},\ Y \subseteq \{x_1, \ldots, x_m, t - x_1, \ldots, t - x_m\}\}.$$

Proof. We first prove the result for the case $A(t; x)$, with the candidate Koszul filtration being $\mathcal{H} = \{I^e + (Y) \mid I \in \mathcal{F}, Y \subseteq \{x, t + x\}\}$. Conditions (i) and (ii) of Definition 5.2.6 are clearly satisfied. As regards Condition 3., any $c \in A(t, x)$ can be expressed as $c = p + qx$ for some $p, q \in A$. Since $\mathrm{ann}_{A(t;x)}(x) = \{0\}$, p and q are uniquely determined modulo the relations of A. We now address several cases separately.

1. $I = \widetilde{I}^e$ for $\widetilde{I} = (a_1, \ldots, a_d)_A \in \mathcal{F} \setminus \{(0)\}$, where $d > 0$ and all $a_i \in A_1$. By hypothesis, there exist some $\widetilde{J} = (\widehat{a_1}, \ldots, \widehat{a_r})_A \in \mathcal{F} \setminus \{\widetilde{I}\}$ and some $a \in A_1$, such that $\widetilde{I} = \widetilde{J} + (a)_A$ and $\widetilde{J} :_A a = (\widetilde{a_1}, \ldots, \widetilde{a_k})_A \in \mathcal{F}$. We then set
$$J = \widetilde{J}^e = (\widehat{a_1}, \ldots, \widehat{a_r})_{A(t;x)} \trianglelefteq A(t; x),$$

so that $I = J + (a)_{A(t;x)}$. We claim that the colon ideal

$$J :_{A(t;x)} a = (\widetilde{a_1}, \dots, \widetilde{a_k})_A^e \in \mathcal{H}.$$

In fact, all generators $\widetilde{a_i}$ belong to $J :_{A(t;x)} a$ by construction. For the reverse inclusion, take any $c = p + qx \in J :_{A(t;x)} a$. Then the element $ca = pa - qax$ belongs to J, which means that $pa - qax$ can be expressed as $pa - qax = \sum_{i=1}^{r} (p_i + q_i x)\widehat{a_i}$ for some suitable $p_i, q_i \in A$. By uniqueness of the normal form, we get that

$$\begin{cases} pa = \sum_{i=1}^{r} p_i \widehat{a_i} \in J, \\ qa = \sum_{i=1}^{r} q_i \widehat{a_i} \in J. \end{cases} .$$

But then

$$p, q \in (J :_{A(t,\{x\})} a) \cap A = \widetilde{J} :_A a = (\widetilde{a_1}, \dots, \widetilde{a_k})_A \trianglelefteq A,$$

which implies that $p + qx \in (\widetilde{a_1}, \dots, \widetilde{a_k})_A^e \trianglelefteq A(t, \{x\})$.

2. $I = \widetilde{I}^e + (x)_{A(t,\{x\})}$ for $\widetilde{I} = (a_1, \dots, a_d)_A \in \mathcal{F} \setminus \{(0\}$, where $d \geq 0$ and all $a_i \in A_1$.
   We set $J = \widetilde{I}^e$, so that $I = J + (x)_{A(t;x)}$, and we claim that

   $$J : x = \widetilde{I}^e + (t - x)_{A(t;x)} \in \mathcal{H}.$$

   In fact, all generators of the right hand side ideal belong to $J : x$ by construction, using the defining relations of $A(t;x)$. For the reverse inclusion, take any $c = p + qx \in J : x$. Then $cx = px + qx^2 = px + qtx = (p + qt)x$ belongs to J, or, in other words, $(p + qt)x$ can be expressed as a sum $(p + qt)x = \sum_{i=1}^{d} (p_i + q_i x)a_i$ for some suitable $p_i, q_i \in A$. Since $p + qt \in A$, the uniqueness of the normal form gives us that $p + qt = -\sum_{i=1}^{d} q_i a_i \in \widetilde{I} \subseteq \widetilde{I}^e$. Finally, $p + qx = p + qt - q(t - x) \in \widetilde{I}^e + (t - x)_{A(t,\{x\})}$.

3. $I = \widetilde{I}^e + (t - x)_{A(t;x)}$ for $\widetilde{I} = (a_1, \dots, a_d)_A \in \mathcal{F} \setminus \{(0)\}$, where $d \geq 0$ and all $a_i \in A_1$.
   This case is completely analogous to the previous one, interchanging the roles of x and $t - x$.

4. $I = \widetilde{I}^e + (x, t-x)_{A(t;x)}$ for $\widetilde{I} = (a_1, \dots, a_d)_A \in \mathcal{F} \setminus \{(0)\}$, where $d \geq 0$ and all $a_i \in A_1$.
   We can write $I = \widetilde{I}^e + (t)_{A(t;x)} + (x)_{A(t;x)}$. Thanks to property $(\diamondsuit)$, $\widetilde{I} + (t)_A \in \mathcal{F}$, so this case is brought back to case 2.

Therefore, the algebra $A(t;x)$ has the Koszul filtration $\mathcal{H} = \{I^e + (Y)\}$, where $I \in \mathcal{F}$ and $Y \subseteq \{x, t-x\}$. Note that the filtration $\mathcal{H}$ inherits Property $(\diamondsuit)$ by $\mathcal{F}$. Since $A(t; x_1, \dots, x_m) = ((A(t;x_1))(t;x_2)\dots)(t;x_m)$, the general statement follows by induction. □

Proposition 10.2.2. *Let A be a quadratic algebra with a Koszul filtration $\mathcal{F}$. Then any twisted extension $A(0; x_1, \dots, x_m)$ has the Koszul filtration $\mathcal{H} = \{I^e + (Y) \mid I \in \mathcal{F}, Y \subseteq \{x_1, \dots, x_m\}\}$.*

Proof. If $t = 0$, $(\diamondsuit)$ is automatically satisfied. □

Corollary 10.2.3. *The twisted extension $A(t; x_1, \dots, x_m)$ of an algebra A with a Koszul filtration by elements $x_1, \dots, x_m$ has a Koszul filtration.*

10.3 Koszul filtrations for 2-rigid fields

Using Proposition 10.2.1, we can show the following

Proposition 10.3.1. *If $\mathbb{F}$ is a superpythagorean field, then $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ has a Koszul filtration satisfying $(\diamondsuit)$.*

Proof. We can view $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ as the twisted extension

$$H^\bullet(\mathbb{F}(2), \mathbb{F}_2) = \mathbb{F}_2[t](t; \alpha_1, \dots, \alpha_d).$$

Now, the algebra $\mathbb{F}_2[t]$ has the Koszul filtration $\mathcal{F} = \{(0), (t)\}$, evidently satisfying $(\diamondsuit)$. Thus, the statement is a direct corollary of Proposition 10.2.1. To see this, note that for any $i = 1, \dots, d$, the identity $(0) : \alpha_i = (t + \alpha_i)$ holds. □

On the other hand, this property can also be shown in the much more tedious way by following the definition.

Proposition 10.3.2. *$H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ has a Koszul filtration.*

Proof. Let $X = \{t, \alpha_2, \ldots, \alpha_d, t + \alpha_2, \ldots, t + \alpha_d\}$ be a system of generators of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$. Then the collection $\mathcal{F} = \{(Y) : Y \subseteq X\}$ is a Koszul filtration of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$. Conditions 1. and 2. of Definition 5.2.6 are trivially satisfied. For condition 3. there are several cases to address. Let $\pi : \mathbb{F}_2[t, \alpha_2, \ldots, \alpha_d] \longrightarrow H^\bullet(\mathbb{F}(2), \mathbb{F}_2) = \mathbb{F}_2[t, \alpha_2, \ldots, \alpha_d]/(\alpha_i\alpha_i = t\alpha_i)$ be the canonical projection.

1. $I = (t)$.
   We set $J = (0)$ and we have $J\colon t = (0) \in \mathcal{F}$.

2. $I = (t, \alpha_{i_1}, \ldots, \alpha_{i_r}, t + \alpha_{i_{r+1}}, \ldots, t + \alpha_{i_{r+s}})$, $r + s \geq 1$.
   We can then rewrite I in the form $I = (t, \alpha_{i_1}, \ldots, \alpha_{i_r}, \alpha_{i_{r+1}}, \ldots, \alpha_{i_{r+s}})$ and set $J = (t, \alpha_{i_2}, \ldots, \alpha_{i_r}, \alpha_{i_{r+1}}, \ldots, \alpha_{i_{r+s}})$. We then show that

   $$J\colon \alpha_{i_1} = J + (t + \alpha_{i_1}) = J + (\alpha_{i_1}) = I.$$

   In fact, the inclusion $I \subseteq J\colon \alpha_{i_1}$ is a direct consequence of the defining relators of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$. Vice versa, let b be a homogeneous element of $J\colon \alpha_{i_1} \backslash I$. For two elements α and β with $\alpha \in I$, we have that $\alpha + \beta \in I$ if and only if $\beta \in I$. So we can assume that b is a sum of monomials none of which lies in I. In more concrete terms, $b = \sum b_j$ such that the b_j's are pairwise unlike terms, meaning that for all j,

   $$t \nmid b_j, \alpha_{i_1} \nmid b_j, \ldots, \alpha_{i_{r+s}} \nmid b_j$$

   and any other generator of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ does not divide any of the b_j's more than once. But then for any k, the fiber $\pi^{-1}(b_k\alpha_{i_1})$ is made of a single element, which means that $b_k\alpha_{i_1}$ cannot be expressed otherwise (modulo commutativity). Hence it cannot be in J, as b_k is not. The same argument extends to the sum of all terms $b_j\alpha_{i_1}$: no two of them can be rewritten as like terms. Hence it is impossible to trigger "compensation processes" which make that sum stay in J even though each summand does not. Therefore, $b \in J\colon \alpha_{i_1}$ if and only if $b \in J + (\alpha_{i_1})$.

3. $I = (\alpha_{i_1}, \ldots, \alpha_{i_r}, t + \alpha_{i_{r+1}}, \ldots, t + \alpha_{i_{r+s}})$, $r \geq 1$.
   We may and do assume that $\{i_1, \ldots, i_r\} \cap \{i_{r+1}, \ldots, i_{r+s}\} = \emptyset$, otherwise $t \in I$, which reduces to the previous case. We set $J = (\alpha_{i_2}, \ldots, \alpha_{i_r}, t + \alpha_{i_{r+1}}, \ldots, t + \alpha_{i_{r+s}})$ and we show that

   $$J\colon \alpha_{i_i} = J + (t + \alpha_{i_i}).$$

Again, the inclusion $J + (t + \alpha_{i_i}) \subseteq J \colon \alpha_{i_i}$ is a direct consequence of the defining relations of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$. On the other hand, consider a homogeneous element $b \in J \colon \alpha_{i_1} \setminus (J + (t + \alpha_{i_1}))$. Since

$$\alpha_{i_1} \equiv \alpha_{i_{r+1}} \equiv \cdots \equiv \alpha_{i_{r+s}} \equiv t \mathrm{mod} J + (t + \alpha_{i_1}),$$

we can assume that

- $b = pt + \sum b_j$, for pairwise unlike monomials b_j's and a polynomial p;
- no generator of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ divides any of the b_j's more than once; no generator except possibly t divides any monomial of p more than once;
- no one of $\alpha_{i_1}, \ldots, \alpha_{i_{r+s}}$ divides any of the b_j's or any monomial of p;
- t does not divide any of the b_j's.

But for elements b with these features it is apparent that $b\alpha_{i_1} \notin J$, in the same fashion as the preceding case. In particular, we explicitly note that for any $i = 1, \ldots, d$,

$$(0) \colon \alpha_i = (t + \alpha_i) \tag{$\spadesuit$}$$

4. $I = (t + \alpha_{i_1}, \ldots, t + \alpha_{i_s})$, $s \leq 2$.
   With a translation of the generators $\{t, \alpha_2, \ldots, \alpha_d\}$ of $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ to the generators $\{t, t + \alpha_2, \ldots, t + \alpha_d\}$, this case reduces to 3. □

We show the analogical results in the case of rigid fields of level two.

Proposition 10.3.3. *If $\mathbb{F}$ is a 2-rigid field of level $s(\mathbb{F}) = 2$, then $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ has a Koszul filtration satisfying ($\diamondsuit$).*

Proof. We imitate the trick used in Proposition 10.3.1. Since

$$H^\bullet(\mathbb{F}(2), \mathbb{F}_2) = (\mathbb{F}_2[t]/(t^2))(t, \alpha_1, \ldots, \alpha_d)$$

and $\mathbb{F}_2[t]/(t^2)$ has the Koszul filtration $\mathcal{F} = \{(0), (t)\}$ satisfying ($\diamondsuit$), the result is a direct corollary of Proposition 10.2.1. The identity $(0) : \alpha_i = (t + \alpha_i)$ holds in this situation as well. □

Proposition 10.3.4. *For a 2-rigid field $\mathbb{F}$ of level $s(\mathbb{F}) = 2$, $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ has a Koszul filtration.*

Proof. The only differences from the proof of Proposition 10.3.2 is that $(0) : t = (t)$ and t cannot divide a nonzero monomial more than once. Noting this, and using the candidate filtration

$$\mathcal{F} = \{(Y) : Y \subseteq \{t, \alpha_2, \dots, \alpha_d, t + \alpha_2, \dots, t + \alpha_d\}\},$$

the proof is identical to Proposition 10.3.2. □

Finally,

Proposition 10.3.5. *Let $\mathbb{F}$ be a rigid field of level $s(\mathbb{F}) = 0$ or $s(\mathbb{F}) = 2$. Then the twisted extension $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)(t; x_1, \dots, x_m)$ has a Koszul filtration.*

Proof. We follow the same notation of Sections 8.2 and 8.3. By Propositions 10.3.1 and 10.3.3, we know that $H^\bullet(\mathbb{F}(2), \mathbb{F}_2)$ has a Koszul filtration $\mathcal{F}$. Nonetheless, the identity $(0) : \alpha_i = (t + \alpha_i)$ implies that if $I \in \mathcal{F}$, then $I + (t) \in \mathcal{F}$ as well. Therefore, Proposition 10.2.1 implies the desired statement. □

Chapter 11

Conclusion

In all known cases where the maximal pro-p-quotient $G_{\mathbb{F}}(p)$ of $G_{\mathbb{F}}$ is finitely generated, we proved that universal Koszulity holds. But also a number of open questions stemmed from this work, that are currently under consideration.

For instance, one problem is to extend the current work to maximal pro-p-quotients that are not necessarily finitely generated. Moreover, another aim is to obtain the unconditional results without relying to the Elementary Type Conjectures. On the other hand, a different direction concerns the Formality Conjecture; and an important problem is to enhance formality to the case of absolute Galois groups. In fact, the aim is to create an enhanced version of formality, which takes into account the cyclotomic character in the very least; this enhanced version should be strong enough to avoid a known counterexample due to L. Positselski. In the very best, we should be able to connect it with the Vanishing n-Massey Products Conjecture, to show that this enhanced version of Formality holds for maximal pro-p-quotients.

Finally, there is hope that all these seemingly different paths will lead to determining the structure of $G_{\mathbb{F}}(p)$ in full generality.

Appendix A

Spectral Sequences

This appendix was added to clarify the proof of the Tower Theorem 2.1.3, which relied heavily on the use of the Hochschild-Serre spectral sequence. The title here is rather deceiving, as we do not establish a general theory of spectral sequences. Rather than this, we only restrict our focus to the Hochschild-Serre spectral sequence and its basic properties. We moreover present examples where we calculate cohomology rings of small groups using the Hochschild-Serre spectral sequence, as a means of clarifying these ideas.

The moral behind spectral sequences is rather simple: computing a cohomology group can be a tough quest; but maybe breaking it down into successive quotients and piecing the individual quotient information together might give us a full understanding of it.

In a more informal setting, let p and q be two nonnegative integers and consider abelian groups E_0^{pq}. Assume that for each p, we have differentials

$$d_0^{pq} : E_0^{pq} \longrightarrow E_0^{p,q+1},$$

such that $d \circ d = 0$. Then for each p, we have a complex of abelian groups

$$E_0^{p,0} \xrightarrow{d_0^{p0}} E_0^{p1} \xrightarrow{d_0^{p1}} E_0^{p2} \xrightarrow{d_0^{p2}} \cdots ,$$

whose cohomology is denoted by

$$E_1^{pq} := \ker d_0^{pq} / \operatorname{im} d_0^{p,q-1}.$$

If we now assume that for each q, we have differentials

$$d_1^{pq} : E_1^{pq} \longrightarrow E^{p+1,q-1},$$

such that $d \circ d = 0$, then we have a complex of abelian groups

$$E_1^{0q} \overset{d_1^{0q}}{\to} E_1^{1,q} \overset{d_1^{1q}}{\to} E_1^{2q} \overset{d_1^{2q}}{\to} \cdots ,$$

whose cohomology groups are denoted for each q by

$$E_2^{pq} = \ker d_1^{pq} / \operatorname{im} d_1^{p-1,q}.$$

In the case that either p or q are negative, we just take both differentials to be zero.

In the same fashion, if we had differentials

$$d_2^{pq} : E_2^{pq} \longrightarrow E_2^{p+2,q-1},$$

such that $d \circ d = 0$, we would then again have a complex of abelian groups whose cohomology we denote by

$$E_3^{pq} = \ker d_2^{pq} / \operatorname{im} d_2^{p-2,q+1},$$

and we can continue this process to infinitely many steps.

Now, notice that all maps from E_2^{p0} have to be trivial, since they land in $E_2^{p+2,-1}$, which is zero. And similarly all maps from E_2^{0q} and E_2^{1q} are also trivial. This means that $E_3^{00} = E_2^{00}$ and $E_3^{13} = E_2^{13}$. In other words, these two maps have been stabilized in the second step, and we denote this (constant) value by E_∞^{00} and E_∞^{01} respectively.

Now, continuing on the third step, all groups E_3^{20}, E_3^{11} and E_3^{12} have also been stabilized, so we get the values E_∞^{20}, E_∞^{11} and E_∞^{12} added to the values E_∞^{00} and E_∞^{01}.

As we reach further steps, we add more groups that have been stabilized. This is what a spectral sequence allows us to do. And if, at some point, all groups have been stabilized, we will then be able to compute the desired cohomology.

Let G be a profinite group, H a closed normal subgroup of G, and A a G-module. Then there exists a spectral sequence

$$E_2^{pq} = H^p(G/H, H^q(H, A)) \longrightarrow H^{p+q}(G, A)$$

called the *Hochschild-Serre* spectral sequence. It is a *first quadrant* spectral sequence, meaning that for either p or q negative, $E_2^{pq} = 0$.

We can directly see by definition that if $H^q(H,A) = 0$ for $q > 0$, then $H^n(G/H, A^H) \cong H^n(G,A)$. Moreover, the first terms of this sequence induce the *five term exact sequence*

$$0 \longrightarrow H^1(G/H, A^H) \overset{\text{inf}}{\to} H^1(G,A) \overset{\text{res}}{\to} H^1(H,A)^{G/H} \overset{\text{tg}}{\to} H^2(G/H, A^H) \overset{\text{inf}}{\to} H^2(G,A).$$

The homomorphism $d_2^{01} = \text{tg} : H^1(H,A)^{G/H} \longrightarrow H^2(G/H, A^H)$ is the *transgression* homomorphism, defined in the following way. If $x : H \longrightarrow A$ is a 1-cocycle in the class $(x) \in H^1(H,A)^{G/H}$, there exists a 1-cochain $y : G \longrightarrow A$, such that

- $y_{|H} = X$, and that
- $(\partial y)(\sigma_1, \sigma_2)$ is contained in A^H and depends only on the cosets $\sigma_1 H$ and $\sigma_2 H$, i.e. may be regarded as a cocycle of G/H.

For each such cochain y, the transgression is give by $\text{tg}(x) = (dy)$.

A powerful property of the Hochschild-Serre spectral sequence is that it allows us to compute cup products. In fact, for $p > 0$, the maps

$$d_2, u \cup - : H^{p-1}(G/H, H^1(H,A)) \longrightarrow H^{p+1}(G/H, A)$$

are the same up to sign, i.e. $d_2(x) = -u \cup x$. In particular, the transgression $\text{tg} : H^1(H,A)^{G/H} \longrightarrow H^2(G/H, A)$ is given by $\text{tg}(x) = -u \cup x$.

Let $1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1$ be a split exact sequence of profinite groups, and let A be a discrete G-module on which H acts trivially. Then $\text{inf}_G^{G/H} : H^\bullet(G/H, A) \longrightarrow H^\bullet(G,A)$ is an injective homomorphism into a direct summand, and all differentials into the horizontal edge of the Hochschild-Serre spectral sequence for A vanish, that is,

$$d_r^{\bullet, r-1} = 0, \forall r \geq 2.$$

Examples.
Below we present an analog of the Universal Coefficient Theorem and of Kunneth Theorem for spectral sequences.

1. Let G and G' be profinite groups and let A be a discrete G'-module, regarded as a $(G \times G')$-module via trivial action of G. Then the Hochschild-Serre spectral sequence

$$E_2^{pq} : H^p(G/G', H^q(G', A)) \longrightarrow H^{p+q}(G \times G', A)$$

degenerates at E_2.
Furthermore, it splits in the sense that there is a decomposition

$$H^n(G \times G', A) \cong \oplus_{p+q=n} H^p(G, H^q(G', A)).$$

2. Let A be a G'-module, regarded as a $(G \times G')$-module via trivial action of G. Then

$$0 \longrightarrow \oplus_{i+j=n} H^i(G, \mathbb{Z}) \otimes H^j(G', A) \longrightarrow H^n(G \times G', A) \longrightarrow$$
$$\longrightarrow \oplus_{i+j=n+1} \mathrm{Tor}_1^{\mathbb{Z}}(H^i(G, \mathbb{Z}), H^j(G', A)) \longrightarrow 0$$

is a split split exact sequence for all $n \geq 0$. Replacing A by a field $\mathbb{F}$ viewed as a trivial module, the Kunneth formula induces the exact sequence

$$0 \longrightarrow \oplus_{i+j=n} H^i(G, \mathbb{F}) \otimes H^j(G', \mathbb{F}) \longrightarrow H^n(G \times G', \mathbb{F}) \longrightarrow$$
$$\longrightarrow \oplus_{i+j=n+1} \mathrm{Tor}_1^{\mathbb{Z}}(H^i(G, \mathbb{F}), H^j(G', \mathbb{F})) \longrightarrow 0.$$

But $\mathrm{Tor}_1^{\mathbb{Z}} = 0$, since $\mathbb{F}$ is a field, which gives us a (non-canonical) isomorphism

$$H^n(G \times G', \mathbb{F}) \cong \oplus_{i+j=n} H^i(G, \mathbb{F}) \otimes_{\mathbb{F}} H^j(G', \mathbb{F}).$$

We say that a spectral sequence *collapses* or degenerates at the α-th page, if $d_\alpha = d_{\alpha+1} = \ldots$. If a spectral sequence collapses at the α-th page, we have that $E^{pq}_{\alpha+1} = E^{pq}_{\alpha}$, and $E^{pq}_{\infty} = E^{pq}_{\alpha}$. This means that on the line $p + q = n$, there is only one nonzero term, and thus the cohomology H^n equals that term.

Below we utilize the theory of spectral sequences in computations of cohomology rings.

Examples.

1. We shall first compute the cohomology ring of $C_2 \times C_2$ with coefficients in $\mathbb{F}_2$ using spectral sequences. First, it is not hard to see that since C_2 acts trivially on $\mathbb{F}_2$, we have that $H^0(C_2, \mathbb{F}_2) \cong \mathbb{F}_2$, $H^1(C_2, \mathbb{F}_2) \cong \langle x \rangle_{\mathbb{F}_2}$, and $H^n(C_2, \mathbb{F}_2) = \langle x^n \rangle$ for $n \geq 2$. Therefore $H^\bullet(C_2, \mathbb{F}_2) \cong \mathbb{F}_2[x]$, with x being in degree 1. Now, the group extension

$$1 \longrightarrow C_2 \longrightarrow C_2 \times C_2 \longrightarrow C_2 \longrightarrow 1$$

gives rise to the spectral sequence

$$E_2^{pq} = H^p(C_2, H^q(C_2, \mathbb{F}_2)) \longrightarrow H^{p+q}(C_2 \times C_2, \mathbb{F}_2).$$

We have that $E_2^{00} = E_\infty^{00} = \mathbb{F}_2$, $E_2^{10} = E_\infty^{10} = \langle y \rangle_{\mathbb{F}_2}$ and $E_2^{11} = E_\infty^{11}$, because the differentials there come from zero and land to zero. So, the sequence degenerates on E_2-page, and we have that the corner of the E_2-page has the following generators.

$$\begin{array}{ccccc} y^2 & y^2x & y^2x^2 & y^2x^3 & \cdots \\ y & yx & yx^2 & yx^3 & \cdots \\ 1 & x & x^2 & x^3 & \cdots . \end{array}$$

Now, we have that $d_2(x) = d_2(y) = 0$ and $d(x^iy^j) = 0$ for all $i, j \geq 0$. Therefore, we have that $H^0(C_2 \times C_2, \mathbb{F}_2) \cong F_2$, $H^1(C_2 \times C_2, \mathbb{F}_2) = E_\infty^{01} \oplus E_\infty^{10} = \mathbb{F}_2[x] \oplus \mathbb{F}_2[y]$ and so

$$\begin{aligned} H^\bullet(C_2 \times C_2, \mathbb{F}_2) = & \quad H^0(C_2 \times C_2, \mathbb{F}_2) \oplus H^1(C_2 \times C_2, \mathbb{F}_2) \\ = & \qquad \mathbb{F}_2 \oplus \mathbb{F}_2[x] \oplus \mathbb{F}_2[y] \cong \mathbb{F}_2[x, y]. \end{aligned}$$

2. Inductively, we can show that $H^\bullet(\prod_{i=1}^n C_2, \mathbb{F}_2) \cong \mathbb{F}_2[x_1, \ldots, x_n]$.

3. We shall now compute the cohomology ring $H^\bullet(C_4, \mathbb{F}_2)$ using the group extension

   $$1 \longrightarrow C_2 \longrightarrow C_4 \longrightarrow C_2 \longrightarrow 1,$$

   which is is non-split, but central, and the associated spectral sequence

   $$E_2^{pq} = H^p(C_2, H^q(C_2, \mathbb{F}_2)) \longrightarrow H^{p+q}(C_4, \mathbb{F}_2) = E^{p+q}.$$

   Recall that $H^\bullet(C_2, \mathbb{F}_2) = \mathbb{F}_2[x]$, for $(x) \in H^1(C_2, \mathbb{F}_2)$. Again, we have that $E_2^{00} = E_\infty^{00} = \mathbb{F}_2$, $E_2^{10} = E_\infty^{10} = \langle x \rangle_{\mathbb{F}_2}$ and $E_2^{01} = \langle y \rangle_{\mathbb{F}_2}$. Therefore, the generators on the corner of the E_2-page are

   $$\begin{array}{cccc} y^2 & y^2x & y^2x^2 & \cdots \\ y & yx & yx^2 & \cdots \\ 1 & x & x^2 & \cdots , \end{array}$$

where $d_2(x) = 0$. But now, since the sequence does not split, we have that $d_2(y) = x^2$. We compute the other differentials.

$$\begin{aligned}
d_2(y^2) = &\quad d_2(y)y + yd_2(y) = 2d_2(y) = 0.\\
d_2(yx) = &\quad d_2(y)x + yd_2(x) = x^2x + y \cdot 0 = x^3.\\
d_2(yx^2) = &\quad d_2(y)x^2 + yd_2(x^2) = x^4.\\
d_2(y^2x) = &\quad d_2(y^2)x + y^2d_2(x) = 0.\\
d_2(y^2x^2) = &\quad d_2(y^2)x^2 + y^2d_2(x^2) = 0.\\
d_2(y^3) = &\quad d_2(y^2)y + y^2d_2(y) = y^2x^2.\\
d_2(y^3x) = &\quad d_2(y^3)d + y^3d_2(x) = y^2x^2x = y^2x^3.
\end{aligned}$$

Hence, we have that

$$d_2(x^iy^{2j}) = 0,$$

and

$$d_2(x^iy^{2j+1}) = x^{i+2}y^{2j}.$$

We can thus see that the elements on E_2 are killed in the following way

$$\begin{tikzcd}
y^3 \arrow[drr] & y^3x \arrow[drr] & y^3x^2 \arrow[drr] & \cdots & \cdots & \\
y^2 & y^2x & y^2x^2 & y^2x^3 & \cdots & \\
y \arrow[drr] & yx \arrow[drr] & yx^2 \arrow[drr] & yx^3 \arrow[drr] & \cdots & \\
1 & x & x^2 & x^3 & \cdots & .
\end{tikzcd}$$

Thus the only elements that survive on the E_3-page are

$$\begin{matrix}
0 & 0 & 0 & \cdots \\
y^2 & y^2x & 0 & \cdots \\
0 & 0 & 0 & \cdots \\
1 & x & 0 & \cdots .
\end{matrix}$$

Now, exactly because all of the elements still left on the E_3-page are surrounded by zeros, all the differentials from/to them have to be trivial, and so the spectral sequence degenerates on the E_3-page and thus $E_\infty = E_3$. This amounts to $H^0(C_4, \mathbb{F}_2) = E_\infty^{00} = \mathbb{F}_2$, $H^1(C_4, \mathbb{F}_2) =$

$E_\infty^{10} = \mathbb{F}_2[x]/(x^2)$, $H^2(C_4, \mathbb{F}_2) = E_\infty^{02} = \mathbb{F}_2[y^2]$, $H^3(C_3, \mathbb{F}_2) = E_\infty^{12} = \mathbb{F}_2[y^2x]$ and so on. Therefore,

$$H^\bullet(C_4, \mathbb{F}_2) = \mathbb{F}_2[x, z]/(x^2) = \mathbb{F}_2[x]/(x^2) \otimes_{\mathbb{F}_2} \mathbb{F}_2[z] = \bigwedge(x) \otimes_{\mathbb{F}_2} \mathbb{F}_2[z],$$

where $|z| = 2$ and z is a lift of y.

4. Similarly, for p odd, we shall compute the cohomology ring $H^\bullet(C_{p^2}, \mathbb{F}_p)$ using the central extension

$$1 \longrightarrow C_p \longrightarrow C_{p^2} \longrightarrow C_p \longrightarrow 1,$$

which induces the spectral sequence

$$E_2^{pq} = H^p(C_p, H^q(C_p, \mathbb{F}_p)) \longrightarrow H^{p+q}(C_{p^2}, \mathbb{F}_p).$$

Recall that $H^\bullet(C_p, \mathbb{F}_p) = \mathbb{F}_p[x]$, where the degree of x is 1. Therefore, the corner of the second page of the spectral sequence looks as follows.

$$\begin{array}{ccccc} x'^2 & x'^2y & x'^2x & \cdots & \\ x' & x'y & x'x & x'yx & x'x^2 \\ y' & y'y & y'x & y'yx & y'x^2 \\ 1 & y & x & yx & x^2. \end{array}$$

Now, $d_2(y) = x$ or $-x$ and $d_2(y') = x$ as well, so y' and $d_2(y)$ kill each other. Moreover

$$\begin{array}{rc} d_2(y'y) = & d_2(y')y - y'd_2(y) = xy. \\ d_2(y'x) = & d_2(y'x) - y'd_2(x) = xx = x^2. \\ x_2(y'yx) = & (d_2y'y)x - y'yd_2(x) = xyx = yx^2. \end{array}$$

In this manner we see that every term of the first row disappears. Continuing to the second row, notice that $d_2(x')$ belongs to the ideal generated by $y'x$. But for $y'x$ we have already seen that $d_2(y'x) = x^2$. And since $d_2^2 = 0$, we deduce that $d_2(x') = 0$. Similarly,

$$\begin{array}{rc} d_2(x'y) = & d_2(x')y + x'd_2(y) = 0. \\ d_2(x'x) = & d_2(x')x + xd_2(x') = 0. \\ d_2(x'yx) = & d_2(x'y)x + x'yd_2(x) = 0. \end{array}$$

and in this manner we deduce that all differentials on the second row are trivial. Now, for the third row,

$$\begin{aligned} d_2(y'x') = & \quad d_2(y')x' - y'd_2(x') = xx'. \\ d_2(y'x'y) = & \quad d_2(y'x')y - y'x'd_2(y) = xx'y - y'x'x. \end{aligned}$$

and we similarly find that every term on the third row f. In this manner, we show that all terms of every odd row disappear, while all differentials of every even row are trivial. Therefore, the generators surviving and creating the third page look as follows.

$$\begin{array}{cccc} x'^2 & x'^2y & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ x' & x'y & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ 1 & y & 0 & \cdots . \end{array}$$

Therefore,

$$H^\bullet(C_{p^2}, \mathbb{F}_p) = \mathbb{F}_p[y]/(y^2) \oplus \mathbb{F}_p[x'] = \mathbb{F}_p[x', y]/(y^2).$$

5. We now complicate the situation a little more by considering a group whose extensions are neither split nor central, namely we compute $H^\bullet(D_4, \mathbb{F}_2)$, where D_4 is the dihedral group of order 8. Consider the group extension $D_4 = (C_2 \times C_2) \rtimes C_2$ and take the associated spectral sequence
$$H^p(C_2, H^q(C_2 \times C_2, \mathbb{F}_2)) \longrightarrow H^{p+q}(D_4, \mathbb{F}_2).$$
We have already seen that $H^\bullet(C_2, \mathbb{F}_2) = \mathbb{F}_2[z]$ and $H^\bullet(C_2 \times C_2) = \mathbb{F}_2[x, y]$, where all of z, x and y are in degree 1. However, since the extension is not central, we cannot immediately describe the E_2 page without considering how C_2 acts on $H^q(C_2 \times C_2, \mathbb{F}_2)$ for all $q \geq 0$. The ring $H^\bullet(C_2 \times C_2, \mathbb{F}_2)$ viewed as a C_2-module can be broken down into the direct sum of two parts, namely the trivial C_2-module and the free transitive C_2-module. Therefore, the corresponding $\mathbb{F}_2$-generators on the E_2 page are
$$\begin{array}{cccc} x^4 + y^4, x^3y + xy^3, x^2y^2 & x^2y^2z & x^2y^2z^2 & \cdots \\ x^3 + y^3, x^2y + xy^2 & x^2yz + xy^2z & x^2yz^2 + xy^2z^2 & \cdots \\ x^2 + y^2, xy & xyz & xyz^2 & \cdots \\ x + y & (x+y)z & (x+y)z^2 & \cdots \\ 1 & z & z^2 & \cdots . \end{array}$$

We now compute the differentials. We first note that $d_2(z) = 0$. We now have

$$\begin{aligned} d_2(x+y) &= z^2. \\ d_2((x+y)z) &= d_2(x+y)z + (x+y)d_2(z) = z^3. \\ d_2((x+y)z^2) &= d_2(x+y)z^2 + (x+y)d_2(z^2) = z^4. \\ d_2(x^2+y^2) &= d_2((x+y)^2) = d_2(x+y)(x+y) + (x+y)d_2(x+y) = 0. \\ d_2(xyz) &= d_2(xy)z + (xy)d_2(z) = 0. \end{aligned}$$

Continuing our computations, we see that all the differentials are trivial and so the sequence degenerates on E_2. Therefore,

$$\begin{aligned} H^0(D_4, \mathbb{F}_2) &= \mathbb{F}_2, \\ H^1(D_4, \mathbb{F}_2) &= E_\infty^{01} \oplus E_\infty^{10} = \mathbb{F}_2[x+y] \oplus \mathbb{F}_2[z], \\ H^2(D_4, \mathbb{F}_2) &= E_\infty^{02} \oplus E_\infty^{11} \oplus E_\infty^{20} = \mathbb{F}_2[xy] \oplus \mathbb{F}_2[z^2]/((x+y)z), \\ H^3(D_4, \mathbb{F}_2) &= \mathbb{F}_2[xyz, z^3]/((x+y)z^2), \end{aligned}$$

and so on. Therefore,

$$E_\infty = E_2 = \mathbb{F}_2[z, x+y, xy]/(z(x+y)).$$

Now, recall that sine E_∞ is finitely generated and commutative as a $\mathbb{F}_2$-algebra, then the generators and the relations of $H^\bullet(D_4, \mathbb{F}_2)$ are given by lifting the corresponding generators and relations of E_∞. Therefore, we deduce that

$$H^\bullet(D_4, \mathbb{F}_2) = \mathbb{F}_2[\omega, \sigma_1, \sigma_2]/(R),$$

where $|\omega| = 1 = |\sigma_1|$, $|\sigma_2| = 2$, σ_1 and σ_2 are lifts of the generators $x+y$ and xy respectively, and R is the lift of the relation $z(x+y) = 0$.

Note that the Hilbert series of $H^\bullet(D_4, \mathbb{F}_2)$ is given as

$$\begin{aligned} p(t) &= \textstyle\sum_{i=0}^{\infty} \dim_{\mathbb{F}_2} H^i(D_4, \mathbb{F}_2) t^i \\ &= \dim_{F_2} H^0(D_4, \mathbb{F}_2) \oplus \dim_{F_2} H^1(D_4, \mathbb{F}_2)t + \dim_{F_2} H^2(D_4, \mathbb{F}_2)t^2 + \cdots \\ &= 1 + 2t + 3t^2 + \cdots \\ &= \tfrac{(1-t)(1+2t+3t^2+\cdots)}{1-t} = \tfrac{1+t+t^2+\cdots}{1-t} = \tfrac{1}{(1-t)^2}. \end{aligned}$$

6. We shall again compute $H^\bullet(D_4, \mathbb{F}_2)$, this time using a different group extension. Consider the decomposition of D_4 as $D_4 = C_4 \rtimes C_2$ and the spectral sequence associated with it

$$H^p(C_2, H^q(C_4, \mathbb{F}_2)) \longrightarrow H^{p+q}(D_4, \mathbb{F}_2).$$

Recall that $H^\bullet(C_2, \mathbb{F}_2) = \mathbb{F}_2[z]$ and $H^\bullet(C_4, \mathbb{F}_2) = \mathbb{F}_2[x, y]/(y^2) = \mathbb{F}_2[x] \otimes \bigwedge(y)$ with $|x| = 2$ and $|y| = 1$. Now, since this extension is not central either, we have to see how C_2 acts on the $H^q(C_4, \mathbb{F}_2)$ for each q. But sine on each degree, $H^q(C_4, \mathbb{F}_2) = \mathbb{F}_2$, we get that C_2 acts trivially on each. Computing the differentials on the E_2 page we have that

$$\begin{array}{rc}
d_2(x) = & z^2. \\
d_2(z) = & 0. \\
d_2(xz) = & d_2(x)z + xd_2(z) = z^3. \\
d_2(y^2) = & 2yd(y) = 0. \\
d_2(y^2z) = & d_2(y^2)z + y^2d_2(z) = 0. \\
d_2(xz^2) = & d_2(x)z^2 + xd_2(z^2) = z^4. \\
d_2(y^2x) = & d_2(y^2)x + y^2d_2(x) = y^2z^2. \\
d_2(y^2xz) = & d_2(y^2x)z + y^2xd_2(z) = y^2z^3.
\end{array}$$

In general,

$$\begin{array}{rc}
d_2(xz^i) = & z^{i+2}, \\
d_2(y^{2i}xz^j) = & y^{2i}z^{j+2}, \\
d_2(y^{2i}z^j) = & 0.
\end{array}$$

Therefore, the generators on the second page kill each other and the page looks as follows.

$$\begin{array}{cccc}
0 & 0 & 0 & \cdots \\
y^2 & 0 & 0 & \cdots \\
x & 0 & 0 & \cdots \\
1 & z & z^2 & \cdots .
\end{array}$$

Therefore, the E_2 page is equal to

$$H^\bullet(C_4, \mathbb{F}_2) \otimes H^\bullet(C_2, \mathbb{F}_2) = \mathbb{F}_2[x] \otimes \bigwedge(y) \otimes \mathbb{F}_2[z] = \mathbb{F}_2[x, y, z]/(y^2).$$

But since all terms survive on E_2-page, we get that the above ring also describes the E_∞ page. Therefore, again we deduce that

$$H^\bullet(D_4, \mathbb{F}_2) = \mathbb{F}_2[z, \sigma_1, \sigma_2]/(R),$$

where $|z| = 1$, σ_1, σ_2 are lifts of x and y respectively, and R is the lift $\sigma_2^2 = \sigma_2 z$ of the relation $y^2 = 0$.

Notice that the computation of the cohomology ring did not depend on the choice of group extension for D_4.

7. Lastly, consider the quaternion group Q_8 and the group extension

$$1 \longrightarrow C_2 \longrightarrow Q_8 \longrightarrow C_2 \times C_2 \longrightarrow 1,$$

which yields the spectral sequence

$$H^p(C_2, H^q(C_2 \times C_2, \mathbb{F}_2)) \longrightarrow H^{p+q}(Q_8, \mathbb{F}_2).$$

Recall that $H^\bullet(C_2 \times C_2, \mathbb{F}_2) = F_2[x, y]$ and $H^\bullet(C_2, \mathbb{F}_2) = \mathbb{F}_2[z]$, and note that the above group extension is central, so

$$E_2 = H^\bullet(C_2, \mathbb{F}_2) \otimes H^\bullet(C_2 \times C_2, \mathbb{F}_2) = F_2[x, y, z].$$

Now, we shall compute the differentials d_2. We have that $d_2(x) = d_2(y) = 0$ and $d_2(z) = x^2 + xy + y^2$, while all the other generators of E_2 kill each other. Therefore, passing to the E_3 page,

$$E_3 = \ker(d_2)/\operatorname{im}(d_2) = \mathbb{F}_2[x, y, z^2]/(x^2 + xy + y^2).$$

Now, each $E_3^{p,q}$-term is $\mathbb{F}_2$, and so not all differentials can be trivial. In fact, the differential

$$d_3 : E_3^{0,2} \longrightarrow E_3^{3,0}$$

has to be an isomorphism, and we can similarly see that all differentials

$$d_3 : E_3^{i,2} \longrightarrow E_3^{i+3,0}$$

and

$$d_3 : E_3^{i,3} \longrightarrow E_3^{i+3,1}$$

are isomorphisms. Therefore, all these terms survive and pass to the E_4-page. Now, on the E_4 page we have that $E_4^{0,j} = E_4^{1,j} = E_4^{2,j}$ if

$j \equiv 0, 1 \bmod 4$, while all the other terms are trivial. However, all the differentials associated to them are trivial, and thus all of the terms survive. This means that the spectral sequence collapses on page E_4, and therefore

$$H^\bullet(Q_8, \mathbb{F}_2) = E_\infty = E_4 = \mathbb{F}_2[x, y, z']/(x^2 + xy + y^2, x^3, y^3),$$

with $|z'| = 4$ and z' is a lift of z.

Bibliography

[Bec74] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern*, J. Reine Angew. Math. **268/269** (1974), Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II, 41-52.

[BGS96] A. Beilinson, V. Ginzburg and W. Soergel, *Koszul duality patterns in representation theory*, J. Amer. Math. Soc. **9** (2996), no. 2, 473-527.

[Ber78] G.M. Bergman, *The Diamond Lemma for Ring Theory*, Advances in Mathematics **29** (1978), 178-218.

[BK86] S. Bloch and K. Kato, *p-adic étale cohomology*, IHES Publ. Math. (1986), no. 63, 107-152.

[CM82] A.B. Carson and M. Marshal, *Decompositions of Witt rings*, Canad. J. Math. **34** (1982), no. 6, 1276-1302.

[CEM12] S.K. Chebolu, I. Efrat and J. Mináč, *Quotients of absolute Galois groups which determine the entire Galois cohomology*, Math. Ann. **352** (2012), no. 1, 205-221.

[Con00] A. Conca, *Universally Koszul algebras*, Math. Ann. **317** (2000), no.2 , 329-346.

[CDR13] A. Conca, E. De Negri and M. E. Rossi, *Koszul algebras and regularity*, Commutative algebra: expository papers dedicated to David Eisenbud on the occasion of his 65th birthday, 285-315, Springer, New York, 2013.

[CTV01] A. Conca, N.V. Trung and G. Valla, *Koszul property for points in projective spaces*, Mathematica Scandinavica **89** (2001), no. 2, 201-216.

[Cor82] C.M. Cordes, *Quadratic forms over fields with four quaternion algebras*, Acta Arith. **41** (1982), no. 1, 55-70.

[Dem61] S.P. Demushkin, *The group of a maximal p-extension of a local field*, Izvestiya Rossiskoi Akademii Nauk. Seriya Matematicheskaya **25** (1961), no.3, 329-346.

[Dem63] S.P. Demushkin, *On 2-extensions of a local field*, Sibirsk. Math. Z. **4** (1963), no.4, 951-955.

[Dic07] L.E. Dickson, *On quadratic forms in a general field*, Bull. Amer. Math. Soc **14** (1907), no.3, 108-115.

[DSMS99] J.D. Dixon, M.P.F. Du Sautoy, A. Mann and D. Segal, *Analytic pro-p-groups*, Cambridge Studies in Advanced Mathematics **61**, Cambridge University Press, Second Edition, 1999.

[EH12] V. Ene and J. Herzog, *Gröbner bases in commutative algebra*, Graduate Studies in Mathematics **130**, AMS, Providence, RI, 2012.

[Eis95] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer-Verlag, New York, 1995.

[EL72] R. Elman and T.-Y. Lam, *Quadratic forms over formally real fields and pythagorean fields*, American Journal of Mathematics **94** (1972), no. 4, 1155-1194.

[EM17] I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, J. Eur. Math. Soc. (JEMS) **19** (2017), 3629-3640.

[GM] P. Guillot and J. Mináč, *Extensions of unipotent groups, Massey products and Galois cohomology*, arXiv preprint arxiv:1711.07711

[GMTW18] P. Guillot, J. Mináč, A. Topaz, *Four-fold Massey products in Galois cohomology*, With an appendix by O. Wittenberg, Compos. Math. **154** (2018), no. 9, 1921-1959.

[HHR00] J. Herzog, T. Hibi and G. Restuccia, *Strongly Koszul Algebras*, Mathematica Scandinavica **86** (2000), no. 2, 161-178.

[Hil90] D. Hilbert, *Ueber die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), no. 4, 473-534.

[HW15] M.J. Hopkins and K.G. Wickelgren, *Splitting varieties for triple Massey products*, J. Pure Appl. Algebra **219** (2015), no. 5, 1304-1319.

[Jac81] B. Jacob, *On the structure of Pythagorean fields*, J. Algebra **68** (1981), no. 2, 247-267.

[Kat80] K. Kato, *A generalization of local class field theory by using K-groups*, J. Fac. Sci. U. Tokyo **27** (1980), 603-683.

[Koch02] H. Koch, *Galois Theory of p-Extensions*, Springer Monographs inn Mathematics, Springer-Verlag, 2002.

[Kul79] M. Kula, *Fields with prescribed quadratic form schemes*, Math. Z. **167** (1979), no. 3, 201-212.

[Kul85] M. Kula, *Fields and quadratic form schemes*, Ann. Math. Sil. (1985), no. 13, 7-22.

[Lab67] J. Labute, *Classification of Demushkin groups* Canad. J. Math **19** (1967), 106-132.

[Lam05] T.-Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics **67**, AMS, Providence, RI 2005.

[LV12] J.-L. Loday and B. Valette, *Algebraic operads*, GMW **346**, Springer, Heidelberg, 2012.

[Mar80] M. Marshall, *Abstract Witt rings*, Queen's Papers in Pure and Applied Mathematics, vol. 57, Queen's University, Kingston, Ontario, 1980.

[Mer81] A. Merkurjev, *On the norm residue symbol of degree* 2, Dokl. Akad. Nauk SSSR **261** (1981), no. 3, 542-547.

[MeSu82] A. Merkurjev and A. Suslin, *K-cohomology of Severy-Brauer varieties and the norm residue homomorphism*, Math. USSR Izvestiya **21** (1982) 307-340.

[MeSu90] A. Merkurjev and A. Suslin, *Norm residue homomorphism of degree* 3, Izv. Akad. Nauk SSSR Ser. Mat. **54** (1990), no. 2, 239-356.

[Mil70] J. Milnor, *Algebraic K-theory and quadratic forms*, Invent. Math. **9** (1970), 357-364.

[Min86] J. Mináč, *Galois groups of some 2-extensions of ordered fields*, C.R. Math. Rep. Acad. Sci. Canada **8** (1986), no. 2, 103-108.

[MPPT] J. Mináč, M. Palaisti, F.W. Pasini and N.D. Tân, *Enhanced Koszul properties in Galois cohomology*, arXiv preprint arxiv:1811.09272.

[MPQT] J. Mináč, F.W. Pasini, C. Quadrelli and N.D. Tân, *Koszul algebras and quadratic duals in Galois cohomology*, arXiv preprint arxiv:1808.01695.

[MRT] J. Mináč, M. Rogelstad and N.D. Tân, *Relations in the maximal pro-p quotients of absolute Galois groups*, arXiv preprint arXiv:1808.01705.

[MiSp96] J. Mináč and M. Spira, *Witt rings and absolute Galois groups*, Ann. Math (2) **144** (1996), no. 1, 35-60.

[MT16] J. Mináč and N.D. Tân, *Triple Massey products vanish over all fields*, J. Lond. Math. Soc (2) **94** (2016), no. 3, 909-932.

[MT17] J. Mináč and N.D. Tân, *Triple Massey products and Galois theory*, J. Eur. Math. Soc. (JEMS) **18** (2017), no. 1, 255-284.

[NSW08] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, Second edition, G.M.W. **323**, Springer-Verlag, Berlin, 2008.

[OVV07] D. Orlov, A. Vishik and V. Voevodsky, *An exact sequence for $K_*^M/2$ with applications to quadratic forms*, Ann. of Math. (2) **165** (2007), no. 1, 1-13.

[Pal] M. Palaisti, *Koszul algebras, the Bloch-Kato Conjecture and Galois cohomology*, in preparation.

[Pio01] D.I. Piontkovskii, *On the Hilbert series of Koszul algebras*, Funct. Anal. Appl. **35** (2001), no. 2 133-137.

[Pio05] D.I. Piontkovskii, *Koszul algebras and their ideals*, Funct. Anal. Appl. **39** (2005), no. 2, 120-130.

[PP05] A. Polishchuk and L. Positselski, *Quadratic algebras*, University Lecture Series **37**, American Mathematical Society, Providence, RI, 2005.

[Pos95] L. Positselski, *The correspondence between the Hilbert series of dual quadratic algebras does not imply their having the Koszul property*, Funct. Anal. Appl. **29** #3 (1995), 213-217.

[Pos05] L. Positselski, *Koszul property and Bogomolov's conjecture*, Int. Math. Res. Not. **31** (2005), 1901-1936.

[Pos14] L. Positselski, *Galois cohomology of a number field is Koszul*, J. Number Theory **145** (2014), 126-152.

[PV95] L. Positselski and A. Vishik, *Koszul duality and Galois cohomology*, Math. Res. Lett. **2** no. 6 (1995), 771-781.

[Pri70] S. Priddy, *Koszul resolutions and the Steenrod algebra*, Bull. Amer. Math. Soc. **76** (1970), no. 4, 834–839.

[Qua] Claudio Quadrelli, *One relator maximal pro-p Galois groups and Koszul algebras*, arXiv preprint arXiv:1601.04480.

[Roo95] J.-E. Roos, *On the characterization of Koszul algebras. Four counter-examples* Rendus Acad. Sci. Paris ser. I **321** #1 (1995), 15-20.

[Ros86] M. Rost, *On Hilbert Satz* 90 *for K_3 of degree-two extensions* (1986), http://www.mathematik.unibielefel.de/∼rost/K3-86.html.

[Ser62] J.-P. Serre, *Structure de certains pro-p-groupes*, Séminaire Bourbaki **63** (1962), 357-364.

[Ser64] J.-P. Serre, *Galois cohomology*, Lecture Notes in Mathematics **5**, Springer, 1964.

[Sha72] S.S. Shatz, *Profinite groups: Arithmetic and Geometry*, Annals of Mathematical Studies **67**, Princeton University Press, 1972.

[Tat76] J. Tate, *Relations between K_2 and Galois cohomology*, Inventiones Math. **36** (1976), 257-274.

[Voe03] V. Voevodsky, *Motivic cohomology with $\mathbb{Z}/2$-coefficients*, Publ. Math. IHÉS **98** (2003), no 1., 59-104.

[Voe11] V. Voevodsky, *On motivic cohomology with $\mathbb{Z}/l$-coefficients*, Ann. of Math. (2) **174** (2011), no. 1, 401–438.

[Wad83] A.R. Wadsworth, *p-Henselian fields: K-theory, Galois cohomology and graded Witt rings*, Pacific J. Math. **105** (1983), no. 2, 473-496.

[War78] *When are Witt rings group rings? II* Pacific J. Math. **76** (1978), no.2, 541-564.

[Wei95] C.A. Weibel, *An introduction to homological algebra*, Cambridge University Press, 1995.

[Wit37] E. Witt, *Theorie de quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. **176** (1937), 31-44.

Curriculum Vitae

Name:	Marina Palaisti	
Post-Secondary Education and Degrees:	Western University London, Ontario, Canada Ph.D. Mathematics	2019
	Aristotle University of Thessaloniki Thessaloniki, Greece M.Sc. Pure Mathematics	2014
Honors and Awards:	Faculty of Science Graduate Teaching Award	2016
	Western Graduate Research Scholarship	2015-2018
Related Work Experience:	Assistant Professor Huron University College, London, Ontario, Canada	2018 - present
	Teaching Assistant Western University, London, Ontario, Canada	2015-2018

Publications:

- J. Mináč, M. Palaisti, F.W. Pasini and N.D. Tân, *Enhanced Koszul properties in Galois cohomology* (2018), submitted.
- M. Palaisti, *Koszul algebras, the Bloch-Kato Conjecture and Galois cohomology* (2018), in preparation.
- A. Chapman, J. Mináč, M. Palaisti and N.D. Tân, *Rost's Chain Equivalence and Galois theory*, in preparation.

- J. Mináč and M. Palaisti, *Chain Equivalence and Galois groups of global fields*, in preparation.

- M. Palaisti, *Tate duality*, expository article, 2017.

- M. Palaisti, *Topics in Linear Algebraic groups*, expository article with a slight generalization of a Theorem, 2016.

- M. Palaisti, *A glimpse towards the Bloch-Kato Conjecture*, expository article, 2016.

- M. Palaisti, *Milnor's Conjecture*, expository article, 2015.