INAUGURAL – DISSERTATION

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

vorgelegt von
Dipl.-Math. Sebastian Basten
aus Frankfurt am Main

Tag der mündlichen Prüfung: 14.04.2011

Thema

The arithmetic lifting property for nilpotent groups

Gutachter: Prof. Dr. Bernd Heinrich Matzat

Prof. Dr. Michael Dettweiler

Abstract

In this thesis it is shown that every finite nilpotent group has the arithmetic lifting property over $\mathbb{Q}^{ab}$, the maximal abelian extension of the field of rational numbers.
For a group G to have the arithmetic lifting property over a field K means that every Galois extension M/K with Galois group G can be obtained from a Galois extension $\tilde{M}/K(t)$, regular over K, with Galois group G by replacing the variable t with an element of K. In particular it is shown that every finite nilpotent group can be realized regularly as Galois group over $\mathbb{Q}^{ab}(t)$.

Zusammenfassung

In dieser Arbeit wird gezeigt, dass jede endliche nilpotente Gruppe die Arithmetische Liftungseigenschaft über $\mathbb{Q}^{ab}$ hat, der maximalen abelschen Erweiterungen des Körpers der rationalen Zahlen.
Hierbei hat eine Gruppe G die Arithmetische Liftungseigenschaft über eine Körper K, wenn jede Galoiserweiterung M/K mit Galoisgruppe G aus einer über K regulären Erweiterung $\tilde{M}/K(t)$ gewonnen werden kann, indem die Variable t durch ein Element aus K ersetzt wird. Insbesondere wird nachgewiesen, dass jede endliche nilpotente Gruppe regulär über $\mathbb{Q}^{ab}(t)$ realisiert werden kann.

Contents

Introduction

The original *Noether problem* formulated by E. Noether in [Noether1] poses the question, whether the fixed field of a permutation group G which acts on a rational function field by permuting the indeterminates is again purely transcendental over the base field. When this is the case, it is possible to obtain a parameterization for all polynomials with Galois group G. Even very small groups do not necessarily have this property: The first counterexamples over the field of rational numbers $\mathbb{Q}$ are abelian groups which contain at least one element of order 8 by [Lenstra1] and C_{47}, the cyclic group of order 47, by [Swan1].

A weaker property of a group G is the existence of *generic polynomials* for this group over a given field K. A generic polynomial is a polynomial $g(t_1, ..., t_n, X)$ which has Galois group G over the rational function field $K(t_1, .., t_n)$ in n indeterminates such that all Galois extensions M/K' of all fields $K' \supseteq K$ can be obtained by specializing the t_i to values $a_i \in K'$ and taking the splitting field of $g(a_1, ..., a_n, X)$. For infinite fields the existence of generic polynomials for a given group is equivalent to the existence of *generic extensions* as described in [Saltman1]. Generic polynomials over $\mathbb{Q}$ exist, for example, for all cyclic groups of odd order, thus for some groups which do not have the properties considered in the Noether problem. For abelian groups which contain elements of order 8, generic polynomials still do not exist by [Saltman1].

If there are no generic polynomials for a given group over a given field, one can ask if there is a "weaker specialization property" which is satisfied by this group. The *arithmetic lifting property*, formulated for the first time in [Beckmann1] in 1992, is such a property. By definition a finite group G has the *arithmetic lifting property* over a given field K if every G-extension M/K is a specialization of a G-extension $\tilde{M}/K(t)$ of $K(t)$, the rational function field in one variable, that is regular over K.

$$\begin{tikzcd}
& \hat{M} \arrow[dl, dash, "G"'] \arrow[dr, dash] & \\
K(t) \arrow[dr, dash] & & M \arrow[dl, dash, "G"] \\
& K &
\end{tikzcd}$$

In this context, a field extension $\tilde{M}/K(t)$ is called *regular (over K)* or *geometric*, if $\bar{K} \cap \tilde{M} = K$ for every algebraic closure $\bar{K}$ of K.

The existence of generic polynomials for a certain group implies the arithmetic lifting property for this group. But the arithmetic lifting property is a weaker property than the existence of generic polynomials. In the very first treatment of the arithmetic lifting property in [Beckmann1] it is proven that all abelian groups have the arithmetic lifting property over $\mathbb{Q}$.

Since the arithmetic lifting property is stable under the formation of certain group products and group extensions, it is possible to construct a wide array of groups for which no generic polynomials exist but which still have have the arithmetic lifting property. A list of groups which have the arithmetic lifting property is contained in the final chapter of this thesis. One important result for the considerations done in this text is the following: Let K be a field, and let G_1 and G_2 be groups which have the arithmetic lifting property over K. Then the direct product $G_1 \times G_2$ has the arithmetic lifting property over K, too.

For now, even over $\mathbb{Q}$ no group is know that does not have the arithmetic lifting property. The conjecture that every finite group has the arithmetic lifting property over an arbitrary number field, mentioned for the first time in [Black1], is called the *Beckmann-Black-Conjecture*. On the other hand for a group G to have the arithmetic lifting property over a field K implies that there exist realizations for G over $K(t)$ that are regular over K. The question if a given finite group has the arithmetic lifting property, however, is not answered for general finite groups over many fields. The “weaker” question if every finite group can be realized by an extension of $\mathbb{Q}(t)$ regular over $\mathbb{Q}$, was first posed by J.-P. Serre and is still a major open problem.

This thesis is concerned with the arithmetic lifting property for nilpotent groups over $\mathbb{Q}^{ab}$, the maximal abelian extension of $\mathbb{Q}$, and hence with regular realizations of nilpotent groups over the same field. Since every nilpotent group can be decomposed into a direct product of p-groups, and since the arithmetic lifting property is stable under the formation of direct products, this question can be reduced to the case of p-groups.

The most extensive result in this direction is due to J. Sonn. In [Sonn1] it is shown that there is a regular realization of every nilpotent group over the field $\mathbb{Q}^{solv}$, the maximal solvable extension of $\mathbb{Q}$. The paper is not, however, concerned with the arithmetic lifting property, and the methods can not be generalized or modified to realize nilpotent groups regularly over $\mathbb{Q}^{ab}$.

The only other results concerning the arithmetic lifting property for nilpotent groups are for small p-groups and dihedral groups. In [Ledet2] and in [Jensen1], Chapter 6, the question for generic polynomials, and hence for the arithmetic lifting property, for 2-groups up to the order of $2^4 = 16$ and p-groups up to the order of p^3 for odd p over $\mathbb{Q}$ is answered. In [Black1] and [Black2] the arithmetic lifting property is proven for dihedral groups of arbitrary order as long as sufficiently many roots of unity are contained in the base field. The diploma theses [DiGiacomo1] and [Basten1] are concerned with the arithmetic lifting property up to the order 2^6 or

p^4 for odd p over number fields that contain sufficiently many roots of unity.

The main result of this thesis is that every finite nilpotent group has the arithmetic lifting property over $\mathbb{Q}^{ab}$ and in fact over every field of characteristic zero and of cohomological dimension ≤ 1 that contains all roots of unity. Furthermore we see that every finite nilpotent group has an realization over $\mathbb{Q}^{ab}(t)$ that is regular over $\mathbb{Q}^{ab}$ and deduce that this assertion holds for every field that contains $\mathbb{Q}^{ab}$, generalizing the result of [Sonn1]. These results are contained in Section 3.3, see in particular the Main Theorem in this section and Corollary 3.3.3.

To prove that every finite p-group has the arithmetic lifting property over a field K of characteristic zero and of cohomological dimension ≤ 1 that contains all roots of unity, we use that every p-group has a non-trivial center and so every p-group can be constructed inductively by taking group extensions with cyclic kernel, starting from the trivial group. We do not, however, consider every single p-group separately. Instead we construct, in terms of generators and relations, a certain central series of p-groups in such a way that the groups are determined by as few relations as possible. In doing so, we obtain that every p-group can be realized as factor group of at least one of the groups of the series. This will be done in Section 2.1.

Since our field K contains all roots of unity, central group extensions lead to Brauer type embedding problems if the groups in question are Galois groups of extensions of K. This is quite useful, because there are very accessible solvability criteria for Brauer type embedding problems and moreover, if one solution to a Brauer type embedding problem is known, all other solutions can be obtained from this solution using one parameter. The necessary parts of the theory of Brauer type embedding problems are summarized in Section 2.2.

The proof that a certain group of our central series has the arithmetic lifting property is by induction on the nilpotency class of the groups in this series. In each step of the induction, we consider for a group E an E-extension F/K that is a solution to a Brauer type embedding problem given by a cyclic and central subgroup C_q of E, a factor group $E/C_q = G$ and a G-extension M/K. We assume that M/K is a specialization of a regular G-extension $\tilde{M}/K(t)$ and prove that the embedding problem given by E, G and $\tilde{M}/K(t)$ is also solvable, that the solution $\tilde{F}$ has Galois group E, and that $\tilde{F}$ specializes to F. This will be done in Section 3.2.

Aside from these considerations, we show in Section 3.1 that for a given group that has the arithmetic lifting property over a field K as described above, every factor group has the arithmetic lifting property as well. This allows us to infer from the fact that every group of our central series has the arithmetic lifting property over K that every finite p-group has the arithmetic lifting property over K. So, roughly speaking, to realize a given p-group G, we "embiggen the embedding problems" leading to the field having this group as Galois group, arrive at a larger field, "step down" to a subfield and thus arrive at the group G as factor group.

Danksagung

Mein Dank gilt zuallererst meinem Betreuer Prof. Dr. B.H. Matzat, der mich bei der Ausarbeitung meiner Doktorarbeit ausgezeichnet betreut hat und jederzeit für Fragen zur Verfügung stand. Darüberhinaus danke ich meiner Familie, die mich während meines Studiums und meiner Arbeit an dieser Doktorarbeit stets unterstützt hat.
Meiner Arbeitsgruppe danke ich für das sehr angenehme und freundschaftliche Arbeitsklima. Insbesondere gilt hierbei mein Dank Julia Hartmann, Andreas Maurischat und Michael Schulte, die diese Arbeit in verschiedenen Stadien gegengelesen haben.

A note on notation

H, G, E	Groups.
$Z(G)$	The center of a group G.
A	An abelian group.
C_q	The cyclic group of order q.
ρ	A generator of a group.
σ	An element of a group or a (basic) commutator.
τ	A generator of the kernel of a cyclic group extension.
F, M, K	Fields.
$K^\times$	The mulitplicative group of a field K.
$\tilde{K}$	$K(t)$.
$\tilde{M}$	A regular extension $\tilde{M}/\tilde{K}$ specializing to M/K.
$(M/K, E, G)$	An embedding problem where $\mathrm{Gal}(M/K) = G$ and E is a group extension with cokernel G.
ω	An element of a field. The solution field of a cyclic embedding problem $(M/K, E, G)$ is given by $M(\sqrt[q]{\omega})$.
$s(\sigma)$	A section of a group extension $s : G \to E$.
$c(\sigma_1, \sigma_2)$	A factor system mapping $\sigma_1, \sigma_2 \in G$ to a cyclic group C_q.
$R_\sigma(x)$	The term $x \cdot \sigma(x) \cdot ... \cdot \sigma^{q-1}(x)$, where $\sigma^q = 1$.
$\mathcal{F}$	A free group.
L_i, U_i	The subgroups of the lower or upper central series of a group.
cl	The nilpotency class of a nilpotent group.
w_i	Usually the weight of a commutator.
$\mathbf{A}_i,\ \mathbf{B}_j$	Sets of indeterminates $X_{i,\alpha}, Y_{j,\beta}$.
$\mathbf{a}_i,\ \mathbf{b}_j$	Sets of elements $x_{i,\alpha}, y_{j,\beta}$ of a field.

Chapter 1

Prerequisites

1.1 Specialization and valuations

This section introduces the *specialization* of a rational function field and summarizes the basic theory of discrete valuations. A more thorough account of these topics can be found in [Neukirch1], Chapter II.

Specializing means roughly the following: Let K be a field and $K(t)$ the function field in one variable over K. By $f(t,X)$ we denote an element in the polynomial ring $K(t)[X]$ such that $\tilde{M}/K(t)$ is a Galois extension of $K(t)$ given by $f(t,X)$. We choose some element $s \in K$ for which $f(s,X)$ is a polynomial in $K[X]$. Of course not every $s \in K$ will do; if we have for example $f(t,X) = \frac{1}{t-1} - X$, replacing t by 1 will not result in a polynomial in $K[X]$. But if $f(s,X) \in K[X]$ (and if $f(s,X)$ is separable) this process will yield a Galois extension M/K satisfying $[M:K] \leq [\tilde{M}:K(t)]$. This extension will be called a *specialization* of $\tilde{M}/K(t)$. We will make this precise:

Let $\tilde{M}$ be a field. A *discrete valuation* of $\tilde{M}$ is a map $v : \tilde{M} \rightarrow \mathbb{Z} \cup \{\infty\}$ such that the following holds:

$v(\tilde{a}\tilde{b}) = v(\tilde{a}) + v(\tilde{b})$
$v(\tilde{a}+\tilde{b}) \geq min\{v(\tilde{a}), v(\tilde{b})\}$
$v(\tilde{a}) = \infty \Longleftrightarrow \tilde{a} = 0$
There exists an element $\tilde{a} \in \tilde{M}^{\times}$ satisfying $v(\tilde{a}) \neq 0$.

The symbol ∞ satisfies the relations: $\infty + \infty = \alpha + \infty = \infty + \alpha = \infty$ and $\alpha < \infty$ for all $\alpha \in \mathbb{Z}$. Two discrete valuations $v_1,\ v_2$ are equivalent if they differ only by a constant, i.e. if there exists a $z \in \mathbb{Z}$ such that $z \cdot v_1(a) = v_2(a)$ for all $a \in \tilde{M}$.

A *place* of $\tilde{M}$ is a map $\varphi : \tilde{M} \rightarrow M \cup \{\infty\}$ for a field M, such that the following holds:

$\varphi(\tilde{a}\tilde{b}) = \varphi(\tilde{a})\varphi(\tilde{b})$
$\varphi(\tilde{a}+\tilde{b}) = \varphi(\tilde{a}) + \varphi(\tilde{b})$
There exists an element $\tilde{a} \in F$ satisfying $\varphi(\tilde{a}) = \infty$.

There exists an element $\tilde{b} \in F$ satisfying $\varphi(\tilde{b}) \neq \infty$ and $\varphi(\tilde{b}) \neq 0$.

The symbol ∞ satisfies the relations: $\infty + \infty = \alpha + \infty = \infty + \alpha = \infty$ and $\alpha \cdot \infty = \infty \cdot \alpha = \infty$ for all $\alpha \in M$. The expressions $\infty \cdot \infty$ and $0 \cdot \infty$ are not defined. (Each of those equations is understood to hold if the right hand side of the equation is defined.) Two places $\varphi_1 : \tilde{M} \to M_1 \cup \{\infty\}$ and $\varphi_2 : \tilde{M} \to M_1 \cup \{\infty\}$ are *equivalent*, if there exists an isomorphism $\lambda : M_1 \to M_2$, such that $\lambda \circ \varphi_1 = \varphi_2$ holds.

In general, each equivalence class of places corresponds to an equivalence class of valuations: Assume we have a discrete valuation v and we want to construct the place φ corresponding to this valuation. The subring $\mathfrak{O}_v := \{a \in \tilde{M} \mid v(a) \geq 0\}$ of $\tilde{M}$ is the *valuation ring* of $\tilde{M}$ with respect to v. The ring $\mathfrak{O}_v$ has precisely one maximal ideal $\mathfrak{m}_v := \{a \in \tilde{M} \mid v(a) > 0\}$, hence $M_v := \mathfrak{O}_v/\mathfrak{m}_v$ is a field.

If we have $M_v := \mathfrak{O}_v/\mathfrak{m}_v$, the quotient map $\varphi : \mathfrak{O}_v \to M_v$ defines a place, denoted again by φ, $\varphi : \tilde{M} \to M_v \cup \infty$ via $\varphi(a) = \infty$ for all $a \in \tilde{M} \backslash \mathfrak{O}_v$.

Hence we have $\mathfrak{O}_v = \{a \in \tilde{M} \mid \varphi(a) < \infty\}$ and $\mathfrak{m}_v = \{a \in \tilde{M} \mid \varphi(a) = 0\}$. As we will be more interested in the place φ than in the valuation v later on, we will denote the valuation ring and its maximal ideal belonging to v, and thus to φ, by $\mathfrak{O}_\varphi := \mathfrak{O}_v$ and $\mathfrak{m}_\varphi := \mathfrak{m}_v$, respectively from now on.

If K is a field, $\tilde{M}/K(t)$ a finite regular Galois extension and $s \in K$, we obtain from the polynomial $(t - s)$ via

$$v_s : \tilde{M}^\times \longrightarrow \mathbb{Z},\ \tilde{f} = \tilde{u}(t-s)^m \mapsto m,$$

a discrete valuation of $\tilde{M}$. The corresponding place will be denoted by φ_s. The valuation ring of $\tilde{M}$ with respect to $(t - s)$ is

$$\mathfrak{O}_{\varphi_s} := \left\{ \frac{\tilde{f}}{\tilde{g}} \mid \tilde{f} \in \tilde{M},\ \tilde{g} \in \tilde{M} \text{ und } (t-s) \nmid \tilde{g} \right\}$$

and its maximal ideal is $\mathfrak{m}_{\varphi_s} := \mathfrak{O}_{\varphi_s}(t - s)$. The quotient map

$$\varphi_s : \mathfrak{O}_{\varphi_s} \longrightarrow M_{\varphi_s} := \mathfrak{O}_{\varphi_s}/\mathfrak{m}_{\varphi_s},\ t \mapsto s$$

gives, as above, the place $\varphi_s : \tilde{M} \to M_{\varphi_s} \cup \{\infty\}$. This place will be called *specialization* of $\tilde{M}$ at s. If the Galois extension $\tilde{M}/K(t)$ is given by a polynomial $f(t, X)$ with coefficients in $\mathfrak{O}_{\varphi_s}$ we obtain a polynomial $f(s, X)$ for the extension M_{φ_s}/K by replacing the coefficients of $f(t, X)$ with their images under φ_s.

For arbitrary fields and an arbitrary valuation v, the degree of the extension M_v/K will be smaller than the degree of the extension $\tilde{M}/K(t)$. We have however the following result due to D. Hilbert:

Theorem 1.1.1. (Hilbert's Irreducibility Theorem) *Let $f(t, X)$ be an irreducible polynomial in $\mathbb{Q}(t)[X]$. Then there exists an $s \in \mathbb{Q}$ such that the specialization $f(s, X)$ is irreducible in $\mathbb{Q}[X]$.*

Since an irreducible polynomial $f(s,X) \in \mathbb{Q}[X]$ gives rise to a Galois extension of $\mathbb{Q}$, this theorem leads to

Corollary 1.1.2. *If a finite group G can be realized as the Galois group of a Galois extension $\tilde{M}/\mathbb{Q}(t)$, then it can be specialized to a Galois extension $M/\mathbb{Q}$ with G as its Galois group.*

For a proof of these statements see for example [Jensen1], *Proposition 3.1.2.*

The field of rational numbers is not the only field that satisfies the property described in Hilbert's Irreducibility Theorem. In general, all fields for which the assertion of Theorem 1.1.1 holds, are called *Hilbertian.* Examples of Hilbertian fields are all algebraic number fields and the field $\mathbb{Q}^{ab}$, the maximal abelian extension of $\mathbb{Q}$, see [Weissauer1].

1.2 Some basic invariant theory

Let K be a field of characteristic zero and let $K[T_1,...,T_n]$ denote the polynomial ring over K in n variables $T_1,..,T_n$. Let G be a subgroup of S_n, the symmetric group of degree n, which acts on $K[T_1,...,T_n]$ by permutation of the indeterminates $T_1,...,T_n$. Let $K[T_1,...,T_n]^G$ denote the subring of invariants of $K[T_1,...,T_n]$ under the action of G.

Example: If $G = S_n$ then $K[T_1,...,T_n]^{S_n} = K[k_0,...,k_{n-1}]$, where $k_0,...,k_{n-1}$ denote the elementary symmetric polynomials in $T_1,...,T_n$.

For an arbitrary finite group G, however, $K[T_1,...,T_n]^G$ will in general be generated by more, but still finitely many, invariants:

Theorem 1.2.1. *Under the assumptions above, the ring $K[T_1,...,T_n]^G$ is a ring generated by finitely many invariants $k_0,...,k_r$.*

This is a classical result of Hilbert, see [Smith1], Chapter 2.1 for example, and even holds for more general linear actions. It is in fact possible to compute the invariants algorithmically:

Theorem 1.2.2. *Under the assumptions above, the ring $K[T_1,...,T_n]^G$ is a ring generated by at most $\binom{n+\mathrm{ord}\, G}{\mathrm{ord}\, G}$ elements of degree at most* ord G.

This theorem is a special case of a theorem by E. Noether and can be found in a more general form in [Smith1] as Corollary 2.4.3. The proof of Theorem 1.2.2 yields an algorithm to compute a set of invariants generating $K[T_1,...,T_n]^G$ as an algebra, see [Smith1] Chapter 2.3 for reference.

Theorem 1.2.3. *Under the assumptions above, let G act by permutation on the field $K(T_1,...,T_n) = \mathrm{Frac}(K[T_1,...,T_n])$. Then we have for the field of invariants $K(T_1,...,T_n)^G = \mathrm{Frac}(K[T_1,...,T_n]^G)$. In particular, it is possible to work with functions fields instead of polynomial rings.*

See [Smith1] Prop. 1.2.4 for reference.

Example: Assume the group $C_3 = \langle\sigma\rangle$ acts on $K[T_1, T_2, T_3]$ via

$$\sigma : (T_1, T_2, T_3) \mapsto (T_2, T_3, T_1).$$

As ord $C_3 = 3$, a generating set of $K[T_1, T_2, T_3]^{C_3}$ will consist of polynomials of degree at most 3. Using the algorithm given in [Smith1] Chapter 2.3 a generating set of invariants can be computed to be given by:

$$\begin{array}{rcl} k_0 & := & T_1 + T_2 + T_3, \\ k_1 & := & T_1T_2 + T_1T_3 + T_2T_3, \\ k_2 & := & T_1T_2T_3, \\ k_3 & := & T_1^2T_2 + T_2^2T_3 + T_3^2T_1. \end{array}$$

This set is minimal since k_0, k_1, k_2 are elementary symmetric polynomials and thus a minimal generating set of the symmetric polynomials in 3 variables and k_3 is not a symmetric polynomial. We see in this example that the ring of invariants

$$K[T_1, T_2, T_3]^{C_3} = K[k_0, k_1, k_2, k_3]$$

is generated by one more invariant than the ring of invariants

$$K[T_1, T_2, T_3]^{S_3} = K[k_0, k_1, k_2].$$

We will use these results in Section 3.2 for a Galois extension L/K of degree n given by an irreducible polynomial $f(X)$ with roots $\theta_1, ..., \theta_n$. In this situation we have $L = K[\theta_1, ..., \theta_n]$ and the Galois group of L/K acts on L by permutation of the θ_i. Hence the results of this section can be used by specializing T_i to θ_i. To illustrate this, we return to the example above:

Example: Let K be a field and assume that the third roots of unity are contained in K. Then, by Kummer theory, a C_3 extension of K is given for example by the polynomial

$$f(X) = X^3 - 2.$$

The roots of this polynomial are

$$\theta_1 = \sqrt[3]{2},\ \theta_2 = \zeta \cdot \sqrt[3]{2},\ \theta_3 = \zeta^2 \cdot \sqrt[3]{2}$$

where ζ denotes a primitive third root of unity. The splitting field of $f(X)$ is given by

$$M = K(\sqrt[3]{2}) = [\sqrt[3]{2}, \zeta \cdot \sqrt[3]{2}, \zeta^2 \cdot \sqrt[3]{2}] = K[\theta_1, \theta_2, \theta_3]$$

and we have $M^{C_3} = K$. Since C_3 acts on the roots of $f(X)$ by permutation, we look at the ring $K[T_1, T_2, T_3]$. We know from the previous example that the ring of invariants $K[T_1, T_2, T_3]^{C_3}$ is generated by

$$\begin{array}{rcl} k_0 & := & T_1 + T_2 + T_3, \\ k_1 & := & T_1T_2 + T_1T_3 + T_2T_3, \\ k_2 & := & T_1T_2T_3, \\ k_3 & := & T_1^2T_2 + T_2^2T_3 + T_3^2T_1. \end{array}$$

Specializing these invariants to roots of the minimal polynomial $f(X)$ yields:

$$\begin{array}{rcl} l_0 & := & \theta_1 + \theta_2 + \theta_3, \\ l_1 & := & \theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3, \\ l_2 & := & \theta_1\theta_2\theta_3, \\ l_3 & := & \theta_1^2\theta_2 + \theta_2^2\theta_3 + \theta_3^2\theta_1. \end{array}$$

A calculation shows that these invariants indeed lie in K:

$$\begin{array}{rcl} l_0 & = & \sqrt[3]{2} + \zeta \cdot \sqrt[3]{2} + \zeta^2 \cdot \sqrt[3]{2} = 0 \cdot \sqrt[3]{2} = 0, \\ l_1 & = & \sqrt[3]{2} \cdot \zeta \cdot \sqrt[3]{2} + \sqrt[3]{2} \cdot \zeta^2 \cdot \sqrt[3]{2} + \zeta \cdot \sqrt[3]{2} \cdot \zeta^2 \cdot \sqrt[3]{2} = 0 \cdot \sqrt[3]{2}^2 = 0, \\ l_2 & = & \sqrt[3]{2} \cdot \zeta \cdot \sqrt[3]{2} \cdot \zeta^2 \cdot \sqrt[3]{2} = 1 \cdot \sqrt[3]{2} = 2, \\ l_3 & = & \sqrt[3]{2}^2 \cdot \zeta \cdot \sqrt[3]{2} + \zeta^2 \cdot \sqrt[3]{2}^2 \cdot \zeta^2 \cdot \sqrt[3]{2} + \zeta^4 \cdot \sqrt[3]{2}^2 \sqrt[3]{2} = 3 \cdot \zeta \cdot \sqrt[3]{2}^3 = 6 \cdot \zeta. \end{array}$$

Hence we obtain again $K[\theta_1, \theta_2, \theta_3]^{C_3} = K[0, 0, 2, 6 \cdot \zeta] = K$.

1.3 The arithmetic lifting property

1.3.1 The Noether problem and generic polynomials

The original *Noether problem* formulated by E. Noether in [Noether1] poses the question, if the fixed field of a permutation group G, that acts on a function field by permuting the indeterminates, is again purely transcendental over the base field. When this is the case, it is possible to obtain a parameterization for all polynomials with Galois group G. Even very small groups do not have this property: The first counterexamples over the field of rational numbers $\mathbb{Q}$ are abelian groups which contain at least one element of order 8 by [Lenstra1] and C_{47}, the cyclic group of order 47, by [Swan1].

A weaker property of a group G is the existence of *generic polynomials* for this group over a given field K. A generic polynomial is a polynomial $g(t_1, ..., t_n, X)$ which has Galois group G over the rational function field $K(t_1, .., t_n)$ in n indeterminates such that all Galois extensions M/K' of all fields $K' \supseteq K$ can be obtained by specializing the t_i to values $a_i \in K'$ and taking the splitting field of $g(a_1, ..., a_n, X)$. For infinite fields the existence of generic polynomials for a given group is equivalent to the existence of *generic extensions* as described in [Saltman1]. Generic polynomials over $\mathbb{Q}$ exist, for example, for all cyclic groups of odd order, thus for some groups which do not have the properties considered in the Noether problem. For abelian groups which contain elements of order 8, generic polynomials still do not exist by [Saltman1].

1.3.2 The arithmetic lifting property

If there do not exist generic polynomials for a given group over a given field, one can ask if there is a "weaker specialization property" which is satisfied by this group. The *arithmetic lifting property*, formulated for the first time in [Beckmann1], is such a property.

Definition: A field extension $\tilde{M}/K(t)$ is *regular (over K)* or *geometric*, if $\bar{K} \cap \tilde{M} = K$ for every algebraic closure $\bar{K}$ of K.

Definition: Let K be an arbitrary field and $K(t)$ the function field in one indeterminate. A finite group G has the *arithmetic lifting property* over K, if every G-extension M/K is a specialization of a G-extension $\tilde{M}/K(t)$ of $K(t)$ regular over K.

$$\begin{tikzcd}
& \tilde{M} \arrow[dl, dash, "G"'] \arrow[dr, dash] & \\
K(t) \arrow[dr, dash] & & M \arrow[dl, dash, "G"] \\
& K &
\end{tikzcd}$$

The existence of generic polynomials for a certain group implies the arithmetic lifting property for this group. A proof can be found in Chapter 3 of [Jensen1].

The arithmetic lifting property is a weaker property than the existence of generic polynomials. In the very first treatment of the arithmetic lifting property in [Beckmann1] this property is proven for all abelian groups over $\mathbb{Q}$:

Theorem 1.3.1 ([Beckmann1], Theorem 2.4)**.** *Let K be an algebraic number field and G an abelian group. Then G has the arithmetic lifting property over K.*

Since the arithmetic lifting property is stable under the formation of certain group products and group extensions, it is possible to construct a wide array of groups for which no generic polynomials exist but that still have have the arithmetic lifting property. A list of groups which have the arithmetic lifting property is contained in the appendix. One important result used in this thesis is the following:

Theorem 1.3.2 ([Black3], Corollary 2.2)**.** *Let K be a field, and let G_1 and G_2 be groups which have the arithmetic lifting property over K. Then the direct product $G_1 \times G_2$ has the arithmetic lifting property over K.*

Proof. Let M/K be a $G_1 \times G_2$-extension. We have to find a $G_1 \times G_2$-extension $\tilde{M}/K(t)$, regular over K, that specializes to M/K. By [Lang1], Chapter VI, Thm. 1.14, there exist subextensions M_1/K, M_2/K, linearly disjoint over K, such that $\mathrm{Gal}(M_1/K) = G_1$, $\mathrm{Gal}(M_2/K) = G_2$ and such that $M = M_1 \otimes_K M_2 = M_1 M_2$. By assumption there are a G_1-extension $\tilde{M}_1/K(t)$ and G_2-extension $\tilde{M}_2/K(t)$, both regular over K, that specialize to M_1 and M_2. Without loss of generality we can assume that the specialization maps $\varphi_1 : \tilde{M}_1 \to M_1$ and $\varphi_1 : \tilde{M}_2 \to M_2$ are given by $\varphi_1 : t \mapsto 0$ and $\varphi_2 : t \mapsto 0$, or, in other words, that the prime ideals of the valuation rings $\mathfrak{O}_{\varphi_1}$ and $\mathfrak{O}_{\varphi_2}$ are given by (t) in both cases.
We then have that $\tilde{M}_1$ and $\tilde{M}_2$ are linearly disjoint over $K(t)$ because they specialize to linearly disjoint extensions at $t = 0$. So $\tilde{M} := \tilde{M}_1 \otimes_{K(t)} \tilde{M}_2 = \tilde{M}_1 \tilde{M}_2$ is a $G_1 \times G_2$-extension of $K(t)$. This extension is regular over K because it is composed of regular extensions and clearly specializes to M at $t = 0$. □

For now no group is known that does not have the arithmetic lifting property even over $\mathbb{Q}$. The conjecture that every finite group has the arithmetic lifting property over an arbitrary number field, mentioned for the first time in [Black1], is called the *Beckmann-Black-Conjecture.*

1.3.3 The arithmetic lifting property for nilpotent groups

Every nilpotent group is the direct product of p-groups, by Theorem 2.1.2. So the question whether a given nilpotent group has the arithmetic lifting property over a given field or not can usually be reduced to the question if the p-groups appearing in this decomposition have the arithmetic lifting property.

Concerning the question of the arithmetic lifting property of p-groups, several results have been obtained in the past.

[Ledet2] and [Jensen1], Chapter 6 deal with the question for generic polynomials for 2-groups up to order $2^4 = 16$ and p-groups up to order p^3 for odd p over $\mathbb{Q}$. In [Black1] and [Black2] the arithmetic lifting property is proven for dihedral groups of arbitrary order, as long as sufficiently many roots of unity are contained in the base field. The diploma theses [DiGiacomo1] and [Basten1] are concerned with the arithmetic lifting property up to order 2^6 or p^4 for odd p over number fields that contain sufficiently many roots of unity.

In the present thesis, the approach of [Basten1] is generalized and used to prove the arithmetic lifting property for arbitrary finite p-groups over the field $\mathbb{Q}^{ab}$, the maximal abelian extension of $\mathbb{Q}$.

Chapter 2

p-groups and embedding problems

2.1 p-groups

In this section, basic properties of finite p-groups are summarized. A reference for the introduction to the theory of p-groups is [McKay1], a more extensive account is [Leedham1].

2.1.1 Nilpotent groups

Definition: Let p be a prime. A *finite p-group* is a finite group whose order is a power of p.

Definition: The *upper (or ascending) central series* of a group G is the series

$$U_0(G) \leq U_1(G) \leq U_2(G) \leq ...$$

of normal subgroups of G defined inductively by

$$U_0(G) = \langle 1 \rangle \text{ and } U_i/U_{i-1} = Z(G/U_{i-1}(G)) \text{ for } i > 0.$$

G is *nilpotent* if there exists an integer n such that $U_n(G) = G$. If G is nilpotent, the *nilpotency class cl* of G is the smallest positive integer $cl \geq 1$ such that $U_{cl}(G) = G$.

Definition: The *lower (or descending) central series of* of a group G is the series

$$G = L_1(G) \geq L_2(G) \geq L_3(G) \geq ...$$

of subgroups of G defined inductively by

$$L_1(G) = G \text{ and } L_i = [L_{i-1}, G] \text{ for } i > 1.$$

Two of the most basic results on nilpotent groups are summarized in the following two theorems:

Theorem 2.1.1. *The following are equivalent:*

(i.) G is nilpotent of class cl.

(ii.) $G = L_1(G) > L_2(G) > .... > L_{cl+1}(G) = \langle 1\rangle$.

(iii.) $\langle 1\rangle = U_0(G) < U_1(G) < .... < U_{cl}(G) = G$.

Theorem 2.1.2. *If G is a finite nilpotent group, then G is the direct product of its p-Sylow subgroups. Hence a finite nilpotent group is a direct product of finite p-groups.*

The first theorem can be found as Lemma 1.1.20 in [Leedham1], the second as Theorem 5.39 in [Rotman1]. Since factor groups of nilpotent groups are again nilpotent, every finite p-group is a nilpotent group as well.

2.1.2 Commutators and collection

This section summarizes the necessary definitions and facts about the collecting process for commutators. It is mainly taken from [McKay1], Chapter 3.

Definition: Let $\mathcal{F}_d$ be a finitely generated free group on d generators ρ_i, $i = 1, .., d$. The *formal commutators* in ρ_i and their *weights* and *orders* are defined as follows.

(i.) The generators ρ_i are formal commutators of weight 1.

(ii.) If σ_i, σ_j are formal commutators of weight w_i and w_j then $[\sigma_i, \sigma_j]$ is a formal commutator of weight $w_i + w_j$.

(iii.) Every formal commutator arises this way.

(iv.) The formal commutators are given an ordering relation "<", which is defined as follows:

(a) If σ_i has smaller weight than σ_j then $\sigma_i < \sigma_j$.

(b) If $i < j$ then $\rho_i < \rho_j$.

(c) Beside these conditions the ordering is chosen arbitrarily.

It is clear that an ordering as described in (iv.) can always be chosen but it is not unique. It depends on the enumeration of the generators ρ_i, and for a given weight $w \in \mathbb{N}$ the commutators of weight w can be ordererd arbitrarily. So if there are n commutators of weight w, the commutators of weight w can be ordered in $n!$ ways, each way defining a different ordering. We assume from now that an arbitrary but fixed ordering has been chosen according to the rules above when we deal with commutators.

It is important to note that these are "formal" commutators in the sense that they are expressions involving ρ_i and [,] built up according to the rules in the definition. If the ρ_i are elements of a group G, commutators in the ρ_i can also be evaluated in G to give elements in G. There will then be relations between these elements. Some such relations will depend on the actual group G. Others will hold in all groups, for example, $[\rho_i, \rho_i] = 1$, $[\rho_i, \rho_j][\rho_j, \rho_i] = 1$. Hence it is possible to speak of the weight of a commutator in a (finite) group G, but an element of that group may be represented by different commutators of different weights. This problem will be dealt with when *basic commutators* are defined. These are chosen in a way that they are independent in the sense that they do not satisfy such “automatic” relations. Before we come to this, we examine what a commutator in a given group G looks like:

Definition: Let G be an arbitrary group. If $\sigma_1, \sigma_2 \in G$ then the *commutator* $[\sigma_1, \sigma_2]$ of σ_1 with σ_2 is $\sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2$.
If $\sigma_1, ..., \sigma_n \in G$ then the *left normed commutator* $[\sigma_1, ..., \sigma_n]$ for $n > 2$ is defined inductively to be $[[\sigma_1, ..., \sigma_{n-1}], \sigma_n]$. Note that the σ_i do not need to be distinct.

We will now describe the *collecting* process for commutators:

Definition: In an arbitrary product of commutators $\sigma_{i_1}\sigma_{i_2}...\sigma_{i_n}$ the *collected part* is the (possibly empty) section $\sigma_{i_1}\sigma_{i_2}...\sigma_{i_m}$ with m maximal subject to

$$\sigma_{i_1} \leq \sigma_{i_2} \leq ... \leq \sigma_{i_m}, \text{ and } \sigma_{i_m} \leq \sigma_{i_k} \text{ if } m < k \leq n,$$

and

$$\sigma_{i_{m+1}} > \sigma_{i_j} \text{ for some } j \text{ such that } m+1 < j \leq n,$$

and the *uncollected part* is the remaining section.

In a (not empty) product of commutators, let σ_u and k be such that

$$\sigma_u < \sigma_{i_j} \text{ for } m+1 \leq j < k \text{ and } \sigma_u = \sigma_{i_k} \text{ and } \sigma_u \leq \sigma_{i_j} \text{ for } k < j < n.$$

Now the commutator collecting process step replaces

$$\sigma_{i_1}...\sigma_{i_m}...\sigma_{i_{k-1}}\sigma_u\sigma_{i_{k+1}}...\sigma_{i_n}$$

by

$$\sigma_{i_1}...\sigma_{i_m}\sigma_u\sigma_{i_{m+1}}[\sigma_{i_{m+1}}, \sigma_u]...\sigma_{i_{k-1}}[\sigma_{i_{k-1}}, \sigma_u]\sigma_{i_{k+1}}...\sigma_{i_n}.$$

Notice that this new expression still represents the same element of the given group and has moved σ_u from the k-th position to the $(m+1)$-th position directly following σ_{i_m}. The collected part of the original product is undisturbed and the collected part of the new product is this with at least one extra term. The uncollected part contains several extra commutators but these are of higher weight than σ_u and so higher in the ordering. There is one less occurrence of σ_u in the new uncollected part, and so a finite number of applications of the collecting process step will move all occurrences of σ_u into the collected part, so that the smallest σ_v in the uncollected part satisfies $\sigma_u < \sigma_v$.

Definition: The process described above is called *collecting* σ_u.

There are two things that should be noted at this point: At first, in general collecting does not terminate. If we start with an arbitrary word, with every collected commutator new commutators of higher weight and order will arise in the uncollected part. The second point is that not all commutators arise when using the collecting process. For example $[\rho_i, \rho_i]$, $[\rho_1, \rho_2]$ are very simple examples of commutators that do not appear in this process. The *basic commutators* are designed to be the ones that do arise this way. Furthermore they are precisely those commutators that do not satisfy ”automatic“ relations.

Definition: Let ρ_i be generators of a finitely generated free group $\mathcal{F}_d$. Assume an ordering on the set of formal commutators of $\mathcal{F}_d$ has been chosen according to the rules in the above definition. The *formal basic commutators* in ρ_i are defined as follows.

(i.) ρ_i are basic commutators;

(ii.) $[\sigma_i, \sigma_j]$ is a basic commutator if and only if σ_i and σ_j are basic commutators with $\sigma_i > \sigma_j$ and if $\sigma_i = [\sigma_k, \sigma_l]$ with σ_k, σ_l basic commutators, then $\sigma_l \leq \sigma_j$.

Note that the set of formal basic commutators depends on the chosen ordering, but for each ordering it is uniquely defined. Since the basic commutators form a subset of the set of formal commutators, the ordering on the set of formal commutators induces an ordering on the set of basic commutators. This ordering still places commutators of greater weight higher in the ordering.

As was noted above, the collecting process does not terminate in general. It does however for nilpotent groups. Furthermore we have certain information about the relation between the lower central series of a group and the basic commutators of a given weight.

Theorem 2.1.3. *Let $\mathcal{F}_d$ be a finitely generated free group. The commutators of weight i generate the section $L_i(\mathcal{F}_d)/L_{i+1}(\mathcal{F}_d)$ as a free abelian group, or equivalently: Let $\sigma_1 < \sigma_2 < ...$ denote all formal basic commutators of $\mathcal{F}_d$ in order. If $\sigma \in \mathcal{F}_d$, then there is a unique sequence $m_1, m_2, ...$ of integers such that, for any $i > 0$, if u is the largest integer such that σ_u has weight i then $\sigma \equiv \sigma_1^{m_1}\sigma_2^{m_2}....\sigma_u^{m_u}$ mod $L_{i+1}(\mathcal{F}_d)$.*

Corollary 2.1.4. *Let G be a nilpotent group of class cl. The commutators of weight greater than cl are equal to 1 in G.*

These results are due to M. Hall and P. Hall, see for example [Leedham1] Chapter 1.1 and Prop. 1.1.29. for details.

We will now look at some examples for the presentation of p-groups by basic commutators.

Example: We consider the pair of groups below given by sets of basic commutators and relations between them. The first group is

$$\begin{aligned} G_1 \quad := \langle \bar{\sigma}_1, ..., \bar{\sigma}_6 \mid \quad & \bar{\sigma}_i^3 = 1,\ [\bar{\sigma}_2, \bar{\sigma}_1] = \bar{\sigma}_4,\ [\bar{\sigma}_3, \bar{\sigma}_1] = \bar{\sigma}_5,\ [\bar{\sigma}_3, \bar{\sigma}_2] = \bar{\sigma}_6, \\ & [\bar{\sigma}_j, \bar{\sigma}_i] = 1 \text{ for } j = 4, 5, 6 \text{ and all } i \rangle. \end{aligned}$$

All σ_i are basic commutators, hence the group G_1 has order 3^6. The nilpotency class is 2 because only commutators of weight 2 appear in G_1. In fact $\bar{\sigma}_4, \bar{\sigma}_5, \bar{\sigma}_6$ are all basic commutators of weight 2 in a group on three generators.

The second group is

$$\begin{aligned} E_1 \quad := \langle \sigma_1, ..., \sigma_6, \tau \mid \quad & \sigma_i^3 = \tau^3 = 1, [\sigma_2, \sigma_1] = \sigma_4[\sigma_3, \sigma_1] = \sigma_5, [\sigma_3, \sigma_2] = \sigma_6, \\ & [\sigma_4, \sigma_3] = [\sigma_2, \sigma_1, \sigma_3] = \tau, \\ & [\sigma_i, \sigma_j] = 1 \text{ for all basic commutators satisfying } j = 4, 5, 6, \\ & [\tau, \sigma_j] = 1 \text{ for } j = 1, 2, 3, 4, 5, 6 \rangle. \end{aligned}$$

Again all σ_i and τ are basic commutators, hence the order of E_1 is 3^7, its nilpotency class is 3 because τ has weight 3. We take closer look at the basic commutators of weight 3. Those are

$$[\sigma_2, \sigma_1, \sigma_1],\ [\sigma_3, \sigma_1, \sigma_1],$$

$$[\sigma_2, \sigma_1, \sigma_2],\ [\sigma_3, \sigma_1, \sigma_2],\ [\sigma_3, \sigma_2, \sigma_2],$$

$$[\sigma_2, \sigma_1, \sigma_3],\ [\sigma_3, \sigma_1, \sigma_3],\ [\sigma_3, \sigma_2, \sigma_3].$$

All basic commutators of weight 3 are left normed commutators and all but $[\sigma_2, \sigma_1, \sigma_3]$ are equal to 1 in E. This does not mean, however, that all left normed commutators except of $[\sigma_2, \sigma_1, \sigma_3]$ vanish. By the Hall-Witt-identity we have

$$[\sigma_2, \sigma_1, \sigma_3] \cdot [\sigma_3, \sigma_2, \sigma_1] \cdot [\sigma_1, \sigma_3, \sigma_2] = 1.$$

Using

$$[\sigma_1, \sigma_3, \sigma_2] = [[\sigma_1, \sigma_3], \sigma_2] = [[\sigma_3, \sigma_1]^{-1}, \sigma_2] = [\sigma_3, \sigma_1, \sigma_2]^{-1} = 1$$

we obtain

$$[\sigma_3, \sigma_2, \sigma_1]^{-1} = [\sigma_2, \sigma_3, \sigma_1] = [\sigma_2, \sigma_1, \sigma_3].$$

So $[\sigma_3, \sigma_2, \sigma_1] \neq 1$, but neither $[\sigma_3, \sigma_2, \sigma_1]$ nor $[\sigma_2, \sigma_3, \sigma_1]$ are basic commutators. In any case we have a cyclic, central group extension

$$\begin{tikzcd} 1 \arrow[r] & C_3 \arrow[r] & E_1 \arrow[r] & G_1 \arrow[r] & 1\,. \\ & \langle \tau \rangle & & & \end{tikzcd}$$

This extension will be used in later examples.

We now want to construct a series of p-groups that is described by relations that are in a way ”minimal“. The idea of this construction is that on the one hand every p-group can be obtained from one (or more) of the groups of this series by taking a factor group. On the other hand the groups of this series will be easy to describe in terms of generators and relations, because they are determined by as few relations as possible.

Definition: Let $\mathcal{F}_d$ be a free group on d generators, q a power of a prime p. For integers cl and d, the group $G(q, cl, d)$ is the factor group of $\mathcal{F}_d$ defined by the following relations:
For each basic commutator σ_i of weight w_i we have $\sigma_1^{(q^{cl+1-w_i})} = 1$ if $w_i < cl$ and $\sigma_i = 1$ if $w_i \geq cl$.

Since there are no ”automatic“ relations between the basic commutators, and none are imposed on them by the definition of $G(q, cl, d)$, two different basic commutators in $G(q, cl, d)$ define two different elements of this group. The group is a finite p-group since its order is exactly the product of the exponents of the basic commutators of weight smaller than cl which is a power of q and hence a power of the prime p. Furthermore, in $G(q, cl, d)$ a basic commutator equals 1 if and only if it is of weight at least $cl + 1$, thus $G(q, cl, d)$ has nilpotency class cl.

Observe that for two basic commutators σ_i, σ_j of $G(q, cl, d)$ neither σ_i is a power of σ_j nor is σ_j a power of σ_i: By the definition of basic commutators there are no relations between basic commutators in a free group aside from the relations appearing in the definition and no relations aside from a power relation to bound the order of basic commutator are imposed on the basic commutators in the definition of the group $G(q, cl, d)$. Hence we have:

Corollary 2.1.5. *A basic commutator of a group $G(q, cl, d)$ is not a power of another basic commutator of this group.*

The groups $G(q, cl, d)$ are a series of p-groups which arise from free groups by imposing "as few relations as possible" on them to obtain a finite p-group. The only relations of $G(q, cl, d)$ are those necessary to bound the order of the group, hence making $G(q, cl, d)$ a finite group. This bound is defined by the parameters q, cl and d. Therefore every p-group can be obtained as a factor group of one (or more) of the groups $G(q, cl, d)$; this is done by simply choosing q, cl and d large enough and imposing additional relations on this group.

2.2 Embedding problems

This section gives a short account of the theory of embedding problems, in particular of the theory of Brauer type embedding problems and their connection with cohomology. General references for this topic are [Malle&Matzat1] Chapter IV and [Ledet1] Chapter 3. We assume throughout this section that all fields have characteristic zero.
For fields of characteristic p, $p \neq 0$, most of the problems considered in this thesis are solved. In [Harbater1] and [Pop1] D. Harbater and F. Pop proved independently that the inverse problem of Galois theory has a positive answer for the field $\bar{\mathbb{F}}_p(t)$, the maximal cyclotomic extension of the field $\mathbb{F}_p(t)$. Furthermore in characteristic p every embedding problem of p-groups is solvable and this can be used to show that there exist generic polynomials for every p-group in characteristic p, see [Jensen1], Chapter 5.6 for reference.

2.2.1 Basic theory of embedding problems

If H and G are finite groups, a finite group $E \geq H$ is called a *group extension* of H by G if there is an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "i"] & E \arrow[r, "\pi"] & G \arrow[r] & 1 \end{tikzcd}.$$

In this situation the subgroup H of E is the *kernel*, the factor group $G = E/H$ the *cokernel* of the extension. The group extension is called *split*, if there exists a homomorphism $\phi : G \to E$, such that $\pi \circ \phi = id_G$. This is equivalent to the property that E is a semidirect product of H and G, i.e. $E = H \rtimes G$. The group extension is called *central*, if the kernel H is a subgroup of the center $Z(E)$ of E.

Two group extensions

$$\begin{tikzcd}1 \arrow[r] & H \arrow[r, "i_1"] & E_1 \arrow[r, "\pi_1"] & G \arrow[r] & 1\end{tikzcd}$$

$$\begin{tikzcd}1 \arrow[r] & H \arrow[r, "i_2"] & E_2 \arrow[r, "\pi_2"] & G \arrow[r] & 1\end{tikzcd}$$

are said to be *equivalent* if $E_1 \cong E_2$.

If M/K is a Galois extension with Galois group G and E is a group extension as above, then the *embedding problem* given by M/K and the group extension is the following question: Does there exist a Galois extension F/K and an injective group homomorphism $\psi : \mathrm{Gal}(F/K) \longrightarrow E$, such that $M \geq F$ and such that the diagram

$$\begin{tikzcd}1 \arrow[r] & H \arrow[r, "i"] & E \arrow[r, "\pi"] & G = \mathrm{Gal}(M/K) \arrow[r] & 1 \\ & & \mathrm{Gal}(F/K) \arrow[u, "\psi"] \arrow[ur, "\mathrm{res}_M"'] & & \end{tikzcd}$$

commutes. (Here $\mathrm{res}_M : \mathrm{Gal}(F/K) \rightarrow \mathrm{Gal}(M/K)$ is the natural restriction map.) Such an embedding problem will be denoted by $(M/K, E, G)$.

A *weak solution* of an embedding problem is a pair F/K and ψ, such that the conditions above are satisfied. The field F is the *solution field* of the embedding problem. If ψ is an isomorphism, the solution is called a *proper solution.* Since only proper solutions are of importance in this thesis, the term *solution* will always and exclusively be used for a *proper* solution. We recall the definition of a regular extension from Section 1.3.2. A field extension $\tilde{M}/K(t)$ is called *regular over* K or *geometric* if $\bar{K} \cap \tilde{M} = K$ for every algebraic closure $\bar{K}$ of K. This gives rise to the following definition:

Definition: An embedding problem $(\tilde{M}/K(t), E, G)$ is called *regular* if $\tilde{M}/K(t)$ is regular over K. A solution with solution field $\tilde{F}$ to this embedding problem is called a *regular solution*, if the extension $\tilde{F}/K(t)$ is regular over K.

The following two fundamental theorems on the solvability of embedding problems will be needed later on:

Theorem 2.2.1.

- *Let F be a field with absolute Galois group of cohomological dimension at most 1. Then every finite embedding problem over F is solvable.*

- *The absolute Galois group of $\mathbb{Q}^{ab}$ has cohomological dimension at most 1.*

These results can be found in [Malle&Matzat1], Chapter IV, Section 1.5.

Theorem 2.2.2. *Assume that the kernel of the finite embedding problem $(M/K, E, G)$ decomposes into a direct product $H = \prod_{i=1}^{r} H_i$ of normal subgroups H_i of E. Then for the induced embedding problems $(M/K, E_i, G)$ given by*

$$\begin{tikzcd}1 \arrow[r] & H_i \arrow[r] & E_i \arrow[r] & G \arrow[r] & 1\end{tikzcd}$$

we have:

- *The embedding problem $(M/K, E, G)$ possesses a (proper) solution if and only if $(M/K, E_i, G)$ possess (proper) solutions, linearly disjoint over M, for $i = 1, .., r$.*
- *The embedding problem $(\tilde{M}/K(t), E, G)$ possesses a regular (proper) solution if and only if $(\tilde{M}/K(t), E_i, G)$ possess regular (proper) solutions, linearly disjoint over $\bar{K}\tilde{M}$, for $i = 1, .., r$.*

This theorem is Theorem 1.6 in Chapter IV of [Malle&Matzat1].

2.2.2 Brauer type embedding problems

Brauer type embedding problems are a special kind of embedding problems with particularly useful properties. We begin with the central definitions and most important properties:

Definition: An embedding problem given by a Galois extension M/K with $\mathrm{Gal}(M/K) = G$ and a central group extension with cyclic kernel of order m

$$\begin{tikzcd}1 \arrow[r] & C_m \arrow[r] & E \arrow[r] & G \arrow[r] & 1\end{tikzcd}$$

is a *Brauer type embedding problem* if the group of m-th roots of unity is contained in M and is isomorphic as G-module to the kernel of the group extension.

The main theorem about Brauer type embedding problems is the following:

Theorem 2.2.3. *If $F = M(\sqrt[m]{\omega})$ is a solution field of a Brauer type embedding problem given by an extension M/K with Gal$(M/K) = G$ and a group extension*

$$\begin{tikzcd}1 \arrow[r] & C_m \arrow[r] & E \arrow[r, "\pi"] & G \arrow[r] & 1\end{tikzcd},$$

then all solution fields are of the form $F' = M(\sqrt[m]{r\,\omega})$ with $r \in K^\times$.

A proof for this theorem will be given in the next section.

Definition: An embedding problem given by a Galois extension M/K with $\mathrm{Gal}(M/K) = G$ and a group extension

$$\begin{tikzcd}1 \arrow[r] & H \arrow[r] & E \arrow[r] & G \arrow[r] & 1\end{tikzcd}$$

is a *Frattini embedding problem* if the kernel H of the group extension is contained in the Frattini subgroup of E. The *Frattini subgroup* of a group is defined as the intersection of all maximal subgroups of this group.

The Brauer type embedding problems (BEPs for short) considered here will all have the property that the m-th roots of unity are already contained in K and that the group extensions are non-split, central extensions. In this case the embedding problems are in addition Frattini embedding problems. For Frattini embedding problems the following important theorem holds:

Theorem 2.2.4. *Every weak solution of a Frattini embedding problem is already a (proper) solution.*
Every solution of a regular Frattini embedding problem is already a regular solution.

A proof for Theorem 2.2.4 can be found in [Malle&Matzat1] *(Proposition IV 5.1)*.

2.2.3 Brauer type embedding problems and cohomology

The following section is a short account of the theory of Brauer type embedding problems and its connection with group cohomology. A more detailed account on this topic, including the proofs omitted here, can be found in [Ledet1].

Let

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & E \arrow[r, "\pi"] & G \arrow[r] & 1 \end{tikzcd},$$

be a group extension with abelian kernel. An abelian group A on which a group G acts by automorphisms is called a G-module. If $\alpha \in A$, a group extension as above induces a G-module structure on its kernel A by $\iota(\sigma(\alpha)) := \sigma'\iota(\alpha)\sigma'^{-1}$, where $\sigma' \in E$ is a preimage of $\sigma \in G$. If the group A is already a G-module, such an extension is called an extension *with the G-module A* if it induces the given G-module structure.

A map $s : G \to E$, such that $\pi \circ s = 1_G$ is called a *section* of the group extension. If $s : G \to E$ is a section, we get a map $c : G \times G \to A$ by

$$s(\sigma) \cdot s(\tau) = \iota(c(\sigma,\tau)) \cdot s(\sigma\tau)$$

for $\sigma, \tau \in G$. (Note that the composition in A is written multiplicatively.)

We then have

$$c(\rho,\sigma) \cdot c(\rho\sigma,\tau) = \rho(c(\sigma,\tau)) \cdot c(\rho,\sigma\tau),\ \ \rho,\sigma,\tau \in G$$

by the associative law of E. Maps $c : G \times G \to A$ fulfilling this relation are called *factor systems*. Point-wise addition turns the set of factor systems into an abelian group $Z^2(G,A)$. For an arbitrary function $x : G \to A$, $\sigma \mapsto x_\sigma$ the map

$$(\sigma,\tau) \mapsto \frac{x_\sigma \cdot \sigma(x_\tau)}{x_{\sigma\tau}}$$

is a factor system. A factor system of this kind is called *splitting* or *split*. The set of splitting factor systems forms a subgroup $B^2(G,A)$ of $Z^2(G,A)$ and the second cohomology group of G with coefficients in A is the factor group

$$H^2(G,A) := Z^2(G,A)/B^2(G,A).$$

The following theorem shows that the elements of $H^2(G, A)$ describe the set of extensions of a group G a with kernel A, see [Ledet1], *Theorem 2.3.1* for reference:

Theorem 2.2.5. *Two extensions of a group G with the G-module A are equivalent, if and only if they have the same cohomology class. Furthermore, for every element of $H^2(G, A)$ there exists an extension corresponding to this cohomology class.*

Consider a field extension M/K with Galois group G, a central group extension

$$\begin{tikzcd} 1 \arrow[r] & C_q \arrow[r] & E \arrow[r, "\pi"] & G \arrow[r] & 1 \end{tikzcd},$$

and the Brauer type embedding problem $(M/K, E, G)$ given by this data. Let $\gamma \in H^2(G, C_q)$ describe the cohomology class corresponding to E. We then have:

Theorem 2.2.6. *The Brauer type embedding problem $(M/K, E, G)$ is weakly solvable if and only if $i(\gamma) = 1 \in H^2(G, M^\times)$ where $i : H^2(G, C_q) \to H^2(G, M^\times)$ is the homomorphism induced by the inclusion $C_q \subseteq M^\times$ when C_q is identified with the group of the q-th roots of unity. Furthermore if $F = M(\sqrt[q]{\omega})$ is a weak solution, then all weak solutions are of the form $F = M(\sqrt[q]{r\omega})$, $r \in K^\times$.*

Proof. Let $c \in Z^2(G, C_q)$ represent γ. If $i(\gamma) = 1$, we have for all $\sigma_1, \sigma_2 \in G$

$$c(\sigma_1, \sigma_2) = x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2}) \cdot x_{\sigma_1\sigma_2}^{-1}$$

for some map $x : G \to M^\times$. Then we have

$$1 = x_{\sigma_1}^q \cdot \sigma_1(x_{\sigma_2}^q) \cdot x_{\sigma_1\sigma_2}^{-q}$$

because $c(\sigma_1, \sigma_2)$ is q-th root of unity and by the cohomological version of Hilbert's Theorem 90 (see, for example, [Ledet1], Chapter 2.3) there exist $\omega \in M^\times$, such that for all $\sigma \in G$

$$\frac{\sigma(\omega)}{\omega} = x_\sigma^q.$$

We claim that $M(\sqrt[q]{\omega})/K$ is a weak solution to the embedding problem:

First of all, $M(\sqrt[q]{\omega})/K$ is Galois, since $\frac{\sigma(\omega)}{\omega} \in (M^\times)^q$ for $\sigma \in G$ by Ex 1.52(2) in [Ledet1]. Thus we can extend $\sigma \in G$ to $\sigma' \in \mathrm{Gal}(M(\sqrt[q]{\omega})/K)$ by

$$\sigma'(\sqrt[q]{\omega}) = \zeta_\sigma x_\sigma \sqrt[q]{\omega}$$

for some q-th root of unity ζ_σ. Let $y_\sigma := \zeta_\sigma x_\sigma$.

Now let $\tau \in \mathrm{Gal}(M(\sqrt[q]{\omega})/M)$, i.e. $\tau = \zeta\sqrt[q]{\omega}$ for some q-th root of unity ζ. Then

$$\sigma'\tau(\sqrt[q]{\omega}) = \sigma'(\zeta \cdot \sqrt[q]{\omega}) = \zeta^{e_\sigma} \cdot y_\sigma \cdot \sqrt[q]{\omega} = \tau^{e_\sigma}(y_\sigma \cdot \sqrt[q]{\omega}) = \tau^{e_\sigma}\sigma'(\sqrt[q]{\omega}),$$

where $\sigma'\zeta = \zeta^{e_\sigma}$, and so $\mathrm{Gal}(M(\sqrt[q]{\omega})/M)$ can be identified with a submodule C_d, $d \mid q$, of C_q by $\tau \mapsto \zeta$. This gives an extension

$$\begin{tikzcd} 1 \arrow[r] & C_d \arrow[r, "\zeta\mapsto(\sqrt[q]{\omega}\mapsto\zeta\sqrt[q]{\omega})"'] & \mathrm{Gal}(M(\sqrt[q]{\omega})/K) \arrow[r, "\mathrm{res}_M"'] & G \arrow[r] & 1. \end{tikzcd}$$

Furthermore,

$$\begin{aligned}\sigma_1'\sigma_2'(\sqrt[q]{\omega}) &= y_{\sigma_1}\cdot\sigma_1(y_{\sigma_2})\cdot\sqrt[q]{\omega}\\ &= (\zeta_{\sigma_1}\sigma_1(\zeta_{\sigma_2})\zeta_{\sigma_1\sigma_2}^{-1})\cdot c(\sigma_1,\sigma_2)\cdot y_{\sigma_1\sigma_2}\cdot\sqrt[q]{\omega}\\ &= (\zeta_{\sigma_1}\sigma_1(\zeta_{\sigma_2})\zeta_{\sigma_1\sigma_2}^{-1})\cdot c(\sigma_1,\sigma_2)\cdot(\sigma_1\sigma_2)'(\sqrt[q]{\omega})\end{aligned}$$

and so the cohomology class of the group extension above in $H^2(G,C_d)$ is given by the factor system

$$(\sigma_1,\sigma_2)\mapsto(\zeta_{\sigma_1}\sigma_1(\zeta_{\sigma_2})\zeta_{\sigma_1\sigma_2}^{-1})\cdot c(\sigma_1,\sigma_2).$$

Obviously, this factor system is equivalent to c when considered in $Z^2(G,C_q)$, meaning that we have an embedding of $\mathrm{Gal}(M(\sqrt[q]{\omega})/K)$ into E as desired. Thus, $M(\sqrt[q]{\omega})/K$ is a weak solution.

Conversely, let $M(\sqrt[q]{\omega})/K$, $\omega\in M^\times$, be a weak solution. Then there exists a monomorphism ϕ: $\mathrm{Gal}(M(\sqrt[q]{\omega})/K)\to E$ such that $\mathrm{res}_M=\pi\circ\phi$. If $d=[M(\sqrt[q]{\omega}):M]$, we then have a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & C_d \arrow[r, "\zeta\mapsto(\sqrt[q]{\omega}\mapsto\zeta\sqrt[q]{\omega})"] \arrow[d, "\zeta\mapsto\zeta^h"'] & \mathrm{Gal}(M(\sqrt[q]{\omega})/K) \arrow[r, "\mathrm{res}_M"] \arrow[d, "\phi"'] & G \arrow[r] \arrow[d, "="'] & 1 \\
1 \arrow[r] & C_q \arrow[r] & E \arrow[r, "\pi"'] & G \arrow[r] & 1
\end{tikzcd}$$

for some $h\in\mathbb{Z}$ which can be chosen to be prime to q. Let $s:G\to E$ be a section with $\mathrm{Im}(s)\subseteq\mathrm{Im}(\phi)$, and let $c'\in Z^2(G,C_d)$ be the corresponding factor system. Also let $\sigma'=\phi^{-1}(s_\sigma)$. By Ex. 1.52(2) in [Ledet1] again, $(\frac{\sigma(\omega)}{\omega})^{i_\sigma}\in(M^\times)^q$ for some $i_\sigma\in\mathbb{Z}$ prime to q, since $M(\sqrt[q]{\omega})/K$ is Galois. And since we know how G operates on $\mathrm{Gal}(M(\sqrt[q]{\omega})/M)$, we know that $i_\sigma=1$. Hence, $\frac{\sigma(\omega)}{\omega}=x_\sigma^q$ for some $x_\sigma\in M^\times$, and we may assume $\sigma'(\sqrt[q]{\omega})=x_\sigma\cdot\sqrt[q]{\omega}$. But then

$$c'(\sigma_1,\sigma_2)=(x_{\sigma_1}\cdot\sigma_1(x_{\sigma_2})\cdot x_{\sigma_1\sigma_2}^{-1})^h$$

for $\sigma_1,\sigma_2\in G$. Thus, as $[c]=[c']\in H^2(G,C_q)$, we have $i(\gamma)=1$. Also $M(\sqrt[q]{r\cdot\omega})/K$ is a solution for $r\in K^\times$, by the first part of the proof.

Now let $M(\sqrt[q]{\lambda})/K$, $\lambda\in M^\times$ be another solution. As above, we get $\sigma(\lambda)=y_\sigma^q\cdot\lambda$, where

$$c''(\sigma_1,\sigma_2)=(y_{\sigma_1}\cdot\sigma_1(y_{\sigma_2})\cdot y_{\sigma_1\sigma_2}^{-1})^k$$

is equivalent to c. Modifying x_σ and y_σ by suitable roots of unity, we may assume that $c=c'=c''$. Then $y_\sigma^k/x_\sigma^h=z_\sigma$ satisfies

$$1=z_{\sigma_1}^q\cdot\sigma_1(z_{\sigma_2}^q)\cdot z_{\sigma_1\sigma_2}^{-q}$$

and by Hilbert's Theorem 90 there exists an $a\in M^\times$, such that for all $\sigma\in G$

$$\frac{\sigma(a)}{a}=z_\sigma.$$

It follows that

$$\frac{\sigma(\lambda^k)}{\lambda^k}=y_\sigma^{qk}=\frac{\sigma a^q}{a^q}x_\sigma^{qk}=\frac{\sigma(a^q\omega^h)}{a^q\omega^h}$$

for all $\sigma \in G$, and thus $\lambda^k = ra^q\omega^h$ for some $r \in K^\times$. Hence,

$$M(\sqrt[q]{\lambda}) = M(\sqrt[q]{\lambda^k}) = M(\sqrt[q]{ra^q\omega^h}) = M(\sqrt[q]{r\omega^h}) = M(\sqrt[q]{s\omega}),$$

where $s = r^j$ for some j with $hj \equiv 1(\bmod\ q)$. Thus every solution is of the form $M(\sqrt[q]{r\omega})/K$ for some $r \in K^\times$. □

This is the proof as given in [Ledet1]. An alternative proof can be found in [Malle&Matzat1] (*Theorem IV 7.2*).

Hence a Brauer type embedding problem $(M/K, E, G)$ is weakly solvable if and only if the image $i(\gamma) \in H^2(G, M^\times)$ of the corresponding cohomology class $\gamma \in H^2(G, C_q)$ vanishes i.e. $i(\gamma) \in B(G, M^\times)$. The image $i(\gamma)$ will be called the *embedding obstruction*. By the definition of split factor systems this is the case if and only if E can be embedded into the semi-direct product $M^\times \rtimes G$ in such a way that the diagram

$$\begin{tikzcd}
E \arrow[r, "\pi"] \arrow[d] & G \\
M^\times \rtimes G \arrow[ur, "(x,\sigma)\mapsto\sigma"'] &
\end{tikzcd}$$

is commutative.

Again by the definition of split factor systems, this is equivalent to the condition that there exist for all pairs $\sigma, \tau \in G$ elements $x_\sigma, x_\tau, x_{\sigma\tau} \in M^\times$ satisfying the following relation

$$c(\sigma, \tau) = \frac{x_\sigma \cdot \sigma(x_\tau)}{x_{\sigma\tau}}.$$

As we see in the proof of Theorem 2.2.6 we have for these elements:

Corollary 2.2.7. *If $F = M(\sqrt[q]{\omega})$ is a solution field of a Brauer type embedding problem given by $(M/K, E, G)$, then the element ω satisfies the following relation for all $\sigma \in G$:*

$$\frac{\sigma(\omega)}{\omega} = x_\sigma^q,$$

or, respectively,

$$\frac{\sigma(\sqrt[q]{\omega})}{\sqrt[q]{\omega}} = x_\sigma$$

where the elements $x_\sigma \in M^\times$ are obtained from the fact that the embedding obstruction vanishes as above.

2.2.4 Factor systems

Assume we have a central, cyclic embedding problem given by a G-extension M/K and a group extension of p-groups

$$\begin{tikzcd}
1 \arrow[r] & C_q \arrow[r] & E \arrow[r] & G \arrow[r] & 1 \\
 & \langle\tau\rangle & & &
\end{tikzcd}$$

with cohomology class $\gamma \in H^2(G, C_q)$. Let $c : G \times G \to C_q$ describe a factor system of this class. Assume that the embedding problem is solvable, i.e., the embedding obstruction $i(\gamma)$ vanishes. We want to describe the map

$$\begin{array}{rccc} x: & G & \to & M \\ & \sigma & \mapsto & x_\sigma \end{array}$$

belonging to this embedding obstruction. As above we identify C_q with its image in $M^\times$ and regard c as a map $c : G \times G \to M^\times$. We then have for $\sigma_1, \sigma_2 \in G$ the relation:

$$c(\sigma_1, \sigma_2) = \frac{x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2})}{x_{\sigma_1\sigma_2}}$$

or, equivalently,

$$c(\sigma_1, \sigma_2) \cdot x_{\sigma_1\sigma_2} = x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2}).$$

Hence the element $x_{\sigma_1\sigma_2}$ belonging to the product $\sigma_1\sigma_2$ is determined by the elements x_{σ_1}, x_{σ_2} and the root of unity $c(\sigma_1, \sigma_2)$.

Lemma 2.2.8. *We have in the situation above for every triple of elements $\sigma_1, \sigma_2, \sigma_3 \in G$:*

$$x_{(\sigma_1\sigma_2)\sigma_3} = x_{\sigma_1(\sigma_2\sigma_3)},$$

i.e. the map $x : G \to M$ is compatible with associativity.

Proof. A short calculation shows

$$x_{(\sigma_1\sigma_2)\sigma_3} = x_{\sigma_1\sigma_2} \cdot \sigma_1\sigma_2(x_{\sigma_3})/c(\sigma_1\sigma_2, \sigma_3) = x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2}) \cdot \sigma_1\sigma_2(x_{\sigma_3})/c(\sigma_1\sigma_2, \sigma_3)c(\sigma_1, \sigma_2)$$

and on the other hand

$$x_{\sigma_1(\sigma_2\sigma_3)} = x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2\sigma_3})/c(\sigma_1, \sigma_2\sigma_3) = x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2}) \cdot \sigma_1\sigma_2(x_{\sigma_3})/c(\sigma_1, \sigma_2\sigma_3)c(\sigma_2, \sigma_3).$$

The two expressions are equal because

$$c(\sigma_1\sigma_2, \sigma_3) \cdot c(\sigma_1, \sigma_2) = c(\sigma_1, \sigma_2\sigma_3) \cdot c(\sigma_2, \sigma_3).$$

This last equality is a consequence of the associativity of E and can be found in [Ledet1], page 31. □

Using this, we can describe $x_{[\sigma_1,\sigma_2]}$, the element belonging to the commutator of two group elements σ_1 and σ_2:

Lemma 2.2.9. *Using the notation above, we have in the situation above for every pair of elements $\sigma_1, \sigma_2 \in G$:*

$$x_{[\sigma_1,\sigma_2]} = \frac{c(\sigma_1\sigma_2, [\sigma_1, \sigma_2]) \cdot c(\sigma_1, \sigma_2)}{c(\sigma_2, \sigma_1)} \cdot \sigma_2^{-1}\sigma_1^{-1}(\frac{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_1})}{x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2})}).$$

Proof. A calculation shows

$$\begin{aligned}
\frac{x_{\sigma_1\sigma_2}\cdot\sigma_1\sigma_2(x_{[\sigma_1,\sigma_2]})}{x_{\sigma_2\sigma_1}} &= c(\sigma_1\sigma_2,[\sigma_1,\sigma_2]) \\
\frac{\sigma_1\sigma_2(x_{[\sigma_1,\sigma_2]})}{c(\sigma_1\sigma_2,[\sigma_1,\sigma_2])} &= \frac{x_{\sigma_2}\cdot\sigma_2(x_{\sigma_1})\cdot c(\sigma_1,\sigma_2)}{x_{\sigma_1}\cdot\sigma_1(x_{\sigma_2})\cdot c(\sigma_2,\sigma_1)} \\
x_{[\sigma_1,\sigma_2]} &= \frac{c(\sigma_1\sigma_2,[\sigma_1,\sigma_2])\cdot c(\sigma_1,\sigma_2)}{c(\sigma_2,\sigma_1)}\cdot\sigma_2^{-1}\sigma_1^{-1}(\frac{x_{\sigma_2}\cdot\sigma_2(x_{\sigma_1})}{x_{\sigma_1}\cdot\sigma_1(x_{\sigma_2})}).
\end{aligned}$$

□

This means, roughly spoken: If G were a free group, M were an infinite field and if we knew the map $c : G \times G \to C_q \subset M^\times$ we had: For every ρ_i of G an element $x_{\rho_i} \in M^\times$ could be chosen arbitrarily and it would be possible to assign to every group element σ by the formula

$$c(\sigma_1,\sigma_2)\cdot x_{\sigma_1\sigma_2} = x_{\sigma_1}\cdot\sigma_1(x_{\sigma_2})$$

an unique element x_σ that can be written as an expression in the elements x_{ρ_i} without any problems. Since the group G is a Galois group, however, it is not a free group. Hence the relations of G "that distinguish G from a free group" have to be taken into account. We will consider now the p-groups $G(q, cl, d)$, introduced in section 2.1.2 which are determined by as few relations as possible.

Assume now that $s : G \to E$ is a section belonging to the factor system c, i.e. we have for each pair $\sigma, \tau \in G$ and the inclusion $\iota : C_q \to E$:

$$s(\sigma)\cdot s(\tau) = \iota(c(\sigma,\tau))\cdot s(\sigma\tau).$$

Without loss of generality we can assume that $s(1) = 1 \in E$. We then have

Lemma 2.2.10. *Assume that $\sigma \in G$ has order n. If $s(\sigma) \in E$ has order n then $R_\sigma(x_\sigma) := x_\sigma \cdot \sigma(x_\sigma) \cdot \ldots \cdot \sigma^{(n-1)}(x_\sigma) = 1$ and if $s(\sigma) \in E$ has order greater than n then $R_\sigma(x_\sigma) = \zeta^i$, for an $i \in 1, ..., q-1$, where ζ is a primitive q-th root of unity.*

Proof. Assume $\sigma' := s(\sigma) \in E$ satisfies the relation $\sigma'^n = 1$. Note that $c(\sigma,\sigma) = 1$ if we have $s(\sigma)^n = 1$, because $1 = s(\sigma)^n = \iota(c(\sigma,\sigma^{n-1}))\cdot s(\sigma^n) = s(1) = 1$. Hence $c(\sigma,\sigma^{n-1}) = 1$ and since n is a power of p this contradicts $c(\sigma,\sigma) \neq 1$. We then have for x_σ:

$$\begin{aligned}
x_{\sigma^2} &= x\cdot\sigma(x_\sigma), \\
&\ldots \\
x_{\sigma^n} &= x\cdot\ldots\cdot\sigma^{n-1}(x_\sigma) = R_\sigma(x_\sigma).
\end{aligned}$$

Hence in this case we conclude

$$1 = x_1 = x_{\sigma^n} = R_\sigma(x_\sigma).$$

The only other possibility is that $s(\sigma)^n = \tau^i$ for some $i \in \{1, ..., q-1\}$ as the preimage of $1 \in G$ is $\langle\tau\rangle = C_q$. In this case we find $\zeta^i = R_\sigma(x_\sigma)$ if $\tau \in C_q$ corresponds to the root of unity $\zeta \in M^\times$. If, in this situation, $s(\sigma)^n$ is a generator of C_q, then the corresponding root of unity ζ^i is a primitive q-th root of unity. □

Summarizing these considerations we obtain: If G is a p-group that is only determined by the orders of its generators and the commutators of generators the elements x_σ must be chosen in such a way that to every generator ρ an element x_ρ is assigned, satisfying $R_\rho(x_\rho) = \zeta^i$, for a suitable i, and to every basic commutator $\sigma_3 := [\sigma_1, \sigma_2]$ an element x_{σ_3} is assigned, satisfying

$$R_{\sigma_3}(x_{\sigma_3}) = \zeta^i$$

and

$$x_{\sigma_3} = \frac{c(\sigma_1\sigma_2, [\sigma_1, \sigma_2]) \cdot c(\sigma_1, \sigma_2)}{c(\sigma_2, \sigma_1)} \cdot \sigma_2^{-1}\sigma_1^{-1}(\frac{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_1})}{x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2})}).$$

We illustrate this with an example:

Example: We consider an embedding problem $(M/K, E_1, G_1)$ given by the group extension

$$\begin{tikzcd} 1 \arrow[r] & C_3 \arrow[r] & E_1 \arrow[r] & G_1 \arrow[r] & 1, \\ & \langle\tau\rangle & & & \end{tikzcd}$$

from the first example of Section 2.1.2. The groups G_1 and E_1 are

$$\begin{aligned} G_1 \;\; := \langle \bar\sigma_1, ..., \bar\sigma_6 \mid \;\; & \bar\sigma_i^3 = 1, [\bar\sigma_2, \bar\sigma_1] = \bar\sigma_4[\bar\sigma_3, \bar\sigma_1] = \bar\sigma_5, [\bar\sigma_3, \bar\sigma_2] = \bar\sigma_6, \\ & [\bar\sigma_j, \bar\sigma_i] = 1 \text{ for } j = 4, 5, 6\rangle. \end{aligned}$$

$$\begin{aligned} E_1 \;\; := \langle \sigma_1, ..., \sigma_6, \tau \mid \;\; & \sigma_i^3 = \tau^3 = 1, [\sigma_2, \sigma_1] = \sigma_4[\sigma_3, \sigma_1] = \sigma_5, [\sigma_3, \sigma_2] = \sigma_6, \\ & [\sigma_4, \sigma_3] = [\sigma_2, \sigma_1, \sigma_3] = \tau, \\ & [\sigma_i, \sigma_j] = 1 \text{ for all basic commutators satisfying } j = 4, 5, 6, \\ & [\tau, \sigma_j] = 1 \text{ for } j = 1, 2, 3, 4, 5, 6\rangle. \end{aligned}$$

We have $\tau \in Z(E_1)$ and hence we see that this extension is a non-split extension: By $[\sigma_4, \sigma_3] = \tau$ we have clearly $E_1 \not\cong \langle\tau\rangle \times G_1$. If $c : G_1 \times G_1 \to E_1$ is the factor system of this group extension, the embedding problem is solvable if and only if we can assign an element $x_{\sigma_i} \in M$ to each basic commutator $\bar\sigma_i$ such that the following holds:

$$R_{\sigma_i}(x_{\sigma_i}) = 1, \text{ for } i = 1, ..., 6,$$

$$x_{\sigma_4} = \frac{c(\sigma_2\sigma_1, [\sigma_2, \sigma_1]) \cdot c(\sigma_2, \sigma_1)}{c(\sigma_1, \sigma_2)} \cdot \sigma_1^{-1}\sigma_2^{-1}(\frac{x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2})}{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_1})}) = \sigma_1^{-1}\sigma_2^{-1}(\frac{x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2})}{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_1})}),$$

$$x_{\sigma_5} = \frac{c(\sigma_3\sigma_1, [\sigma_3, \sigma_1]) \cdot c(\sigma_3, \sigma_1)}{c(\sigma_1, \sigma_3)} \cdot \sigma_1^{-1}\sigma_3^{-1}(\frac{x_{\sigma_1} \cdot \sigma_3(x_{\sigma_3})}{x_{\sigma_3} \cdot \sigma_3(x_{\sigma_1})}) = \sigma_1^{-1}\sigma_3^{-1}(\frac{x_{\sigma_1} \cdot \sigma_3(x_{\sigma_3})}{x_{\sigma_3} \cdot \sigma_3(x_{\sigma_1})}),$$

$$x_{\sigma_6} = \frac{c(\sigma_3\sigma_2, [\sigma_3, \sigma_2]) \cdot c(\sigma_3, \sigma_2)}{c(\sigma_2, \sigma_3)} \cdot \sigma_2^{-1}\sigma_3^{-1}(\frac{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_3})}{x_{\sigma_3} \cdot \sigma_3(x_{\sigma_2})}) = \cdot\sigma_2^{-1}\sigma_3^{-1}(\frac{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_3})}{x_{\sigma_3} \cdot \sigma_3(x_{\sigma_2})})$$

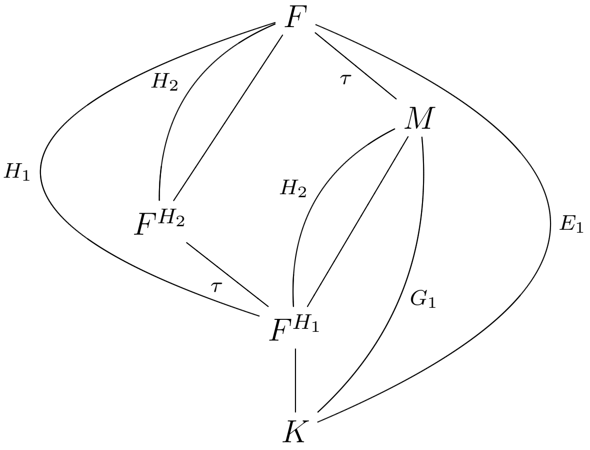
and

$$1 = \frac{c(\sigma_j\sigma_i, [\sigma_j, \sigma_i]) \cdot c(\sigma_j, \sigma_i)}{c(\sigma_j, \sigma_i)} \cdot \sigma_i^{-1}\sigma_j^{-1}(\frac{x_{\sigma_i} \cdot \sigma_i(x_{\sigma_j})}{x_{\sigma_j} \cdot \sigma_j(x_{\sigma_i})})$$

for all other basic commutators $[\sigma_j, \sigma_i]$.

As there are 3 basic commutators of weight 2 and 8 basic commutators weight 3 we end up with a total of $3 + 8 + 6 = 17$ equations. We can do better however.

Firstly we observe that we have $c(\sigma_4, \sigma_3) = \zeta$ and $c(\sigma_j, \sigma_i) = 1$ for all other pairs of basic commutators σ_j, σ_i. We know by Theorem 2.2.7 that the embedding problem is solvable if and only if there exists an element $\omega \in M$ satisfying $x_{\sigma_i}^p = \frac{\sigma_i(\omega)}{\omega}$. The solution to the embedding problem will then be $F = M(\sqrt[p]{\omega})$. On the other hand we can take a closer look on the subgroup structure of E_1. Let $H_2 := \langle\sigma_3, \sigma_5, \sigma_6\rangle$. We see that $\tau \notin H_2$ and thus we define $H_1 := \langle\sigma_3, \sigma_5, \sigma_6, \tau\rangle$.



Since $H_1/H_2 \cong \langle\tau\rangle$ and $\tau \in C(E_1)$ we have in fact $H_1 = H_2 \times \langle\tau\rangle$, hence H_2 can be identified with a subgroup of G_1. Furthermore we see that $H_1 \triangleleft E_1$ and $H_2 \triangleleft H_1$. Thus the element $\sqrt[p]{\omega}$ of the extension F/M can be chosen to lie in $F^{H_2} \subset M$. Since $x_{\sigma_i} = \frac{\sigma_i(\sqrt[p]{\omega})}{\sqrt[p]{\omega}}$ we obtain the the relations $x_{\sigma_3} = x_{\sigma_5} = x_{\sigma_6} = 1$. Hence the equation

$$1 = \frac{c(\sigma_j\sigma_i, [\sigma_j, \sigma_i]) \cdot c(\sigma_j, \sigma_i)}{c(\sigma_i, \sigma_j)} \cdot \frac{x_{\sigma_i} \cdot \sigma_i(x_{\sigma_j})}{x_{\sigma_j} \cdot \sigma_j(x_{\sigma_i})}$$

vanishes for the pairs $(i, j) = (3, 5), (3, 6)$. For the pairs $(i, j) = (1, 3), (2, 3), (1, 5)$, $(2, 5)$, $(2, 6)$ we immediately find

$$1 = \frac{c(\sigma_j\sigma_i, [\sigma_j, \sigma_i]) \cdot c(\sigma_j, \sigma_i)}{c(\sigma_i, \sigma_j)} \cdot \frac{x_{\sigma_i} \cdot \sigma_i(x_{\sigma_j})}{x_{\sigma_j} \cdot \sigma_j(x_{\sigma_i})} = \frac{x_{\sigma_i}}{\sigma_j(x_{\sigma_i})} = 1,$$

hence they are always satisfied. (Note that the pairs $(1, 6)$ and $(5, 6)$ do not yield a basic commutator, as seen in Section 2.1.2.)

Thus the 7 remaining equations are

$$R_{\sigma_1}(x_{\sigma_1}) = 1,$$

$$R_{\sigma_2}(x_{\sigma_2}) = 1,$$

$$R_{\sigma_4}(x_{\sigma_4}) = 1,$$

$$x_{\sigma_4} = \frac{c(\sigma_2\sigma_1, [\sigma_2, \sigma_1]) \cdot c(\sigma_2, \sigma_1)}{c(\sigma_1, \sigma_2)} \cdot \sigma_1^{-1}\sigma_2^{-1}(\frac{x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2})}{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_1})}) = \sigma_1^{-1}\sigma_2^{-1}(\frac{x_{\sigma_1} \cdot \sigma_1(x_{\sigma_2})}{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_1})}),$$

$$1 = \frac{c(\sigma_4\sigma_1, [\sigma_4, \sigma_1]) \cdot c(\sigma_4, \sigma_1)}{c(\sigma_1, \sigma_4)} \cdot \frac{x_{\sigma_1} \cdot \sigma_1(x_{\sigma_4})}{x_{\sigma_4} \cdot \sigma_4(x_{\sigma_1})} = \frac{x_{\sigma_1} \cdot \sigma_1(x_{\sigma_4})}{x_{\sigma_4} \cdot \sigma_4(x_{\sigma_1})},$$

$$1 = \frac{c(\sigma_4\sigma_2, [\sigma_4, \sigma_2]) \cdot c(\sigma_4, \sigma_2)}{c(\sigma_2, \sigma_4)} \cdot \frac{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_4})}{x_{\sigma_4} \cdot \sigma_4(x_{\sigma_2})} = \frac{x_{\sigma_2} \cdot \sigma_2(x_{\sigma_4})}{x_{\sigma_4} \cdot \sigma_4(x_{\sigma_2})},$$

$$1 = \frac{c(\sigma_4\sigma_3, [\sigma_4, \sigma_3]) \cdot c(\sigma_4, \sigma_3)}{c(\sigma_3, \sigma_4)} \cdot \frac{x_{\sigma_3} \cdot \sigma_3(x_{\sigma_4})}{x_{\sigma_4} \cdot \sigma_4(x_{\sigma_3})} = \zeta^{-1}\frac{\sigma_3(x_{\sigma_4})}{x_{\sigma_4}}.$$

2.3 Embedding problems for p-groups

We will now look at the connection between the construction of p-groups, or more generally nilpotent groups, as Galois groups and Brauer type embedding problems.

Since p-groups are nilpotent, there are central series for every p-group. Consequently every p-group can be constructed, starting from the trivial group, by central group extensions. In fact, even more is known about these group extensions: By [Leedham1] Prop. 1.2.4, the commutator subgroup of a p-group G is a subgroup of the Frattini subgroup of G. Hence if $[G, G]$ is the commutator subgroup of G and $A := G/[G, G]$, then the group extension

$$\begin{tikzcd} 1 \arrow[r] & {[G,G]} \arrow[r] & G \arrow[r] & A \arrow[r] & 1 \end{tikzcd}$$

is a Frattini extension. This extension can be subdivided into extensions with cyclic kernel, which are still Frattini extensions. Hence we have:

Theorem 2.3.1. *Let G be an arbitrary p-group and $A := G/[G, G]$. Then G can be constructed, starting from the abelian group A, by cyclic Frattini group extensions. If M/K is a field extension with Gal$(M/K) = G$, then M can be obtained from an abelian extension of K by solving cyclic Frattini embedding problems. If K contains sufficiently many p^n-th roots of unity, those embedding problems are Brauer type embedding problems and all solutions of each step are of the form described in Theorem 2.2.3.*

Proof. A weak solution of a Frattini embedding problem is already a proper solution by 2.2.4. The rest follows from the considerations above. □

Thus if we consider a field K that contains sufficiently many roots of unity, the problem of realizing p-groups as Galois groups over K can be addressed by solving only Brauer type embedding problems. This is of course far easier than dealing with general embedding problems, as there are easy criteria for solvability and we even have a comfortable way to describe the solutions (if there are any). These observations will be used in the next chapter.

Chapter 3

The arithmetic lifting property for nilpotent groups

We will now address the problem of proving the Arithmetic Lifting property for nilpotent groups over the field $\mathbb{Q}^{ab}$, the maximal abelian extension of $\mathbb{Q}$. In the first section we show that in certain situations the arithmetic lifting property is preserved under the formation of factor groups, a statement that does not need to hold for arbitrary fields. In our situation, however, we will see that if a group E has the arithmetic lifting property so do all factor groups of E. In the second section it will be shown that the groups $G(q, cl, d)$ introduced in Section 2.1.2 have the arithmetic lifting property over fields that contain sufficiently many roots of unity. Those two results will then be used to prove the arithmetic lifting property over $\mathbb{Q}^{ab}$ for finite nilpotent groups. We assume throughout this chapter that all fields have characteristic zero.

3.1 The arithmetic lifting property for factor groups

In certain situations, it is possible to deduce from the fact that some group E has the arithmetic lifting property over a given field K, that factor groups of E have the arithmetic lifting property as well. While it is obviously always possible to infer that every factor group of a group E has a regular realization over a given field K if E has a regular realization over the same field, the same does not need to be true for the arithmetic lifting property. This assertion holds, however, if the field K has cohomological dimension ≤ 1.

Theorem 3.1.1. *Let E be a finite group having the arithmetic lifting property over a given field K. If E has the decomposition $E = A \rtimes G$ where A is an abelian normal subgroup of E. Then G has the arithmetic lifting property over the field K.*

Proof. Split embedding problems with abelian kernel are always solvable (see [Malle&Matzat1], Thm. IV 2.4), thus every G-extension M is a subextension of an E-extension F.

$$\begin{tikzcd}
 & & \tilde{F} \arrow[dl, dash] \arrow[dr, dash] & \\
 & \tilde{M} \arrow[dl, dash] \arrow[dr, dash] & & F \arrow[dl, dash, "A"] \\
K(t) \arrow[dr, dash] & & M \arrow[dl, dash, "G"] & \\
 & K & &
\end{tikzcd}$$

As E has the arithmetic lifting property, every E-extension F is a specialization of a regular E-extension $\tilde{F}/K(t)$. For an arbitrary G-extension M choose F and $\tilde{F}$ such that $M \subset F$. The subextension M is a specialization of the corresponding subextension $\tilde{M}/K(t)$ of $\tilde{F}$.

□

Theorem 3.1.2. *Let K be a field with cohomological dimension ≤ 1 and E be a finite group having the arithmetic lifting property over K. Then every factor group G of E has the arithmetic lifting property over the field K.*

Proof. Let M/K be an arbitrary G-extension. Since the cohomological dimension of K is less than 2, every finite embedding problem over K is solvable, see [Malle&Matzat1], Thm. IV 1.10, Cor. IV 1.11). Thus M/K can be embedded in an E-extension F/K which is specialization of a regular E-extension $\tilde{F}/K(t)$. Hence M is a specialization of a subextension $\tilde{M}/K(t)$ of $\tilde{F}$.

□

3.2 The arithmetic lifting property for embedding problems

In the next section we will prove that every finite p-group, and hence every finite nilpotent group, has the arithmetic lifting property over the field $\mathbb{Q}^{ab}$. In this section the main part of the proof will be done. The proof is by induction on the nilpotency class of the groups $G(q, cl, d)$ introduced in Section 2.1.2. In each step of the induction we consider an E-extension F/K that is a solution of a Brauer type embedding problem $(M/K, E, G)$. We assume that M/K is specialization of a regular G-extension $\tilde{M}/K(t)$ and conclude that the embedding problem given by E, G and $\tilde{M}/K(t)$ is also solvable and that the solution $\tilde{F}$ has Galois group E. This is the main part of the proof and is contained in Theorem 3.2.3 and Lemma 3.2.4. Consequently we show that $\tilde{F}$ specializes to F and that the results of Theorem 3.2.3 can be extended to certain embedding problems with abelian kernel. We start with two preliminary results needed later on. The first is a variation of Hilbert's Theorem 90, the second a technical Lemma needed for the proof of Lemma 3.2.4.

Theorem 3.2.1. *Let K be a field and M/K be a Galois extension with Galois group G. Let $\sigma \in G$ satisfy $\sigma^q = 1$ and let $x \in M$. We have $R_\sigma(x) = 1$ if and only if there exists an element $y \in M^\times$ such that $\frac{\sigma(y)}{y} = x$.*

Proof. The proof is similar to the proof of Hilbert's Theorem 90. Assume such an element y exists. Applying R_σ gives $R_\sigma(x) = \frac{R_\sigma(\sigma(y))}{R_\sigma(y)}$. Inserting σ just permutes the powers of σ, hence $R_\sigma(x) = 1$.
On the other hand assume that we have $R_\sigma(x) = 1$. By Artin's theorem on the linear independence of characters, see [Lang1] Thm. VI.4.1, the map given by

$$\sigma^0 + x \cdot \sigma^1 + x \cdot \sigma(x) \cdot \sigma^2 + ... + x \cdot \sigma(x) \cdot ... \cdot \sigma^{q-2}(x) \cdot \sigma^{q-1}$$

on M is not identically zero. Hence there exists $z \in M$ such that the element

$$\frac{1}{y} := z + x \cdot \sigma^1(z) + x \cdot \sigma(x) \cdot \sigma^2(z) + ... + x \cdot \sigma(x) \cdot ... \cdot \sigma^{q-2}(x) \cdot \sigma^{q-1}(z)$$

is not equal to 0. Application of σ and multiplication by x yields:

$$x \cdot \sigma(\frac{1}{y}) = x \cdot \sigma(z) + x \cdot \sigma(x) \cdot \sigma^2(z) + ... + x \cdot \sigma(x) \cdot ... \cdot \sigma^{q-1}(x)\sigma^q(z) = \frac{1}{y},$$

because $R_\sigma(x) = 1$ and $\sigma^q = 1$. Multiplication by $\sigma(y)$ completes the proof. □

Lemma 3.2.2. *Using the notations of Section 1.2, let $\boldsymbol{L}$ denote a system of linear equations over the function field $K(T_1, ..., T_n)$. Let $\bar{\boldsymbol{L}}$ denote a system of linear equations over a field $K(\theta_1, ..., \theta_n)$, where the θ_i are the roots of an irreducible polynomial of degree n over K, and assume $\bar{\boldsymbol{L}}$ is obtained from $\boldsymbol{L}$ by specializing the coefficients of $\boldsymbol{L}$ via $T_i \mapsto \theta_i$. If $\bar{\boldsymbol{L}}$ consists of linearly independent equations over $K(\theta_1, ..., \theta_n)$ and has a solution in K, then $\boldsymbol{L}$ consists of linearly independent equations over $K(T_1, ..., T_n)$ and is also solvable.*

Proof. Assume $\mathbf{L}$ consists of the following m equations

$$\begin{aligned} c_{1,1}Z_1 + ... + c_{1,n}Z_n &= d_1 \\ &... \\ c_{m,1}Z_1 + ... + c_{m,n}Z_n &= d_m \end{aligned}$$

where $c_{i,j}, d_i \in K(T_1, ..., T_n)$, and assume $\bar{\mathbf{L}}$ consists of the linearly independent equations

$$\begin{aligned} \bar{c}_{1,1}\bar{Z}_1 + ... + \bar{c}_{1,n}\bar{Z}_n &= \bar{d}_1 \\ &... \\ \bar{c}_{m,1}\bar{Z}_1 + ... + \bar{c}_{m,n}\bar{Z}_n &= \bar{d}_m \end{aligned}$$

where $\bar{c}_{i,j}, \bar{d}_i \in K(\theta_1, .., \theta_n)$.
Since $\bar{\mathbf{L}}$ has a solution, we have $n \geq m$ and we assume a solution is given by $z_1, ..., z_n \in K$. As the equations are linearly independent we can add $n-m$ equations to this system to arrive at a new system $\bar{\mathbf{L}}^*$ which is uniquely solvable. Without loss of generality we may add the linear equations

$$z_1 = \bar{Z}_1, ..., z_{n-m} = \bar{Z}_{n-m}.$$

Since the new system $\bar{\mathbf{L}}^*$ is uniquely solvable we have for the determinant of the matrix $\bar{C}^*$, describing the homogeneous system of linear equations corresponding to

$\bar{\mathbf{L}}^*$, $det(\bar{C}^*) \neq 0$.
If we expand the system $\mathbf{L}$ to a new system $\mathbf{L}^*$ by adding the equations

$$z_1 = Z_1, ..., z_{n-m} = Z_{n-m},$$

$\bar{\mathbf{L}}^*$ will be obtained from $\mathbf{L}^*$ by specializing the coefficients of $\mathbf{L}$ via $T_i \mapsto \theta_i$. Correspondingly the determinant $\det(C^*)$ of the matrix C^* describing the homogeneous system of linear equations corresponding to $\mathbf{L}^*$ will specialize to $\det(\bar{C}^*)$. Since $\det(\bar{C}^*) \neq 0$ we have $\det(C^*) \neq 0$. Hence the system $\mathbf{L}^*$ is uniquely solvable and thus the subsystem $\mathbf{L}$ is solvable. □

Now, we consider the groups introduced in Section 2.1.2. Let $cl, d \in \mathbb{N}$ be arbitrary but fixed integers and let q be a fixed power of a fixed prime p. Let $G := G(q, cl, d)/Z(G(q, cl, d))$. Since $Z(G(q, cl, d))$ is a direct product of cyclic groups of order q, the embedding problem $(M/K, G(q, cl, d), G)$ is given by a group extension

$$\begin{tikzcd} 1 \arrow[r] & Z(G(q,cl,d)) \arrow[r, "i"] & G(q,cl,d) \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

and it can be decomposed into embedding problems with cyclic kernel by Theorem 2.2.2. If $(M/K, E, G)$ is such an embedding problem we have $cl(E) > cl(G)$. Observe that $Z(G(q, cl, d)) = L_{cl}(G(q, cl, d))$ is generated by basic commutators of $G(q, cl, d)$ by Theorem 2.1.3. Hence the kernel of the cyclic embedding problem $(M/K, E, G)$ is generated by a basic commutator of E.

As noted above the proof is by induction on the nilpotency class of the groups $G(q, cl, d)$ introduced in Section 2.1.2. A given group $G(q, cl, d)$ can be obtained from the group $G(q, cl, d)/C(G(q, cl, d))$, which has smaller nilpotency class, by a group extension with abelian kernel. This group extension can then be decomposed into group extensions with cyclic kernel. So the group $G(q, cl, d)$ can be constructed inductively by group extensions with cyclic kernels, starting from the trivial group. So if we want to realize $G(q, cl, d)$ regularly over K as Galois group over $K(t)$ we can follow this decomposition of $G(q, cl, d)$ and, since all roots of unity are assumed to be in the field K, solve Brauer type embedding problems in each step.
So we will now consider an E-extension F/K that is a solution to a Brauer type embedding problem $(M/K, E, G)$, given by a group extension

$$\begin{tikzcd} 1 \arrow[r] & C_q \arrow[r, "\iota"] & E \arrow[r] & G \arrow[r] & 1 \\ & \langle \tau \rangle & & & \end{tikzcd}$$

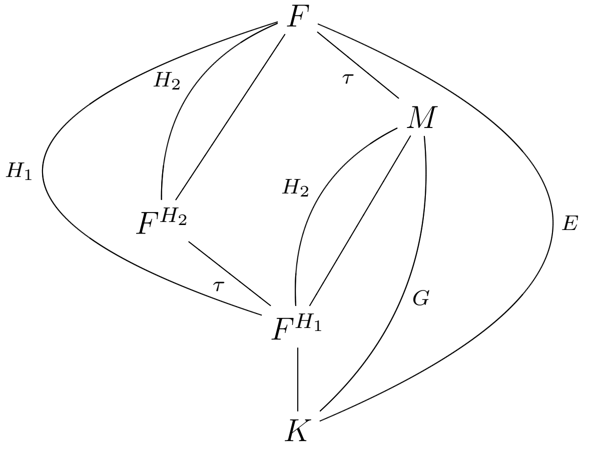
and a G-extension M/K. We will assume that M/K is specialization of a regular G-extension $\tilde{M}/K(t)$ and show that the embedding problem given by E, G and $\tilde{M}/K(t)$ is also solvable and that the solution $\tilde{F}$ has Galois group E.

Before we come to the central Theorem 3.2.3 we introduce some notation and make some preliminary observations.

Let F be a solution of the embedding problem $(M/K, E, G)$. We define two subgroups H_1 and H_2 of E. Let H_2 be a subgroup of E that is generated by basic commutators, that does not contain τ and that has the following property: The group $H_1 := \langle \tau, H_2 \rangle$ satisfies $H_1 \lhd E$ and H_2 is maximal with these properties. Since $\langle \tau \rangle \lhd E$, such an H_2 exists always, but it can be trivial. We note that $\langle \tau \rangle \lhd H_1$, hence the group extension

$$\begin{tikzcd} 1 \arrow[r] & H_2 \arrow[r, "\iota"] & H_1 \arrow[r] & \langle \tau \rangle \arrow[r] & 1 \end{tikzcd}$$

splits. Since τ is a central element of G we have thus $H_1 = \langle \tau \rangle \times H_2$.
By [Lang1] VI.1.14, H_2 can be identified with a subgroup of G.



We will see later on that the question whether the embedding problem $(M/K, E, G)$ can be solved can be decided by examining the field $F^{H_1} < M$ instead of M itself. We note that F^{H_1} is the smallest Galois subextension of M such that the corresponding Galois group E/H_1 is generated by basic commutators. In other words, the group E/H_1 is build up from just enough classes of basic commutators of E such that it is not possible to "build up τ from the remaining basic commutators in H_2". These basic commutators will be denoted by $\sigma_1, ..., \sigma_m$, hence m denotes the number of basic commutators generating E/H_1. Let n the order of E/H_1. The group H_2 will be used later on to reduce the elements in the factor system corresponding to the embedding problem to a minimal set. The proof will then contain an induction on those elements.

As stated above, we assume now that M/K is a specialization of a regular Galois extension $\tilde{M}/K(t)$ with $\mathrm{Gal}(\tilde{M}/K(t)) = G$ via a specialization φ, i.e., the extension $\tilde{M}/K(t)$ and the specialization M/K are Galois extensions of the same degree.

By the definition of a specialization, this means that there exists a $s \in K$ such that the specialization is given by $\varphi : t \mapsto s$ and the polynomial $(t - s)$ gives via

$$v : \tilde{M}^{\times} \longrightarrow \mathbb{Z}, \ \tilde{f} = \tilde{u}(t-s)^m \mapsto m,$$

a discrete valuation of $\tilde{M}$. This valuation is inert in $\tilde{M}/K(t)$ and the following assertions hold, see Section 1.1 for reference: The valuation ring of $\tilde{M}$ with respect to $(t - s)$ is

$$\mathfrak{O}_{\varphi} := \left\{ \frac{\tilde{f}}{\tilde{g}} \mid \tilde{f} \in \tilde{M}, \ \tilde{g} \in \tilde{M} \text{ and } (t-s) \nmid \tilde{g} \right\}$$

and its maximal ideal is $\mathfrak{m}_\varphi := \mathfrak{O}_\varphi(t-s)$. The quotient map

$$\varphi : \mathfrak{O}_\varphi \longrightarrow M := \mathfrak{O}_\varphi/\mathfrak{m}_\varphi,\ t \mapsto s$$

is a place from $\tilde{M}$ to M. The map φ is the specialization of $\tilde{M}$ at s and since this is the only specialization map considered here, we will simply call it *the* specialization.

We will now restrict ourselves to the subextension $\tilde{M}^{H_2}/K(t)$ of $\tilde{M}/K(t)$ which, by assumption, specializes to $F^{H_1} = M^{H_2}$ via the map φ and describe these extensions via minimal polynomials and primitive elements: Let $\theta := \theta_1$ denote a primitive element of the extension F^{H_1}/K and let $\theta_1, ..., \theta_n$ denote a normal basis for F^{H_1}/K. Furthermore, let

$$P(X) := X^n + (-1)k_{n-1}X^{n-1} + ... + (-1)^n k_0$$

denote a minimal polynomial for θ over this extension, i.e. a polynomial that has $\theta_1, ..., \theta_n$ as roots. We pick a preimage $\tilde{\theta} := \tilde{\theta}_1$ of θ_1 under the specialization φ that is a primitive element of the extension $\tilde{M}^{H_2}/K(t)$ and let $\mathrm{Gal}(\tilde{M}^{H_2}/K(t)) = \mathrm{Gal}(F^{H_1}/K)$ act on this element. In doing so, we obtain preimages $\tilde{\theta}_1, ..., \tilde{\theta}_n$ of $\theta_1, ..., \theta_n$. Let

$$P(t, X) := \tilde{P}(X) := X^n + (-1)\tilde{k}_{n-1}X^{n-1} + ... + (-1)^n \tilde{k}_0$$

be a polynomial that has $\tilde{\theta}_1, ..., \tilde{\theta}_n$ as roots, i.e., a minimal polynomial for $\tilde{M}^{H_2}/K(t)$. Then $P(t, X)$ specializes to $P(X)$ under the specialization φ and the roots $\tilde{\theta}_1, ..., \tilde{\theta}_n$ form a normal basis for the extension $\tilde{M}^{H_2}/K(t)$. We come now to the central Theorem:

Theorem 3.2.3. *Let K be a field of characteristic zero that contains all roots of unity and let M be a Galois extension of K with Galois group $G := G(q, cl, d)/Z(G(q, cl, d))$ for a group $G(q, cl, d)$ as described above.*
Let $(M/K, E, G)$ be an embedding problem with central, cyclic kernel $C_q = \langle \tau \rangle$. Assume that $\tilde{M}/K(t)$ is a regular G-extension that specializes to M/K. If the embedding problem $(M/K, E, G)$ is solvable, then the embedding problem $(\tilde{M}/K(t), E, G)$ is also solvable.

Proof. Using the notation introduced above, we see that if the embedding problem $(M/K, E, G)$ above is solvable, then $F = M(\sqrt[q]{\omega})$ for an element $\omega \in F^{H_1}$. Since F^{H_2}/F^{H_1} is a cyclic extension of order q and the q-th roots of unity are contained in K, we have without loss of generality

$$\tau(\sqrt[q]{\omega}) = \zeta \cdot \sqrt[q]{\omega}$$

for a primitive q-th root of unity ζ. Furthermore there exists a factor system with elements $x_\sigma := \frac{\sigma(\sqrt[q]{\omega})}{\sqrt[q]{\omega}}$ from F^{H_1} corresponding to those elements σ whose images under the canonical projection on E/H_1 do not disappear by Corollary 2.2.7. Due to the compatibility of the composition $x_\sigma \cdot \sigma(x_{\sigma'}) = x_{\sigma\sigma'}$ with associativity for arbitrary group elements σ, σ' it is sufficient to consider the elements x_σ for basic commutators $\sigma_i \in E/H_1$. All other elements can be obtained from those by the considerations done in Lemma 2.2.8, Lemma 2.2.9 and Lemma 2.2.10 in Section 2.2.4. For three basic commutators $\sigma_i, \sigma_j, \sigma_k \in E/H_1$ with the relation $\sigma_k = [\sigma_i, \sigma_j]$ we get by Lemma 2.2.9 the following relation for their corresponding elements x_i, x_j, x_k:

$$x_k = \frac{c(\sigma_i\sigma_j, [\sigma_i, \sigma_j]) \cdot c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot \sigma_j^{-1}\sigma_i^{-1}(\frac{x_j \cdot \sigma_j(x_i)}{x_i \cdot \sigma_i(x_j)})$$

or, equivalently,

$$\sigma_i\sigma_j(x_k) \cdot x_i \cdot \sigma_i(x_j) = \frac{c(\sigma_i\sigma_j, [\sigma_i, \sigma_j]) \cdot c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot x_j \cdot \sigma_j(x_i).$$

In case $[\sigma_i, \sigma_j] = 1$, the expression reduces to

$$x_i \cdot \sigma_i(x_j) = \frac{c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot x_j \cdot \sigma_j(x_i).$$

Since τ is a basic commutator, we have $\tau = [\sigma'_m, \sigma'_l]$ for a uniquely determined pair of basic commutators $\sigma'_l, \sigma'_m \in E$. We denote the classes of σ'_l, σ'_m in E/H_1 by σ_l, σ_m. (Note that m denotes also the number of basic commutators generating E/H_1. Since there is for now no ordering on the basic commutators, this choice can be made without loss of generality. We will, however, in the proof of Lemma 3.2.4 choose an ordering and σ_m will then turn out to be the highest basic commutator with respect to this ordering.)

At most one of these two commutators lies in H_2, since we can assume without loss of generality $\sigma_m \neq 1 \in E/H_1$. Because of the relation

$$\zeta \cdot \sqrt[q]{\omega} = \tau(\sqrt[q]{\omega}) = [\sigma'_m, \sigma'_l](\sqrt[q]{\omega}) \neq \sqrt[q]{\omega}$$

we obtain, in the case $\sigma'_l \in H_2$, one additional equation:

$$x_m \cdot \sigma_m(x_l) = \frac{c(\sigma_m\sigma_l, [\sigma_m, \sigma_l]) \cdot c(\sigma_m, \sigma_l)}{c(\sigma_l, \sigma_m)} \cdot x_l \cdot \sigma_l(x_m).$$

(If $\sigma'_l \notin H_2$ we have $\sigma_l, \sigma_m \neq 1 \in E/H_1$ and the equation is already contained in the system above because the system contains all equations that come from commutators $[\sigma_i, \sigma_j], \sigma_i, \sigma_j \in E/H_1$.) This equation is a special case of the expression for commutators of the form $1 = [\sigma_i, \sigma_j]$. We have $c(\sigma_m\sigma_l, [\sigma_m, \sigma_l]) = 1$ because $1 = [\sigma_m, \sigma_l] \in E/H_1$. By the definition of the factor system c we have $\sigma'_m\sigma'_l = \iota(c(\sigma_m, \sigma_l))(\sigma_m\sigma_l)'$ and $\sigma'_l\sigma'_m = \iota(c(\sigma_l, \sigma_m))(\sigma_l\sigma_m)'$, where $\iota : C_q \to E$ denotes the inclusion map. Hence we get $c(\sigma_m, \sigma_l) = 1$ and $c(\sigma_l, \sigma_m) = \zeta^{-1}$ because of $\tau = [\sigma'_m, \sigma'_l]$ and the generator τ of C_q corresponds to the primitive q-th root of unity ζ via $\zeta \cdot \sqrt[q]{\omega} = \tau(\sqrt[q]{\omega})$. Since $\sigma_l \in H_2$ we have $x_l = 1$ and so by Lemma 2.2.9 the equation can be reduced to

$$x_m = \zeta \cdot \sigma_l(x_m).$$

Furthermore we have by Lemma 2.2.10

$$R_{\sigma_i}(x_i) = 1$$

for all elements x_i, because τ is a basic commutator of E and by the definition of the groups $G(q, cl, d)$ not a power of another basic commutator, see Corollary 2.1.5.

Hence every preimage $\sigma_i' \in E$ of a basic commutator $\sigma_i \in E/H_1$ has the same order as σ_i.

To prove solvability of the embedding problem over $K(t)$, we have to obtain a factor system for $K(t)$ from the factor system for K. Hence we have to find elements $\tilde{x}_i \in \tilde{M}^{H_2}$ that satisfy the conditions above.

Using Theorem 3.2.1 we can write each element x_i as $x_i = \frac{\sigma_i(y_i)}{y_i}$ with elements $y_i \in F^{H_1}$. Hence we have an equivalent system of equations of the following form: For all triples of basic commutators $\sigma_i, \sigma_j, \sigma_k \in E/H_1$ and for the commutator relation $\tau = [\sigma_i, \sigma_j]$:

$$\begin{aligned}
\sigma_i\sigma_j(x_k) \cdot x_i \cdot \sigma_i(x_j) &= \frac{c(\sigma_i\sigma_j, [\sigma_i, \sigma_j]) \cdot c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot x_j \cdot \sigma_j(x_i) \text{ for } \sigma_k = [\sigma_i, \sigma_j], \\
x_i \cdot \sigma_i(x_j) &= \frac{c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot x_j \cdot \sigma_j(x_i) \text{ for } 1 = [\sigma_i, \sigma_j] \text{ or } \tau = [\sigma_i, \sigma_j], \\
\sigma_i(y_i) &= x_i \cdot y_i.
\end{aligned}$$

If $n := [F^{H_1} : K]$, the elements x_i and y_j can be written as

$$x_i := \sum_{\alpha=1}^{n} x_{i,\alpha}\theta_\alpha, \;\; x_{i,\alpha} \in K,$$

$$y_j := \sum_{\beta=1}^{n} y_{j,\beta}\theta_\beta, \;\; y_{j,\beta} \in K,$$

for a normal basis $\theta_1, ..., \theta_n$ and these expressions can be inserted into the system above. In doing so we obtain expressions in the elements $x_{i,\alpha}, \; y_{j,\beta} \in K$. We write for the sets of coefficients

$$\mathbf{a}_i := \{x_{i,\alpha} \mid \alpha = 1, ..., n\}, \mathbf{b}_i := \{y_{j,\beta} \mid \beta = 1, ..., n\}.$$

Hence we can consider $x_{i,\alpha}, \; y_{j,\beta} \in K$ as a solution of the following system of equations, denoted by $(*)_\theta$:

$$\begin{aligned}
\sigma_i\sigma_j(\bar{X}_k) \cdot \bar{X}_i \cdot \sigma_i(\bar{X}_j) &= \frac{c(\sigma_i\sigma_j, [\sigma_i, \sigma_j]) \cdot c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot \bar{X}_j \cdot \sigma_j(\bar{X}_i) \text{ for } \sigma_k = [\sigma_i, \sigma_j], \\
\bar{X}_i \cdot \sigma_i(\bar{X}_j) &= \frac{c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot \bar{X}_j \cdot \sigma_j(\bar{X}_i) \text{ for } 1 = [\sigma_i, \sigma_j] \text{ or } \tau = [\sigma_i, \sigma_j], \\
\sigma_i(\bar{Y}_i) &= \bar{X}_i \cdot \bar{Y}_i,
\end{aligned}$$

where

$$\bar{X}_i := \sum_{\alpha=1}^{n} \bar{X}_{i,\alpha}\theta_\alpha,$$

$$\bar{Y}_j := \sum_{\beta=1}^{n} \bar{Y}_{j,\beta}\theta_\beta,$$

with parameters $\bar{X}_{i,\alpha}, \bar{Y}_{j,\beta}$ and a normal basis $\theta_1, ..., \theta_n$ for the extension F^{H_1}/K. We denote this system of equations by $(*)_\theta$.

All the considerations above are of course also true for the embedding problem $(\tilde{M}/K(t), E, G)$, because it is a Brauer type embedding problem as well and the structure of the system of equations above depends only on the group G =Gal(M/K) =Gal$(\tilde{M}/K(t))$. Thus the embedding problem $(\tilde{M}/K(t), E, G)$ is solvable if we find a solution to a similar system of equations, denoted by $(*)_{\tilde{\theta}}$,

$$\begin{aligned}
\sigma_i\sigma_j(\tilde{X}_k)\cdot\tilde{X}_i\cdot\sigma_i(\tilde{X}_j) &= \frac{c(\sigma_i\sigma_j,[\sigma_i,\sigma_j])\cdot c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)}\cdot\tilde{X}_j\cdot\sigma_j(\tilde{X}_i) \text{ for } \sigma_k=[\sigma_i,\sigma_j],\\
\tilde{X}_i\cdot\sigma_i(\tilde{X}_j) &= \frac{c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)}\cdot\tilde{X}_j\cdot\sigma_j(\tilde{X}_i) \text{ for } 1=[\sigma_i,\sigma_j] \text{ or } \tau=[\sigma_i,\sigma_j],\\
\sigma_i(\tilde{Y}_i) &= \tilde{X}_i\cdot\tilde{Y}_i
\end{aligned}$$

in $\tilde{M}^{H_2}$.

Lemma 3.2.4 belows shows precisely that a solution $x_i, y_j \in M^{H_2}$ of the system $(*)_\theta$ can be lifted to a solution $\tilde{x}_i, \tilde{y}_j \in \tilde{M}^{H_2}$ of the system $(*)_{\tilde{\theta}}$ and so the embedding problem $(\tilde{M}/K(t), E, G)$ is solvable if the embedding problem $(M/K, E, G)$ is solvable. □

We need the following Lemma to complete the proof of Theorem 3.2.3.

Lemma 3.2.4. *Assume we have embedding problems given as in Theorem 3.2.3. When we have a specialization $\varphi : \tilde{M} \to M$, a normal basis $\tilde{\theta}_1, ..., \tilde{\theta}_n$ for $\tilde{M}^{H_2}/K(t)$ that specializes to a normal basis $\theta_1, ..., \theta_n$ of M^{H_2}/K via the specialization φ, the following holds: If we have a system of equations, denoted by $(*)_\theta$ with parameters $\bar{X}_{i,\alpha}, \bar{Y}_{j,\beta}$*

$$\begin{aligned}
\sigma_i\sigma_j(\bar{X}_k)\cdot\bar{X}_i\cdot\sigma_i(\bar{X}_j) &= \tfrac{c(\sigma_i\sigma_j,[\sigma_i,\sigma_j])\cdot c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)}\cdot\bar{X}_j\cdot\sigma_j(\bar{X}_i) \text{ for } \sigma_k=[\sigma_i,\sigma_j], \quad (1)\\
\bar{X}_i\cdot\sigma_i(\bar{X}_j) &= \tfrac{c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)}\cdot\bar{X}_j\cdot\sigma_j(\bar{X}_i) \text{ for } 1=[\sigma_i,\sigma_j] \text{ or } \tau=[\sigma_i,\sigma_j], \quad (2)\\
\sigma_i(\bar{Y}_i) &= \bar{X}_i\cdot\bar{Y}_i \quad (3)
\end{aligned}$$

where

$$\bar{X}_i := \sum_{\alpha=1}^{n} \bar{X}_{i,\alpha}\theta_\alpha,$$

$$\bar{Y}_j := \sum_{\beta=1}^{n} \bar{Y}_{j,\beta}\theta_\beta,$$

and there exists a nontrivial solution

$$x_i := \sum_{\alpha=1}^{n} x_{i,\alpha}\theta_\alpha,\ y_i := \sum_{\beta=1}^{n} y_{j,\beta}\theta_\beta \in F^{H_1} = M^{H_2}$$

with $x_{i,\alpha}, y_{j,\beta} \in K$, this solution can be lifted to a solution $\tilde{x}_i, \tilde{y}_i$ of a similar system, denoted by $(*)_{\tilde{\theta}}$ over $K(t)$ where the θ_i are replaced by $\tilde{\theta}_i$, where $\varphi(\tilde{\theta}_i) = \theta_i$. In other words, the system

$$\begin{array}{rcll} \sigma_i\sigma_j(\tilde{X}_k) \cdot \tilde{X}_i \cdot \sigma_i(\tilde{X}_j) & = & \frac{c(\sigma_i\sigma_j,[\sigma_i,\sigma_j]) \cdot c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)} \cdot \tilde{X}_j \cdot \sigma_j(\tilde{X}_i) \textit{ for } \sigma_k = [\sigma_i,\sigma_j], & (1) \\ \tilde{X}_i \cdot \sigma_i(\tilde{X}_j) & = & \frac{c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)} \cdot \tilde{X}_j \cdot \sigma_j(\tilde{X}_i) \textit{ for } 1 = [\sigma_i,\sigma_j] \textit{ or } \tau = [\sigma_i,\sigma_j], & (2) \\ \sigma_i(\tilde{Y}_i) & = & \tilde{X}_i \cdot \tilde{Y}_i & (3) \end{array}$$

has a solution $\tilde{x}_i, \tilde{y}_i \in \tilde{M}^{H_2}$ over $K(t)$.

Proof. The proof of this Lemma will be split into five steps. In the first step we translate the system of equations to a system of equations over the function field $K(T_1, ..., T_n)$ to work with indeterminates T_i instead of roots θ_i. In the second step we establish a method to order the equations of type (1) and (2) in a certain convenient way. In the third step we use this ordering to write some of the parameters of these equations as rational functions of the remaining parameters. The fourth step is concerned with the equations of type (3) and in the last step it is shown how a solution of the system $(*)_\theta$ can be lifted to a solution of $(*)_{\tilde{\theta}}$ using the previous results.

Step 1:

In this step, we want to translate the system of equations $(*)_\theta$ into a system of equations over the function field $K(T_1, ..., T_n)$ where the roots θ_i are replaced by indeterminates T_i.
We recall the notation established in the beginning of this section: Let $\tilde{\theta} := \tilde{\theta}_1$ denote a primitive element of the extension $\tilde{M}^{H_2}$, $\tilde{\theta}_1, ..., \tilde{\theta}_n$ a normal basis of $\tilde{M}^{H_2}$ and let

$$P(t, X) := \tilde{P}(X) := X^n + (-1)\tilde{k}_{n-1}X^{n-1} + ... + (-1)^n\tilde{k}_0$$

denote a minimal polynomial for $\tilde{\theta}$ over this extension, i.e., a polynomial that has $\tilde{\theta}_1, ..., \tilde{\theta}_n$ as roots. The polynomial

$$P(X) := X^n + (-1)k_{n-1}X^{n-1} + ... + (-1)^n k_0$$

denotes a minimal polynomial for the extension F^{H_1}, obtained by specializing $P(t, X)$ via the map φ. Correspondingly, each θ_i is a root of $P(X)$ obtained by specializing $\tilde{\theta}_i$ via the map φ and $\theta_1, ..., \theta_n$ is a normal basis of the extension F^{H_1}. We write $\theta := \theta_1$.

We want to write eventually some of the elements $\bar{X}_{i,\alpha}$, we denote them by $\bar{X}_{i,\alpha'}$, as rational functions in the remaining elements $\bar{X}_{i,\alpha''}$, the primitive element θ and the other roots of the minimal polynomial obtained from θ via the Galois action.

This will be done in the following way: We recall that the Galois group E/H_1 of the extension F^{H_1}/K acts on the roots θ_i by permutation. Furthermore each θ_i is a specialized value of a root $\tilde{\theta}_i \in \tilde{M}^{H_2}$ of the minimal polynomial of the extension $\tilde{M}/K(t)$ by the specialization map $\varphi : \tilde{M} \to M$. The group E/H_1 acts on the roots $\tilde{\theta}_i$ in the same ways as on the roots θ_i. We will now replace the roots $\theta_1, ..., \theta_n$ by

variables $T_1, ..., T_n$:
We map the K vector space generated by $\theta_1, ..., \theta_n$ to the (isomorphic) K vector space generated by $T_1, ..., T_n$ via the vector space isomorphism

$$\Psi : \theta_i \mapsto T_i.$$

Furthermore we let the group $\mathrm{Gal}(M^{H_2}/K) = E/H_1$ act on the K vector space generated by the $T_1, ..., T_n$ via this vector space isomorphism, i.e., if $\sigma \in E/H_1$ acts by $\sigma(\theta_i) = \theta_j$, then $\sigma(T_i) = T_j$. We then extend this action multiplicatively to the field $K(T_1, ..., T_n)$ to obtain that the Galois group E/H_1 acts on the indeterminates T_i as a permutation group in the same way as on the roots θ_i. See Section 1.2 for the prerequisites from invariant theory needed here. Again, as with the roots $\theta = \theta_1$, we write $T := T_1$.
We note that $\Psi : K(\theta_1, ..., \theta_n) \to K(T_1, ..., T_n)$ is not compatible with multiplication. We have for example $\Psi(\theta_i) \cdot \Psi(\theta_i) = T_i \cdot T_i = T_i^2 \neq \Psi(\theta_i^2)$, as T_i^2 is not an element of the K vector space generated by indeterminates $T_1, ..., T_n$. On the other hand the specialization

$$\Phi : K(T_1, ..., T_n) \to K(\theta_1, ..., \theta_n), T_i \mapsto \theta_i$$

is a place of $K(T_1, ..., T_n)$ to $K(\theta_1, ..., \theta_n)$ and thus we have $\Phi(f \cdot g) = \Phi(f) \cdot \Phi(g)$ for all $f, g \in K(T_1, ..., T_n)$ whenever $\Phi(f), \Phi(g)$ are well defined elements of $K(\theta_1, ..., \theta_n)$.
Furthermore we have for each $\sigma \in \mathrm{Gal}(F^{H_1}/K) = E/H_1$

$$\sigma(\Phi(T_i) = \sigma(\theta_i) = \theta_{\sigma(i)} = \Phi(T_{\sigma(i)}) = \Phi(\sigma(T_i)).$$

Hence specializing via Φ commutes with the action of E/H_1 on $K(T_1, ..., T_n)$ and $K(\theta_1, ..., \theta_n)$, i.e. Φ is $\mathrm{Gal}(F^{H_1}/K)$-equivariant. If ι denotes the embedding of the K vector space generated by $T_1, ..., T_n$ into the function field $K(T_1, ..., T_n)$ we then have that

$$\Phi \circ \iota \circ \Psi : K(\theta_1, ..., \theta_n) \to K(\theta_1, ..., \theta_n)$$

is the identity map and a $\mathrm{Gal}(F^{H_1}/K)$-equivariant isomorphism of fields. We then have the following commutative diagram:

$$\begin{tikzcd}
K(T_1, ..., T_n) \arrow[r, dash, "T_i \mapsto \theta_i"] \arrow[d, dash, "E/H_1"'] & K(\theta_1, ..., \theta_n) = F^{H_1} \arrow[d, dash, "E/H_1"'] \\
K(T_1, ..., T_n)^{E/H_1} \arrow[r, dash, "T_i \mapsto \theta_i"] & K(\theta_1, ..., \theta_n)^{E/H_1} = K.
\end{tikzcd}$$

With these definitions we translate the equations obtained from the commutator relations into a system of equations over $K(T_1, ..., T_n)$: Via the map Ψ we replace the elements

$$\bar{X}_i := \sum_{\alpha=1}^{n} \bar{X}_{i,\alpha} \theta_\alpha,$$

$$\bar{Y}_j := \sum_{\beta=1}^{n} \bar{Y}_{j,\beta} \theta_\beta,$$

by

$$X_i := \sum_{\alpha=1}^{n} X_{i,\alpha} T_\alpha,$$

$$Y_j := \sum_{\beta=1}^{n} Y_{j,\beta} T_\beta,$$

and consider then a system of equations, denoted by $(*)$. Thus each equation of the original system will then give rise to an equation with its parameters defined over the field $K(T_1, ..., T_n)$, i.e., we obtain a system of equations

$$\begin{aligned}
\sigma_i\sigma_j(X_k) \cdot X_i \cdot \sigma_i(X_j) &= \frac{c(\sigma_i\sigma_j, [\sigma_i, \sigma_j]) \cdot c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot X_j \cdot \sigma_j(X_i) \text{ for } \sigma_k = [\sigma_i, \sigma_j], \\
X_i \cdot \sigma_i(X_j) &= \frac{c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot X_j \cdot \sigma_j(X_i) \text{ for } 1 = [\sigma_i, \sigma_j] \text{ or } \tau = [\sigma_i, \sigma_j], \\
\sigma_i(Y_i) &= X_i \cdot Y_i.
\end{aligned}$$

with

$$X_i := \sum_{\alpha=1}^{n} X_{i,\alpha} T_\alpha,$$

$$Y_j := \sum_{\beta=1}^{n} Y_{j,\beta} T_\beta,$$

with parameters $X_{i,\alpha}, Y_{j,\beta}$ and coefficients in the field $K(T_1, ..., T_n)$ and we try to find a solution for the $X_{i,\alpha}, Y_{j,\beta}$ in $K(T_1, ..., T_n)^{E/H_1}$. The system $(*)$ looks similar to the system $(*)_\theta$, we have just replaced the roots $\theta_i \in F^{H_1}$ by indeterminates $T_i \in K(T_1, ..., T_n)$ over K and renamed the $\bar{X}_{i,\alpha}, \bar{X}_{j,\beta}$, which represent elements of K, to $X_{i,\alpha}, Y_{j,\beta}$, because we are now looking for a solution of this system in $K(T_1, ..., T_n)^{E/H_1}$.

From now on we will call the original system

$$\sigma_i\sigma_j(\bar{X}_k) \cdot \bar{X}_i \cdot \sigma_i(\bar{X}_j) = \frac{c(\sigma_i\sigma_j, [\sigma_i, \sigma_j]) \cdot c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot \bar{X}_j \cdot \sigma_j(\bar{X}_i) \text{ for } \sigma_k = [\sigma_i, \sigma_j], \quad (1)$$

$$\bar{X}_i \cdot \sigma_i(\bar{X}_j) = \frac{c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot \bar{X}_j \cdot \sigma_j(\bar{X}_i) \text{ for } 1 = [\sigma_i, \sigma_j] \text{ or } \tau = [\sigma_i, \sigma_j], \quad (2)$$

$$\sigma_i(\bar{Y}_i) = \bar{X}_i \cdot \bar{Y}_i \quad (3)$$

with

$$\bar{X}_i := \sum_{\alpha=1}^{n} \bar{X}_{i,\alpha} \theta_\alpha,$$

$$\bar{Y}_j := \sum_{\beta=1}^{n} \bar{Y}_{j,\beta} \theta_\beta,$$

over K, which can be regained from the system above by specializing the T_i with the roots of the minimal polynomial $\theta_1, ..., \theta_n$, the *specialized* system. We recall that this system is denoted by $(*)_\theta$. We keep in mind that by assumption this specialized system of equations over the field $F^{H_1} = K(\theta_1, ..., \theta_n)$ has at least one solution $x_{i,\alpha}, y_{j,\beta} \in K$.

Hence, now the system $(*)$ is a system of equations with coefficients in $K(T_1, ..., T_n)$. The Galois group acts on the indeterminates $T_1, ..., T_n$ by permutation as explained above and we will solve the system over the same field $K(T_1, ..., T_n)$. We will do all computations and all transformations of these equations over the field $K(T_1, ..., T_n)$. In doing so, we will by transformations of the equations be able to express some elements $X_{i,\alpha}$, denoted by $X_{i,\alpha'}$, as rational functions in the remaining elements, denoted by $X_{i,\alpha''}$, with coefficients in $K(T_1, ..., T_n)$. Thus we "keep track" of the Galois action. After we have done the transformations over the field $K(T_1, ..., T_n)$, we specialize the indeterminates T_i to the roots θ_i and hence obtain corresponding parameters $\bar{X}_{i,\alpha'}$ as rational functions in the remaining parameters $\bar{X}_{i,\alpha''}$, with coefficients in $K(\theta_1, ..., \theta_n)$.

We have to make sure that the transformations used to isolate the $X_{i,\alpha'}$ are compatible with specializing, i.e., that this process yields the same rational function as isolating the parameters $\bar{X}_{i,\alpha'}$ in the system $(*)_\theta$ would yield. When we look at the equations of the system $(*)$ we see that each side of the equations is an element of

$$K(T_1, ..., T_n)[X_{1,1}, ..., X_{m,n}] \subset K(\theta_1, ..., \theta_n)(T_1, ..., T_n)(X_{1,1}, ..., X_{m,n}).$$

Correspondingly, each side of each equation of the system $(*)_\theta$ is an element of

$$K(\theta_1, ..., \theta_n)[\bar{X}_{1,1}, ..., \bar{X}_{m,n}] \subset K(\theta_1, ..., \theta_n)(\bar{X}_{1,1}, ..., \bar{X}_{m,n}).$$

To isolate a certain $X_{i,\alpha'}$ in one of the equations of $(*)$ we change both sides of the equation by successively adding elements of $K(T_1, ..., T_n)(X_{1,1}, ..., X_{m,n})$ or by multiplying each side with elements of $K(T_1, ..., T_n)(X_{1,1}, ..., X_{m,n})$. Note that we do not need the action of the group E/H_1 on the indeterminates $T_1, ..., T_n$ in this process.

We observe that the specialization

$$K(\theta_1, ..., \theta_n)[T_1, ..., T_n] \to K(\theta_1, ..., \theta_n),\ T_i \mapsto \theta_i$$

is a ring homomorphism, the evaluation homomorphism. It can be extended to a ring homomorphism

$$K(\theta_1, ..., \theta_n)[T_1, ..., T_n]_{\theta_i} \longrightarrow K(\theta_1, ..., \theta_n),$$

where

$$K(\theta_1, ..., \theta_n)[T_1, ..., T_n]_{\theta_i} := \left\{ \frac{f}{g} \mid f, g \in K(\theta_1, ..., \theta_n)[T_1, ..., T_n], (T_i - \theta_i) \nmid g \right\}.$$

Furthermore the map

$$K(\theta_1, ..., \theta_n)(T_1, ..., T_n)(X_{1,1}, ..., X_{m,n}) \to K(\theta_1, ..., \theta_n)(T_1, ..., T_n)(\bar{X}_{1,1}, ..., \bar{X}_{m,n})$$

given by

$$X_{i,\alpha} \mapsto \bar{X}_{i,\alpha}$$

is an isomorphism of fields. Then the specialization of the equations considered above is obtained by restricting the composition of these maps to $K[T_1,...,T_n]_{\theta_i}(X_{1,1},...,X_{m,n})$, where

$$K[T_1,...,T_n]_{\theta_i} := K(\theta_1,...,\theta_n)[T_1,...,T_n]_{\theta_i} \cap K(T_1,...,T_n)$$

and hence it is a ring homomorphism on this restriction. We note that $K[T_1,...,T_n]_{\theta_i}$ is the localization of $K[T_1,...,T_n]$ at $P(t,X)$. Thus specializing is compatible with all transformations of the equations as long as we use only elements of $K[T_1,...,T_n]_{\theta_i}(X_{1,1},...,X_{m,n})$ for our transformations. We can however assume that we need only elements of $K[T_1,...,T_n]_{\theta_i}(X_{1,1},...,X_{m,n})$ when isolating a given parameter $X_{i,\alpha'}$, as long as we know that the specialized system has a solution and that the corresponding parameter $\bar{X}_{i,\alpha'}$ can be isolated in the specialized system. Otherwise it would not be possible to isolate $\bar{X}_{i,\alpha'}$ in the specialized system at all, because isolating would require a "division by zero".

Step 2:

From now on we work with the system of equations $(*)$ defined over $K(T_1,...,T_n)$. Our aim in this step is to order the equations of types (1) and (2) of this system in a certain convenient way.

We recall that the basic commutators can be ordered in such a way that basic commutators of higher weight appear later in the ordering. We choose such an ordering and enumerate the basic commutators not equal to 1 according to this ordering,

$$\sigma_1 < \sigma_2 < ... < \sigma_m.$$

As G is finite nilpotent, this sequence terminates by Corollary 2.1.4, i.e., there exists a "last basic commutator, necessary to describe G", which will be denoted by σ_m. If $n = [F^{H_1} : K] = \text{ord } E/H_1$ as before, we have $m < n$ because the number of elements of a finite p-group exceeds the number of basic commutators generating it. We look at the equations of type (1) and (2), i.e., those of the form

$$\sigma_i\sigma_j(X_k) \cdot X_i \cdot \sigma_i(X_j) = \frac{c(\sigma_i\sigma_j, [\sigma_i,\sigma_j]) \cdot c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)} \cdot X_j \cdot \sigma_j(X_i)$$

or

$$X_i \cdot \sigma_i(X_j) = \frac{c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)} \cdot X_j \cdot \sigma_j(X_i).$$

Each equation comes from a commutator expression of the form $\sigma_k = [\sigma_i,\sigma_j]$, $i > j$. By the definition of the ordering relation of the basic commutators, we know that commutators of higher weight appear later in the ordering than basic commutators of lower weight. Hence, since σ_k has higher weight than σ_j and σ_i, we have $\sigma_k > \sigma_i > \sigma_j$. We have thus always the relation $k > i > j$ in the equations above.

To standardize notation we write now $k = k_{i,j}$ and all commutator expressions yielding equations of types (1) or (2) in the form

$$\sigma_{k_{j,i}} = [\sigma_j, \sigma_i]$$

instead of distinguishing between equations of the two types. Hence each $\sigma_{k_{j,i}}$ denotes either a basic commutator satisfying $k_{j,i} > j > i$ or we have $\sigma_{k_{j,i}} = 1$. In the second case we add a new parameter $\bar{X}_{k_{j,i}}$ belonging to $\sigma_{k_{j,i}}$. This does not change anything, this element will simply have to take the value 1 in a solution for this system of equations. (We note already at this point that we will not isolate the parameter $\bar{X}_{k_{j,i}}$ in the system of equations when we solve the system of equations later on. We have $k_{i,j} > i > j$ and we will always isolate parameters with the least index. Hence no problems occur with the fact that we know beforehand which values the $\bar{X}_{k_{j,i}}$ have to assume to yield a solution of the system of equations.)

We write as above

$$X_i := \sum_{\alpha=1}^{n} X_{i,\alpha} T_\alpha,$$

and, to shorten notation,

$$c_{i,j,k_{j,i}} := \frac{c(\sigma_i\sigma_j, [\sigma_i, \sigma_j]) \cdot c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} = \frac{c(\sigma_i\sigma_j, \sigma_{k_{j,i}}) \cdot c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)}.$$

Since $c : G \to M$ is a factor system, its image consists of roots of unity and so the expression $c_{i,j,k_{j,i}}$ is a well defined root of unity for all $i, j, k_{j,i}$.
Using this notation, we obtain equations of the form:

$$\sigma_i\sigma_j(X_{k_{j,i}}) \cdot (\sum_{\alpha=1}^{n} X_{i,\alpha}T_\alpha) \cdot \sigma_i(X_j) \quad = \quad c_{i,j,k_{j,i}} \cdot X_j \cdot (\sum_{\alpha=1}^{n} X_{i,\alpha}\sigma_j(T_\alpha)).$$

We look now at the equations of type (1) and (2) of the system defined over $K(T_1, ..., T_n)$. We isolate in the equations the parameters $X_{i,\alpha'}$, and hence equate each $X_{i,\alpha'}$ to a rational function in the remaining parameters $X_{i,\alpha''}$ with coefficients in $K(T_1, ..., T_n)$ as follows: All equations come from commutator relations of the form $\sigma_{k_{i,j}} = [\sigma_j, \sigma_i]$. We order these commutator relations by the second argument σ_i of the commutator first and then by the first argument σ_j, both in descending order:

$$\begin{array}{rrcl}
 & \tau & = & [\sigma_m, \sigma_l] \\
1.\ \textit{block}\ \{ & \sigma_{k_{m,m-1}} & = & [\sigma_m, \sigma_{m-1}] \\
2.\ \textit{block}\ \left\{ \begin{array}{c} \\ \\ \end{array} \right. & \begin{array}{r} \sigma_{k_{m,m-2}} \\ \sigma_{k_{m-1,m-2}} \end{array} & \begin{array}{c} = \\ = \end{array} & \begin{array}{l} [\sigma_m, \sigma_{m-2}] \\ [\sigma_{m-1}, \sigma_{m-2}] \end{array} \\
 & & \ldots & \\
i.\ \textit{block} \left\{ \begin{array}{c} \\ \\ \\ \end{array} \right. & \begin{array}{r} \sigma_{k_{m,i}} \\ \ldots \\ \sigma_{k_{i+1,i}} \end{array} & \begin{array}{c} = \\ \\ = \end{array} & \begin{array}{l} [\sigma_m, \sigma_i] \\ \\ [\sigma_{i+1}, \sigma_i] \end{array} \\
 & & \ldots & \\
(m-1).\ \textit{block} \left\{ \begin{array}{c} \\ \\ \\ \end{array} \right. & \begin{array}{r} \sigma_{k_{m,1}} \\ \ldots \\ \sigma_{k_{2,1}} \end{array} & \begin{array}{c} = \\ \\ = \end{array} & \begin{array}{l} [\sigma_m, \sigma_1] \\ \\ [\sigma_2, \sigma_1] \end{array}
\end{array}$$

We let the first commutator equation aside and divide the remaining equations into blocks as indicated above. In this subdivision the equations of the i-th block have the following properties: The block consists of i commutator expressions and every expression is a commutator of the basic commutator σ_{m-i} with a basic commutators σ_j that is higher in the ordering of basic commutators than σ_{m-i}. Hence the commutator $[\sigma_j, \sigma_{m-i}]$ itself is either higher in the ordering than σ_{m-i} or equal to 1.

Step 3:

In this step we use the ordering of the equations obtained above to write some of the parameters of the equations of types (1) and (2) as rational functions in the remaining parameters.

Assume now that we have a solution to the original specialized system of equations (1), (2), (3) over K, i.e., we have a set of elements $x_{i,\alpha} \in K$ that satisfies all those equations. We now want to write some of the $X_{i,\alpha}$, we denote them by $X_{i,\alpha'}$, as rational functions in the remaining $X_{i,\alpha''}$ and the indeterminates $T_1, ..., T_n$. Hence we have to isolate some of the variables $X_{i,\alpha}$ in these equations.

We will do this stepwise: Since every equation of the system consisting of equations of types (1) and (2) comes from one of the commutator relations above, we can order the equations in the same way as the commutator relations above. Now the idea is to solve the system of equations blockwise, starting with the first block. We isolate in the equations of the i-th block coefficients of X_{m-i} and obtain coefficients of X_{m-i}, denoted $X_{m-i,\alpha'}$ as expressions in the remaining coefficients of X_{m-1} and elements X_j, $j > m - i$. Now we will do this in detail:

The ordered system of equations consists of:

The first equation, corresponding to the first commutator relation:

$$\zeta\sigma_l(\sum_{\alpha=1}^{n} X_{m,\alpha}T_\alpha) = \sum_{\alpha=1}^{n} X_{m,\alpha}T_\alpha.$$

Equations of the 1. block, corresponding to the 1. block of commutator relations:

$$\sigma_{m-1}\sigma_m(X_{k_{m,m-1}})\cdot(\sum_{\alpha=1}^{n} X_{m-1,\alpha}T_\alpha)\cdot\sigma_{m-1}(X_m) = c_{m-1,m,k_{m,m-1}}\cdot X_m\cdot(\sum_{\alpha=1}^{n} X_{m-1,\alpha}\sigma_m(T_\alpha)).$$

Equations of the 2. block, corresponding to the 2. block of commutator relations:

$$\begin{aligned} & \sigma_{m-2}\sigma_m(X_{k_{m,m-2}})\cdot(\textstyle\sum_{\alpha=1}^{n} X_{m-2,\alpha}T_\alpha)\cdot\sigma_{m-2}(X_m) \\ = \; & c_{m-2,m,k_{m,m-2}}\cdot X_m\cdot(\textstyle\sum_{\alpha=1}^{n} X_{m-2,\alpha}\sigma_m(T_\alpha)), \\ & \sigma_{m-2}\sigma_{m-1}(X_{k_{m-1,m-2}})\cdot(\textstyle\sum_{\alpha=1}^{n} X_{m-2,\alpha}T_\alpha)\cdot\sigma_{m-2}(X_{m-1}) \\ = \; & c_{m-2,m-1,k_{m-1,m-2}}\cdot X_{m-1}\cdot(\textstyle\sum_{\alpha=1}^{n} X_{m-2,\alpha}\sigma_{m-1}(T_\alpha)). \end{aligned}$$

...

Equations of the i. block, corresponding to the i. block of commutator relations:

$$\begin{aligned} \sigma_i\sigma_m(X_{k_{m,i}})\cdot(\sum_{\alpha=1}^{n} X_{i,\alpha}T_\alpha)\cdot\sigma_i(X_m) &= c_{i,m,k_{m,i}}\cdot X_m\cdot(\sum_{\alpha=1}^{n} X_{i,\alpha}\sigma_m(T_\alpha)), \\ & ... \\ \sigma_i\sigma_{i+1}(X_{k_{i+1,i}})\cdot(\sum_{\alpha=1}^{n} X_{i,\alpha}T_\alpha)\cdot\sigma_i(X_{i+1}) &= c_{i,i+1,k_{i+1,i}}\cdot X_{i+1}\cdot(\sum_{\alpha=1}^{n} X_{i,\alpha}\sigma_{i+1}(T_\alpha)). \end{aligned}$$

...

Equations of the $m-1$. block, corresponding to the $m-1$. block of commutator relations:

$$\begin{aligned} \sigma_1\sigma_m(X_{k_{m,1}})\cdot(\sum_{\alpha=1}^{n} X_{1,\alpha}T_\alpha)\cdot\sigma_1(X_m) &= c_{1,m,k_{m,1}}\cdot X_m\cdot(\sum_{\alpha=1}^{n} X_{1,\alpha}\sigma_m(T_\alpha)), \\ & ... \\ \sigma_1\sigma_2(X_{k_{2,1}})\cdot(\sum_{\alpha=1}^{n} X_{1,\alpha}T_\alpha)\cdot\sigma_1(X_2) &= c_{1,2,k_{2,1}}\cdot X_2\cdot(\sum_{\alpha=1}^{n} X_{1,\alpha}\sigma_2(T_\alpha)). \end{aligned}$$

Note that all equations look basically alike. Different equations depend on different elements $X_{i,\alpha}$ and commutators σ_i but their structure is always the same. The very first equation of the system depends only on $X_{m,1}, ..., X_{m,n}$ and no other element $X_{i,\alpha}$, so we consider this equation separately. We divide the remaining equations into $m-1$ blocks as indicated above. In this subdivision the equations of the i-th block have the following properties: The block consist of i equations and every equation contains the parameters $X_{m-i,1}, ..., X_{m-i,n}$ (which come from a basic commutator σ_{m-i}). All other elements $X_{j,\alpha}$ appearing in any of the equations of the i-th block satisfy $j > m-i$, because they come from basic commutators σ_j that are higher in the ordering of basic commutators than σ_{m-i}. We will now solve the system of equations:

The very first equation

$$\zeta \cdot \sigma_l(\sum_{\alpha=1}^{n} X_{m,\alpha}T_\alpha) = \sum_{\alpha=1}^{n} X_{m,\alpha}T_\alpha$$

contains only $X_{m,1}, ..., X_{m,n}$ none of which appear to any powers other than 1 and no other coefficients $X_{i,\alpha}$. So the equation is a linear equation in $X_{m,1}, ..., X_{m,n}$ and we know that it is not zero because the specialized system has a nontrivial solution $x_{m,1}, ..., x_{m,n}$ by assumption. We have to make sure that the denominator of this expression will not become zero when specializing the equations later on:
We know by assumption that the set of elements $x_{i,\alpha} \in K$ is a solution to the whole system of all the equations of types (1) and (2) of the specialized system. Hence the elements $x_{m,1}, ..., x_{m,n}$ form a solution of the "subsystem" consisting of only one equation obtained from specializing this equation. Furthermore the equation is not zero and is a linear equations. Thus we have a solvable "system of linear equations" (consisting of only one equation). So there exists at least one parameter in the specialized equation that can be isolated, hence be expressed as a rational function of in the other parameters. So by Lemma 3.2.2 the same holds for the equation considered here and thus we can choose X_{m,α'_1} in such a way that the function above and its specialization are well defined.
We denote the set of coefficients $X_{m,\alpha}$ of X_m by $\mathbf{A}_m := \{X_{m,\alpha} \mid \alpha = 1, ..., n\}$, the set containing the coefficient which has been isolated in this equation by $\mathbf{A}'_m := \{X_{m,\alpha'_1}\}$ and the set of the remaining coefficients by $\mathbf{A}''_m := \{X_{m,\alpha} \mid \alpha = 1, ..., n, \ \alpha \neq \alpha'_1\}$. Thus we have a disjoint decomposition

$$\mathbf{A}_m = \mathbf{A}'_m \cup \mathbf{A}''_m$$

and we write to visualize that X_{m,α'_1} depends on the elements of $\mathbf{A}''_m$ and the T_i:

$$X_{m,\alpha'_1} = X_{m,\alpha'_1}(\mathbf{A}''_m, T_1, ..., T_n).$$

As explained above, we solve the other equations stepwise, solving the equations of one block in each step:

In the first step we consider all equations coming from commutators of the form $\sigma_{k_{j,m-1}} = [\sigma_j, \sigma_{m-1}]$ satisfying $j > m-1$. Since the only commutator higher in the ordering than σ_{m-1} is σ_m, there is only one equation of this type, the first equation in our list, namely:

$$\begin{aligned} & \sigma_{m-1}\sigma_m(X_{k_{m,m-1}}) \cdot (\textstyle\sum_{\alpha=1}^n X_{m-1,\alpha}T_\alpha) \cdot \sigma_{m-1}(X_m) \\ = \quad & c_{m-1,m,k_{m,m-1}} \cdot X_m \cdot (\textstyle\sum_{\alpha=1}^n X_{m-1,\alpha}\sigma_m(T_\alpha)). \end{aligned}$$

Note that the specialized system has a nontrivial solution by assumption, hence neither side of the equation is zero. If we consider the parameters $X_{m,\alpha}$ as fixed and look just at the $X_{m-1,0}, ..., X_{m-1,n-1}$, the equation forms a "system of linear equations" in $X_{m-1,0}, ..., X_{m-1,n-1}$. This system consists of only 1 equation and has n indeterminates. Isolating one coefficient of X_{m-1}, denoted by $X_{m-1,\alpha_1'}$, gives us the following expression for $X_{m-1,\alpha_1'}$:

$$\frac{(\sum_{\alpha''\neq\alpha_1'} X_{m,\alpha''}\sigma_m(T^{\alpha''})) \cdot c_{m-1,m,k_{m,m-1}} \cdot X_m - (\sum_{\alpha''\neq\alpha_1'} X_{m-1,\alpha''}T^{\alpha''}) \cdot \sigma_{m-1}\sigma_m(X_{k_{m,m-1}}) \cdot \sigma_{m-1}(X_m)}{T \cdot \sigma_{m-1}\sigma_m(X_{k_{m,m-1}}) \cdot \sigma_{m-1}(X_m) - \sigma_m(T) \cdot c_{m-1,m,k_{m,m-1}} \cdot X_m}.$$

Hence $X_{m-1,\alpha_1'}$ is a rational function in the remaining $n-1$ coefficients, denoted by $X_{m-1,\alpha''}$, and $T_1, ..., T_n$ and the elements $X_{m,1}, ..., X_{m,n}$. We have to make sure that the denominator of this expression will not become zero when specializing the equations later on:

We know by assumption that the set of elements $x_{i,\alpha} \in K$ is a solution to the whole system of all the equations of types (1) and (2) of the specialized system. Hence the elements $x_{m-1,1}, ..., x_{m-1,n}$ form a solution of the "subsystem" consisting of only one equation obtained from specializing this equation. Furthermore the equation is not zero and is a linear equations. Thus we have a solvable "system of linear equations". So there exists at least one parameter in the specialized equation that can be isolated, hence be expressed as a rational function of in the other parameters. So by Lemma 3.2.2 the same holds for the equation considered here and thus we can choose $X_{m-1,\alpha_1'}$ in such a way that the function above and its specialization are well defined. Again, we denote the set of coefficients $X_{m-1,\alpha}$ of X_{m-1} by $\mathbf{A}_{m-1} := \{X_{m-1,\alpha} \mid \alpha = 1, ..., n\}$, the set containing the isolated coefficient by $\mathbf{A}'_{m-1} := \{X_{m-1,\alpha_1'}\}$ and the set of the remaining coefficients by $\mathbf{A}''_{m-1} := \{X_{m-1,\alpha} \mid \alpha = 1, ..., n, \ \alpha \neq \alpha_1'\}$. Thus we have a disjoint decomposition

$$\mathbf{A}_{m-1} = \mathbf{A}'_{m-1} \cup \mathbf{A}''_{m-1}$$

and we write to visualize that $X_{m-1,\alpha_1'}$ depends on the elements of $\mathbf{A}_m, \mathbf{A}''_{m-1}$ and the T_i:

$$X_{m-1,\alpha_1'} = X_{m-1,\alpha_1'}(\mathbf{A}_m, \mathbf{A}''_{m-1}, T_1, ..., T_n).$$

We see that the expression thus obtained does not contain any roots, as it is obtained from solving a linear equation. Now we replace in this expression the coefficient $X_{m,\alpha_1'}$ with the term obtained above (from solving the equation belonging to the commutator $\tau = [\sigma_m, \sigma_l]$) and arrive at an expression depending only on $\mathbf{A}''_m, \mathbf{A}''_{m-1}$ and $T_1, ..., T_n$, hence we write

$$X_{m-1,\alpha_1'} = X_{m-1,\alpha_1'}(\mathbf{A}''_m, \mathbf{A}''_{m-1}, T_1, ..., T_n)$$

to visualize that $x_{m-1,\alpha_1'}$ can be written as a rational function in $\mathbf{A}''_m, \mathbf{A}''_{m-1}$ and $T_1, ..., T_n$.

We continue by examining the equations coming from commutator equations of the form $\sigma_{k_{j,m-2}} = [\sigma_j, \sigma_{m-2}]$ satisfying $j > m-2$. There are two equations of this type:

$$\begin{array}{rl} & \sigma_{m-2}\sigma_m(X_{k_{m,m-2}}) \cdot (\sum_{\alpha=1}^{n} X_{m-2,\alpha}T_\alpha) \cdot \sigma_{m-2}(X_m) \\ = & c_{m-2,m,k_{m,m-2}} \cdot X_m \cdot (\sum_{\alpha=1}^{n} X_{m-2,\alpha}\sigma_m(T_\alpha)) \end{array}$$

$$\begin{array}{rl} & \sigma_{m-2}\sigma_{m-1}(X_{k_{m-1,m-2}}) \cdot (\sum_{\alpha=1}^{n} X_{m-2,\alpha}T_\alpha) \cdot \sigma_{m-2}(X_{m-1}) \\ = & c_{m-2,m-1,k_{m-1,m-2}} \cdot X_{m-1} \cdot (\sum_{\alpha=1}^{n} X_{m-2,\alpha}\sigma_{m-1}(T_\alpha)) \end{array}$$

We proceed now exactly as before: The equations are of the same form as above, but we consider now $X_{m-2,0}, ..., X_{m-2,n}$, as the parameters of this system of equations and assume $X_{m-1,1}, ..., X_{m-1,n}$ and $X_{m,1}, ..., X_{m,n}$ to be fixed. As above, the equations then form a system of linear equations. This system consists of 2 equations and has again n indeterminates and we know again that there exists a solution of the specialized system given by $x_{m-2,0}, ..., x_{m-2,n}$.
We know that the specialized system is solvable but we have to make sure that the system defined over $K(T_1, ..., T_n)$ considered here is also solvable. This follows from the following considerations: Assume the specialized equations are not linearly independent. Then one of the equations can be omitted or is automatically satisfied. Since each equation reflects a commutator relation, this means that one of the commutator relations in the list on page 54 is not needed. Hence the solvability of the embedding problem is independent of one of those commutator relations. So either the basic commutator described by this relation is not necessary for the description of τ (in terms of basic commutators of lower weight) or the relation for this basic commutator is determined by the remaining relations.
In the first case, this contradicts the fact that the subgroup H_2 of G is chosen as the largest possible subgroup, generated by basic commutators, such that τ cannot be build up by its basic commutators: By adding the basic commutator of the relation in question to H_2 we would obtain a larger group. This group is still generated by basic commutators, because we see from Theorem 2.1.3 that the preimage of a basic commutator of E/H_1 can be chosen to be a basic commutator of E a canonical way. Hence we have a contradiction to maximality of H_2.
The second case means that we have a commutator relation that is not necessary to determine E/H_1 uniquely, i.e. it is already determined by the remaining relations. But we have imposed no relations on the basic commutators generating the group E/H_1 aside from bounding the orders of the basic commutators. So this contradicts the fact that the only relations between basic commutators are the very relations needed for their definition, which is a minimal set of relations. Hence with the specialized equations being linearly independent, we know from Lemma 3.2.2 that the system of equations over $K(T_1, ..., T_n)$ consists of linearly independent equations and is solvable.

Using the same argument as in the step above, we can thus find 2 coefficients of

X_{m-2}, denoted by X_{m-2,α'_1} and X_{m-2,α'_2}, that can be written as well defined rational functions in the remaining $n-2$ coefficients, denoted by $X_{m-2,\alpha''}$, and $T_1, ..., T_n$ and the elements X_{m-1}, X_m. Again, we denote the set of coefficients $X_{m-2,\alpha}$ of X_{m-2} by $\mathbf{A}_{m-2} := \{X_{m-2,\alpha} \mid \alpha = 1, ..., n\}$, the set containing the coefficients that have been isolated in the equations by $\mathbf{A}'_{m-2} := \{X_{m-2,\alpha'_1}, X_{m-2,\alpha'_2}\}$ and the set of the remaining coefficients by $\mathbf{A}''_{m-2} := \{X_{m-2,\alpha} \mid \alpha = 1, ..., n,\ \alpha \neq \alpha'_1, \alpha'_2\}$. Thus we have a disjoint decomposition

$$\mathbf{A}_{m-2} = \mathbf{A}'_{m-2} \cup \mathbf{A}''_{m-2}.$$

Now we replace in the expressions above the coefficients $X_{m,\alpha'_1}, X_{m-1,\alpha'_1}$ by the terms obtained before and arrive at rational functions dependent only on $\mathbf{A}''_m, \mathbf{A}''_{m-1}, \mathbf{A}''_{m-2}$ and $T_1, ..., T_n$, hence we write

$$X_{m-2,\alpha'_1} = X_{m-2,\alpha'_1}(\mathbf{A}''_m, \mathbf{A}''_{m-1}, \mathbf{A}''_{m-2}, T_1, ..., T_n)$$

and

$$X_{m-2,\alpha'_2} = X_{m-2,\alpha'_2}(\mathbf{A}''_m, \mathbf{A}''_{m-1}, \mathbf{A}''_{m-2}, T_1, ..., T_n).$$

The rational functions thus obtained do not contain any roots as they are obtained from solving a linear equation, it is however possible that some coefficients $X_{j,\alpha''}$, $j > m-2$ appear nonlinearly.

The other steps are done inductively in the same way for decreasing i. We consider in the i-th step the equations coming from commutators of the form $\sigma_{k_{j,i}} = [\sigma_j, \sigma_i]$ satisfying $j > i$, i.e. the equations

$$\begin{aligned}
\sigma_i\sigma_m(X_{k_{m,i}}) \cdot (\sum_{\alpha=1}^{n} X_{i,\alpha}T_\alpha) \cdot \sigma_i(X_m) &= c_{i,m,k_{m,i}} \cdot X_m \cdot (\sum_{\alpha=1}^{n} X_{i,\alpha}\sigma_m(T_\alpha)) \\
&\cdots \\
\sigma_i\sigma_{i+1}(X_{k_{i+1,i}}) \cdot (\sum_{\alpha=1}^{n} X_{i,\alpha}T_\alpha) \cdot \sigma_i(X_{i+1}) &= c_{i,i+1,k_{i+1,i}} \cdot X_{i+1} \cdot (\sum_{\alpha=1}^{n} X_{i,\alpha}\sigma_{i+1}(T_\alpha)).
\end{aligned}$$

Considering $X_{i+1,1}, ...X_{i+1,n}, ..., X_{m,1}, ..., X_{m,n}$ as fixed as above, the equations then form a system of $m-i$ linear equations for $X_{i,0}, ..., X_{i,n-1}$. Since the subsystem of equations considered in the i-th step is part of the whole system of equations of type (1) and (2), we know that the specialized subssystem has a solution given by $x_{i,0}, ..., x_{i,n-1}$. We know again, with the same argument as in the previous step and by using Lemma 3.2.2, that the subsystem is linearly independent over $K(T_1, ..., T_n)$ and solvable. Again, we denote the set of coefficients $X_{i,\alpha}$ by $\mathbf{A}_i := \{X_{i,\alpha} \mid \alpha = 1, ..., n\}$, the set containing the coefficient that have been isolated in the equations by $\mathbf{A}'_i := \{X_{i,\alpha'_1}, ..., X_{i,\alpha'_{m-i}}\}$ and the set of the remaining coefficients by $\mathbf{A}''_i := \{X_{i,\alpha} \mid \alpha = 1, ..., n,\ \alpha \neq \alpha'_1, ..., \alpha'_{m-i}\}$. Thus we have a disjoint decomposition

$$\mathbf{A}_i = \mathbf{A}'_i \cup \mathbf{A}''_i.$$

Thus we arrive at rational functions

$$\begin{aligned} X_{i,\alpha'_1} &= X_{i,\alpha'_1}(\mathbf{A}_m, ..., \mathbf{A}_{i+1}, \mathbf{A}''_i, T_1, ..., T_n), \\ &\;... \\ X_{i,\alpha'_{m-i}} &= X_{i,\alpha'_{m-i}}(\mathbf{A}_m, ..., \mathbf{A}_{i+1}, \mathbf{A}''_i, T_1, ..., T_n). \end{aligned}$$

Now we replace for all $j > i$ in these expressions those coefficients $X_{j,\alpha'}$ that have been determined in the steps before and arrive at expressions dependent only on $\mathbf{A}''_m, ..., \mathbf{A}''_i$ and $T_1, ..., T_n$:

$$\begin{aligned} X_{i,\alpha'_1} &= X_{i,\alpha'_1}(\mathbf{A}''_m, ..., \mathbf{A}''_i, T_1, ..., T_n), \\ &\;... \\ X_{i,\alpha'_{m-i}} &= X_{i,\alpha'_{m-i}}(\mathbf{A}''_m, ..., \mathbf{A}''_i, T_1, ..., T_n). \end{aligned}$$

In doing so, we finally arrive at a system of equations:

$$\begin{aligned} X_{m,\alpha'_1} &= X_{m,\alpha'_1}(\mathbf{A}''_m, T_1, ..., T_n), \\ \\ X_{m-1,\alpha'_1} &= X_{m-1,\alpha'_1}(\mathbf{A}''_m, ..., \mathbf{A}''_{m-1}, T_1, ..., T_n), \\ \\ X_{m-2,\alpha'_1} &= X_{m-2,\alpha'_1}(\mathbf{A}''_m, ..., \mathbf{A}''_{m-2}, T_1, ..., T_n), \\ X_{m-2,\alpha'_2} &= X_{m-2,\alpha'_2}(\mathbf{A}''_m, ..., \mathbf{A}''_{m-2}, T_1, ..., T_n), \\ \\ &\;... \\ \\ X_{i,\alpha'_1} &= X_{i,\alpha'_1}(\mathbf{A}''_m, ..., \mathbf{A}''_i, T_1, ..., T_n), \\ &\;... \\ X_{i,\alpha'_{m-i}} &= X_{i,\alpha'_{m-i}}(\mathbf{A}''_m, ..., \mathbf{A}''_i, T_1, ..., T_n), \\ \\ &\;... \\ \\ X_{1,\alpha'_1} &= X_{1,\alpha'_1}(\mathbf{A}''_m, ..., \mathbf{A}''_1, T_1, ..., T_n), \\ &\;... \\ X_{1,\alpha'_{m-1}} &= X_{1,\alpha'_{m-1}}(\mathbf{A}''_m, ..., \mathbf{A}''_1, T_1, ..., T_n). \end{aligned}$$

This system is equivalent to the original system described by the equations of types (1) and (2) but expresses some coefficients $X_{i,\alpha'}$ as rational functions of the remaining coefficients $X_{i,\alpha''}$ from the sets $\mathbf{A}''_i$ and the powers of $T_1, ..., T_n$. This system is not necessarily unique. In each step other choices for $X_{i,\alpha'}$ might be expressable in the remaining coefficients of a given X_i. The important part is that in each step at least one choice is possible. But as noted above this is assured, because we know that each subsystem has a solution and because each subsystem consists of linear equations it is possible to isolate the respective $X_{i,\alpha'}$.

We note that up to this point the fact that the extension M/K is obtained from specializing an extension $\tilde{M}/K(t)$ has not been used. We have only used the fact that there are solutions to certain equations (the equations of types (1), (2) and (3)) and then reformulated some of these equations (the equations of types (1) and (2)).

Step 4:

In this step we will consider the equations of type (3). We will use these equations to write some of the parameters as rational functions in the remaining parameters.

We will now use the equations (3), i.e. those of the form

$$\sigma_i(Y_i) = X_i \cdot Y_i,$$

to determine the coefficients of $y_{j,\beta}$ as functions of $x_{i,\alpha}$ and $\theta_1, ..., \theta_n$. We write

$$Y_j := \sum_{\beta=1}^{n} Y_{j,\beta} T_\beta$$

to arrive at equations

$$\sigma_i(\sum_{\beta=1}^{n} Y_{j,\beta} T_\beta) = X_i \cdot (\sum_{\beta=1}^{n} Y_{j,\beta} T_\beta).$$

Again, we have replaced the roots $\theta_1, ..., \theta_n$ in the original equations by the indeterminates $T_1, ..., T_n$ and we solve now each equation for one coefficient $Y_{i,\beta'}$. Again this is possible because we know that $x_i \in M, y_{i,\beta} \in K$ are part of a solution to the whole specialized system of equations of types (1),(2),(3) over K, so we know in particular that the system is solvable. Hence we arrive at expressions of the form

$$Y_{i,\beta'} = \frac{\sum_{\beta''\neq\beta'} Y_{i,\beta''}\sigma_i(T^{\beta''}) - X_i \cdot (\sum_{\beta''\neq\beta'} Y_{i,\beta''} T^{\beta''})}{\sigma_i(T^{\beta'}) - X_i \cdot T^{\beta'}}.$$

As above, these expressions are well-defined: For some fixed $x_{i,1}, ..., x_{i,n}$ from a solution of the whole system of the original set of all specialized equations of types (1),(2),(3) defined over the field K, the $y_{i,\beta}$ form a solution of the linear “subsystem” given by the equation

$$\sigma_i(\sum_{\beta=1}^{n} \bar{X}_{j,\beta}\theta_\beta) = x_i \cdot (\sum_{\beta=1}^{n} \bar{X}_{j,\beta}\theta_\beta).$$

Thus we have a “system of linear equations” consisting of one equation, not equal to zero, and so there exists at least one parameter that can be expressed as a rational function in the remaining parameters without the denominator becoming zero. So we can choose $Y_{i,\beta'}$ in a way that the function above and its specialization obtained by replacing the T_i by θ_i are well-defined.

As above, not all coefficients will by determined in this process. We denote the sets of coefficients $Y_{j,0}, ..., Y_{j,n-1}$ for a given Y_j by $\mathbf{B}_j$ and we denote again all coefficients determined by the process above by $Y_{j,\beta'}$ and the sets of coefficients thus determined by $\mathbf{B}'_j$. The sets of the remaining coefficients will be denoted by $\mathbf{B}''_j$. Hence we arrive at a system of equations that gives some coefficients $Y_{j,\beta'} \in \mathbf{B}'_j$ as functions of the remaining coefficients $Y_{j,\beta''} \in \mathbf{B}''_j$, the coefficients $X''_{i,\alpha} \in \mathbf{A}''_i$ and the powers of $T_1, ..., T_n$ that is equivalent to the system of equations (3).

In total we have shown that the sets of coefficients $\mathbf{A}_i = \{X_{i,\alpha} \mid \alpha = 1, ..., n\}$, $\mathbf{B}_i = \{Y_{i,\beta} \mid \beta = 1, ..., n\}$ of the X_i and Y_j can be subdivided into two disjoint subsets

$$\mathbf{A}_i = \mathbf{A}'_i \cup \mathbf{A}''_i \text{ for each of the elements } X_i,$$

$$\mathbf{B}_i = \mathbf{B}'_i \cup \mathbf{B}''_i \text{ for each of the elements } Y_i,$$

such that the coefficients $X_{i,\alpha'} \in \mathbf{A}'_i$ and $Y_{j,\beta'} \in \mathbf{B}'_j$ are determined by the remaining coefficients $X_{i,\alpha''} \in \mathbf{A}''_i$ and $Y_{j,\beta''} \in \mathbf{B}''_j$ the $T_1, ..., T_n$ via the original set of equations. We replace now each coefficient $X_{i,\alpha'}$ by its expression gained from solving the equations of types (1) and (2) and get a system of equations $(*)$:

$$X_{i,\alpha'} = X_{i,\alpha'}(\mathbf{A}''_m, ..., \mathbf{A}''_1, T_1, ..., T_n),$$

$$Y_{j,\beta'} = Y_{j,\beta'}(\mathbf{A}''_m, ..., \mathbf{A}''_1, \mathbf{B}''_m, ..., \mathbf{B}''_1, T_1, ..., T_n),$$

that is equivalent to the original system of equations (1), (2), (3). Still, we have not used the fact that the extension M/K is obtained from specializing an extension $\tilde{M}/K(t)$. Up to this point we have only reformulated the equations of types (1), (2) and (3) using the fact that we know that they are solvable over K by assumption.

Step 5:

We will now address the problem of lifting the solutions of $(*)_\theta$ to a solution of the corresponding system $(*)_{\tilde{\theta}}$ of equations over $K(t)$.

We start with a solution x_i, y_j of the original system of equations. If $x_{i,\alpha}$ denotes the coefficient of x_i corresponding to $X_{i,\alpha}$ for all $i = 1, ..., m, \alpha = 1, ..., n$ and $y_{j,\beta}$ denotes the coefficient of y_j corresponding to $Y_{j,\beta}$ for all $j = 1, ..., m$, $\beta = 1, ..., n$, we get an induced decomposition of the sets $\mathbf{a}_i := \{x_{i,\alpha} \mid \alpha = 1, ..., n\}$, $\mathbf{b}_i = \{y_{i,\beta} \mid \beta = 1, ..., n\}$ of the x_i and y_j via:

$$\mathbf{a}_i = \mathbf{a}'_i \cup \mathbf{a}''_i \text{ for each of the elements } x_i,$$

$$\mathbf{b}_i = \mathbf{b}'_i \cup \mathbf{b}''_i \text{ for each of the elements } y_i.$$

When we "evaluate" the rational functions

$$X_{i,\alpha'} = X_{i,\alpha'}(\mathbf{A}''_m, ..., \mathbf{A}''_1, T_1, ..., T_n),$$
$$Y_{j,\beta'} = Y_{j,\beta'}(\mathbf{A}''_m, ..., \mathbf{A}''_1, \mathbf{B}''_m, ..., \mathbf{B}''_1, T_1, ..., T_n),$$

by specializing the indeterminates T_i to the roots θ_i and each $X''_{i,\alpha} \in \mathbf{A}''_i$ and $Y''_{i,\beta} \in \mathbf{B}''_i$ to the corresponding $x''_{i,\alpha} \in \mathbf{a}''_i$ and $y''_{i,\beta} \in \mathbf{b}''_i$ we get

$$x_{i,\alpha'} = X_{i,\alpha'}(\mathbf{a}''_m, ..., \mathbf{a}''_1, \theta_1, ..., \theta_n),$$
$$y_{j,\beta'} = Y_{j,\beta'}(\mathbf{a}''_m, ..., \mathbf{a}''_1, \mathbf{b}''_m, ..., \mathbf{b}''_1, \theta_1, ..., \theta_n).$$

We note that we have for each of the elements $x_{i,\alpha'}, y_{j,\beta'}$ obtained rational functions in the $x''_{i,\alpha}, y''_{i,\beta}$ and the roots θ_i but we do not know how these functions exactly look like without actually computing the function using the process above. In particular, the θ_i will appear in these functions nonlinearly. This is no problem however, since the specialization $\Phi : K(T_1, ..., T_n) \to K(\theta_1, ..., \theta_n)$ is $\mathrm{Gal}(F^{H_1}/K)$-equivariant. Hence it makes no difference whether we compute the action of $\mathrm{Gal}(F^{H_1}/K) = E/H_1$ on any $X_{i,\alpha'}, Y_{j,\beta'}$ before we specialize these elements or if we compute the action of $\mathrm{Gal}(F^{H_1}/K) = E/H_1$ on the specialized $x_{i,\alpha'}, y_{j,\beta'}$.

We can now do the same over $K(t)$. We specialize the system via $T_i \mapsto \tilde{\theta}_i$. We note that the specialization $T_i \mapsto \theta_i$ is the composition of the specialization $T_i \mapsto \tilde{\theta}_i$ and the specialization $\varphi : \tilde{\theta}_i \mapsto \theta_i$, hence as long as all the images under the specialization $T_i \mapsto \theta_i$ are well defined, the images under the specialization $T_i \mapsto \tilde{\theta}_i$ are well defined as well. Thus we get equations in the parameters $\tilde{X}_{1,0}, ..., \tilde{X}_{m,n-1}$ over $K(t)$:

$$\begin{aligned}
\sigma_i\sigma_j(\tilde{X}_k) \cdot \tilde{X}_i \cdot \sigma_i(\tilde{X}_j) &= \frac{c(\sigma_i\sigma_j, [\sigma_i, \sigma_j]) \cdot c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot \tilde{X}_j \cdot \sigma_j(\tilde{X}_i) \text{ for } \sigma_k = [\sigma_i, \sigma_j], \\
\tilde{X}_i \cdot \sigma_i(\tilde{X}_j) &= \frac{c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)} \cdot \tilde{X}_j \cdot \sigma_j(\tilde{X}_i) \text{ for } 1 = [\sigma_i, \sigma_j] \text{ or } \tau = [\sigma_i, \sigma_j], \\
\sigma_i(\tilde{Y}_i) &= \tilde{X}_i \cdot \tilde{Y}_i
\end{aligned}$$

with

$$\tilde{X}_i := \sum_{\alpha=1}^{n} \tilde{X}_{i,\alpha}\tilde{\theta}_\alpha,$$
$$\tilde{Y}_j := \sum_{\beta=1}^{n} \tilde{Y}_{j,\beta}\tilde{\theta}_\beta,$$

The system $(*)$ becomes then a system of equations over $K(t)$, denoted by $(*)_{\tilde{\theta}}$ and we have

$$\begin{tikzcd}
K(T_1, ..., T_n) \arrow[r, dash, "T_i \mapsto \tilde{\theta}_i"] \arrow[d, dash, "E/H_1"'] & K(\tilde{\theta}_1, ..., \tilde{\theta}_n) \subseteq \tilde{M}^{H_2} \arrow[r, dash, "\tilde{\theta}_i \mapsto \theta_i"] \arrow[d, dash, "E/H_1"'] & K(\theta_1, ..., \theta_n) = F^{H_1} \arrow[d, dash, "E/H_1"'] \\
K(T_1, ..., T_n)^{E/H_1} \arrow[r, dash, "T_i \mapsto \tilde{\theta}_i"] & K(\tilde{\theta}_1, ..., \tilde{\theta}_n)^{E/H_1} \subseteq K(t) \arrow[r, dash, "\tilde{\theta}_i \mapsto \theta_i"] & K(\theta_1, ..., \theta_n)^{E/H_1} = K.
\end{tikzcd}$$

We define now

$$\tilde{x}_{i,\alpha''} := x_{i,\alpha''},$$

$$\tilde{x}_{i,\alpha'} := X_{i,\alpha'}(\mathbf{a}''_1, ..., \mathbf{a}''_m, \tilde{\theta}_1, ..., \tilde{\theta}_n,),$$

$$\tilde{y}_{j,\beta''} := y_{j,\beta''},$$

$$\tilde{y}_{j,\beta'} := Y_{j\beta'}(\mathbf{a}''_1, ..., \mathbf{a}''_m, \mathbf{b}''_1, ..., \mathbf{b}''_m, \tilde{\theta}_1, ..., \tilde{\theta}_n).$$

Since each θ_i is an image of the corresponding $\tilde{\theta}_i$ under the specialization map φ, each $x'_{i\alpha}, y'_{i,\beta}$ is an image of the corresponding $\tilde{x}'_{i\alpha}, \tilde{y}'_{i,\beta}$. Thus all $\tilde{x}'_{i\alpha}, \tilde{y}'_{i,\beta}$ are well-defined, because all $x'_{i\alpha}, y'_{i,\beta}$ are well-defined. Furthermore we let

$$\tilde{x}_i := \sum_{\alpha=1}^{n} \tilde{x}_{i,\alpha}\tilde{\theta}_\alpha$$

and

$$\tilde{y}_j := \sum_{\beta=1}^{n} \tilde{y}_{j,\beta}\tilde{\theta}_\beta.$$

Since the system $(*)$ yields a solution of the system of all equations of types (1), (2), (3) if considered as a system for the indeterminates $T_1, ..., T_n$ over $K(T_1, ..., T_n)$, it yields a solution of every specialized system of the equations of types (1), (2), (3). So it does in particular for the specialization $T_i \mapsto \tilde{\theta}_i$.
Hence we have gained a set of coefficients $\tilde{x}_{i,\alpha}, \tilde{y}_{j,\beta}$ precisely in a way, that the elements

$$\tilde{x}_i = \sum_{\alpha=1}^{n} \tilde{x}_{i,\alpha}\tilde{\theta}_\alpha,$$

$$\tilde{y}_j = \sum_{\beta=1}^{n} \tilde{y}_{j,\beta}\tilde{\theta}_\beta$$

satisfy the specialized system of equations of types (1), (2), (3) over $K(t)$. Since the roots $\tilde{\theta}_1, ..., \tilde{\theta}_n$ are elements of $\tilde{M}^{H_2}$, the elements $\tilde{x}_i, \tilde{y}_j$ are then elements of $\tilde{M}^{H_2}$ as desired. □

We revisit the first example of Section 2.1.2 to illustrate how the process of ordering the equations works:

Example: We consider again the embedding problem $(M/K, E_1, G_1)$ given by the group extension

$$\begin{tikzcd} 1 \arrow[r] & \underset{\langle\tau\rangle}{C_3} \arrow[r] & E_1 \arrow[r] & G_1 \arrow[r] & 1 \end{tikzcd},$$

from the first example of Section 2.1.2. The groups G_1 and E_1 are

$$\begin{aligned} G_1 \ := \langle \bar{\sigma}_1, ..., \bar{\sigma}_6 \mid \ & \bar{\sigma}_i^3 = 1, [\bar{\sigma}_2, \bar{\sigma}_1] = \bar{\sigma}_4 [\bar{\sigma}_3, \bar{\sigma}_1] = \bar{\sigma}_5, [\bar{\sigma}_3, \bar{\sigma}_2] = \bar{\sigma}_6, \\ & [\bar{\sigma}_j, \bar{\sigma}_i] = 1 \text{ for } j = 4, 5, 6 \rangle, \end{aligned}$$

$$\begin{aligned} E_1 \ := \langle \sigma_1, ..., \sigma_6, \tau \mid \ & \sigma_i^3 = \tau^3 = 1, [\sigma_2, \sigma_1] = \sigma_4 [\sigma_3, \sigma_1] = \sigma_5, [\sigma_3, \sigma_2] = \sigma_6, \\ & [\sigma_4, \sigma_3] = [\sigma_2, \sigma_1, \sigma_3] = \tau, \\ & [\sigma_i, \sigma_j] = 1 \text{ for any other basic commutator with } j = 4, 5, 6 \rangle. \end{aligned}$$

The embedding problem $(M/K, E_1, G_1)$ is solvable if the equations

$$R_{\sigma_1}(X_{\sigma_1}) = 1, R_{\sigma_2}(X_{\sigma_2}) = 1, R_{\sigma_4}(X_{\sigma_4}) = 1,$$

and

$$X_{\sigma_4} = \sigma_1^{-1} \sigma_2^{-1} (\frac{X_{\sigma_1} \cdot \sigma_1(X_{\sigma_2})}{X_{\sigma_2} \cdot \sigma_2(X_{\sigma_1})}), 1 = \frac{X_{\sigma_1} \cdot \sigma_1(X_{\sigma_4})}{X_{\sigma_4} \cdot \sigma_4(X_{\sigma_1})}, 1 = \frac{X_{\sigma_2} \cdot \sigma_2(X_{\sigma_4})}{X_{\sigma_4} \cdot \sigma_4(X_{\sigma_2})}, 1 = \zeta^{-1} \frac{\sigma_3(X_{\sigma_4})}{X_{\sigma_4}}$$

have a solution in F^{H_1}, where ζ is a primitive 3-rd root of unity. We order the equations of types (1) and (2) according to the rules of Lemma 3.2.4:

$$1 = \zeta^{-1} \frac{\sigma_3(X_{\sigma_4})}{X_{\sigma_4}}$$

will be resolved for one coefficient of X_{σ_4}, this coefficient will be replaced by the expression thus gained in

$$1 = \frac{X_{\sigma_2} \cdot \sigma_2(X_{\sigma_4})}{X_{\sigma_4} \cdot \sigma_4(X_{\sigma_2})},$$

which will then be resolved for one coefficient of X_{σ_2}. Both coefficients will be replaced by the expressions obtained from the two equations above in the system

$$1 = \frac{X_{\sigma_1} \cdot \sigma_1(X_{\sigma_4})}{X_{\sigma_4} \cdot \sigma_4(X_{\sigma_1})},$$

$$X_{\sigma_4} = \sigma_1^{-1} \sigma_2^{-1} (\frac{X_{\sigma_1} \cdot \sigma_1(X_{\sigma_2})}{X_{\sigma_2} \cdot \sigma_2(X_{\sigma_1})}),$$

which will be resolved for two coefficients of X_{σ_1}.

Since the kernel of the embedding problems considered in Theorem 3.2.3 is always contained in the commutator subgroup E, we note that the embedding problems are Frattini embedding problems by [Leedham1], Prop. 1.2.4 (see Section 2.3). The solutions obtained by solving these embedding problems are therefore proper regular solutions by Theorems 2.2.6 and 2.2.4. Hence we have:

Corollary 3.2.5. *Every solution field $\tilde{F}$ of an embedding problem $(\tilde{M}/K(t), E, G)$ described in Theorem 3.2.3 is a regular extension of $K(t)$ and has Galois group E.*

There are two obvious questions that arise from Theorem 3.2.3. Firstly, if there is a solvable embedding problem $(M/K, E, G)$ with a solution field F that is obtained from a regular extension $\tilde{M}/K(t)$ by specialization, is there a solution field $\tilde{F}$ of $(\tilde{M}/K(t), E, G)$ that specializes to F? The second question is whether the results obtained in 3.2.3 for embedding problems with cyclic kernel can be generalized to embedding problems with abelian kernel.

These first conjecture is true, the second will be proven for abelian groups that are direct products of isomorphic cyclic groups, as can be seen below:

Theorem 3.2.6. *Let K be a field of characteristic zero that contains all roots of unity and let $(M/K, E, G)$ be a solvable embedding problem as in Theorem 3.2.3 and let $\tilde{M}/K(t)$ be a regular G-extension that specializes to M/K via the specialization map φ. Every solution field F of the embedding problem $(M/K, E, G)$ can be obtained by specializing a solution field $\tilde{F}$ of the embedding problem $(\tilde{M}/K(t), E, G)$.*

Proof. By Theorem 3.2.3 the embedding problem $(\tilde{M}/K(t), E, G)$ is solvable and a solution is of the form $\tilde{F} = \tilde{M}(\sqrt[q]{\tilde{\omega}})$ for an element $\tilde{\omega} \in \tilde{M}$. By Corollary 2.2.7 we have $\frac{\sigma(\tilde{\omega})}{\tilde{\omega}} = \tilde{x}_\sigma^q$, where $\tilde{x}_\sigma$ is defined as in Theorem 3.2.3. Let $\varphi : t \mapsto s, s \in K$ denote the specialization map from $\tilde{M}/K(t)$ to M/K,

$$\mathfrak{O}_\varphi := \left\{ \frac{\tilde{f}}{\tilde{g}} \mid \tilde{f} \in \tilde{M},\ \tilde{g} \in \tilde{M} \text{ and } (t-s) \nmid \tilde{g} \right\}$$

the corresponding valuation ring and $\mathfrak{m}_\varphi := \mathfrak{O}_\varphi(t-s)$ its maximal ideal.
We can assume that $\tilde{\omega} \in \mathfrak{O}_\varphi$: If $\tilde{\omega} \notin \mathfrak{O}_\varphi$, we can multiply it with an appropriate $\tilde{r} \in K(t)$ to arrive at an element $\tilde{\omega}' := \tilde{r}\tilde{\omega} \in \mathfrak{O}_\varphi$. This might change the field $\tilde{F}$ to a new field $\tilde{F}' := \tilde{M}(\sqrt[q]{\tilde{\omega}'})$ but we still have $\mathrm{Gal}(\tilde{F}'/K(t)) = E$, because $(\tilde{M}/K(t), E, G)$ is a Brauer type embedding problem.
Since $\frac{\sigma(\tilde{\omega}')}{\tilde{\omega}'} = \tilde{x}_\sigma^q$ and $\varphi(\tilde{x}_\sigma^q) = x_\sigma^q \neq 0$ we have $\tilde{x}_\sigma^q \notin \mathfrak{m}_\varphi$ and hence $\sigma(\tilde{\omega}') \notin \mathfrak{m}_\varphi$ for all $\sigma \in G$. Hence φ maps $\tilde{\omega}'$ to an element ω' of M that satisfies the relations $\frac{\sigma(\omega')}{\omega'} = x_\sigma^q$, and so $F' = M(\sqrt[q]{\omega'})$ gives a solution of the embedding problem $(M/K, E, G)$.
Every solution of $(M/K, E, G)$ is given by $M(\sqrt[q]{r\omega'})$, for some $r \in K$, and so we can obtain an arbitrary solution by specializing $\tilde{M}(\sqrt[q]{r\tilde{\omega}'})$ for the correct $r \in K$. □

Theorem 3.2.7. *Let K be a field of characteristic zero that contains all roots of unity and let $(M/K, E, G)$ be an embedding problem with abelian kernel of the form $A = C_i^q$, for a cyclic group C_i, such that the embedding problems $(M/K, E_i, G)$ with cyclic kernel induced by the decomposition $A = C_i^q$ are of the form described in Theorem 3.2.3. Then the following holds:*
If $\tilde{M}/K(t)$ is a regular G-extension which specializes to M/K, then there exists a solvable embedding problem $(\tilde{M}/K(t), E, G)$ that specializes to $(M/K, E, G)$.

Proof. In general, an embedding problem with abelian kernel is solvable if and only if the induced embedding problems with cyclic kernel are solvable and have linearly disjoint solutions by [Malle&Matzat1] Theorem IV 1.6. Hence we have to decompose a solution F of $(M/K, E, G)$ into linearly disjoined solutions F_i of $(M/K, E_i, G)$: By Theorem 3.2.3 we have solutions $\tilde{F}_i$ of the embedding problems $(\tilde{M}/K(t), E_i, G)$

specializing to the F_i under the specialization map that maps $\tilde{M}$ to M. Every solution $\tilde{F}_i$ is given by the q-th roots of an element $c_i \in \tilde{M}$, so two solutions are either equal or linearly disjoint over $\tilde{M}$. Hence we obtain a solution of $(\tilde{M}/K(t), E, G)$. Specializing $\tilde{F}$ (using the map above) produces a field that contains all F_i as subextensions. Thus it contains the composite of the F_i as well and this is exactly the solution F of $(M/K, E, G)$ we started with. □

3.3 The arithmetic lifting property for nilpotent groups over $\mathbb{Q}^{ab}$

Using the results of the previous section we can now show that every finite p-group has the arithmetic lifting property over the field $\mathbb{Q}^{ab}$, and in fact over every field of characteristic zero and of cohomological dimension ≤ 1 that contains all roots of unity. This is main result of this thesis. Consequently every nilpotent group can be realized as the Galois group of an extension of $\mathbb{Q}^{ab}(t)$ that is regular over $\mathbb{Q}^{ab}$. We will assume for the following two results that K is a field such that for given primes p every p-group can be realized over K. Otherwise there is nothing to prove; if a p-group cannot be realized over K, there is no extension that could be obtained as a specialization of some extension of $K(t)$, regular over K.

Theorem 3.3.1. *Let q be a power of a prime p. Let K be a field of characteristic zero and of cohomological dimension ≤ 1 that contains all roots of unity and such that every finite p-group can be realized over K as Galois group. For every triple (q, cl, d), where cl and d are integers, the group $G(q, cl, d)$ has the arithmetic lifting property over K. Hence every finite p-group has the arithmetic lifting property over K.*

Proof. The proof is by induction on the class cl. For the first step of the induction we have $G(q, 1, d) = C_q^d$, so the group $G(q, 1, d)$ is abelian and has the arithmetic lifting property over $\mathbb{Q}$ for arbitrary q, d by Theorem 1.3.1. Thus it has the arithmetic lifting property over K as well.
For the inductive step we choose q, d arbitrary but fixed. We have to show that the group $G(q, i+1, d)$ has the arithmetic lifting property over K under the assumption, that for all integers d' and all powers q' of p, the groups $G(q', i, d')$ have the arithmetic lifting property. Assume that F/K is an arbitrary Galois extension with Galois group $G(q, i+1, d)$. Since the center of $G(q, i+1, d)$ is generated by n basic commutators of maximal weight, all of those having order q, we have a central group extension

$$\begin{tikzcd} 1 \arrow[r] & C_q^n \arrow[r] & G(q, i+1, d) \arrow[r] & G(q, i+1, d)/C_q^n \arrow[r] & 1, \end{tikzcd}$$

where $C_q^n = Z(G(q, i+1, d))$.

The group $G(q, i+1, d)/C_q^n$ has nilpotency class i. It is in fact a factor group of the group $G(q^2, i, d)$: Let σ be a basic commutator of $G(q^2, i, d)$ of weight w. The relation in $G(q^2, i, d)$ bounding the order of σ is then given by $\sigma^{q^{2(i-w)}} = 1$. We obtain $G(q, i+1, d)/C_q^n$ as factor group by taking $G(q^2, i, d)$ modulo the relation

$\sigma^{q^{(i+1-w)}} = 1$ for every basic commutator σ of weight w.

By assumption $G(q^2, i, d)$ has the arithmetic lifting property, and by Theorem 3.1.2 the same is true for $G(q, i+1, d)/C_q^n$. At this point we use that all roots of unity are contained in K and that there exist $G(q^2, i, d)$-extensions of K.
Hence, F is the solution field of an embedding problem

$$(M/K, G(q, i+1, cl), G(q, i+1, d)/C_q^n)$$

with abelian kernel. Since $G(q, i+1, d)/C_q^n$ has the arithmetic lifting property by assumption, M/K is a specialization of a regular extension $\tilde{M}/K(t)$ with Galois group $G(q, i+1, d)/C_q^n$. Hence by Theorem 3.2.7, F/K is a specialization of a regular extension $\tilde{F}/K(t)$ with Galois group $G(q, i+1, d)$. This means precisely that $G(q, i+1, d)$ has the arithmetic lifting property over K.

Now, let G be an arbitrary p-group. Since there exist integers q, cl, d such that G can be realized as a factor group of $G(q, cl, d)$ and K has cohomological dimension ≤ 1, G has the arithmetic lifting property over K by Theorem 3.1.2. □

This statement immediately leads to the Main Theorem of this thesis:

Main Theorem: *Let K be a field of characteristic zero and of cohomological dimension ≤ 1 that contains all roots of unity and such that every finite nilpotent group can be realized as Galois group over K. Then every finite nilpotent group has the arithmetic lifting property over K.*

Proof. A finite nilpotent group G is a direct product of finite p-groups by Theorem 2.1.2. Hence G has the arithmetic lifting property over a field of cohomological dimension ≤ 1 that contains all roots of unity by Theorem 1.3.2 and Theorem 3.3.1. □

The most prominent example of a field of cohomological dimension ≤ 1 that contains all roots of unity is $\mathbb{Q}^{ab}$, the maximal abelian extension of $\mathbb{Q}$. From the Main Theorem we deduce immediately:

Corollary 3.3.2. *Every finite nilpotent group can be realized as the Galois group of an extension of $\mathbb{Q}^{ab}(t)$ that is regular over $\mathbb{Q}^{ab}$.*

Proof. Every nilpotent group can be realized as the Galois group of an extension of $\mathbb{Q}^{ab}$ by a classical result of I. R. Shafarevich, see [Shafarevich1]. Furthermore every finite nilpotent group has the arithmetic lifting property over $\mathbb{Q}^{ab}$ by the Main Theorem of this thesis. Thus every nilpotent group can be certainly realized as the Galois group of an extension of $K(t)$ that is regular over K. □

Corollary 3.3.3. *Let K be a field that contains $\mathbb{Q}^{ab}$. Then every finite nilpotent group can be realized as the Galois group of an extension of $K(t)$ that is regular over K.*

Proof. Let G be a nilpotent group. Let $\tilde{M}$ be an extension of $\mathbb{Q}^{ab}(t)$ that is regular over $\mathbb{Q}^{ab}$, and has Galois group G. Such an extension exists by Corollary 3.3.2. We may assume that K and $\mathbb{Q}^{ab}(t)$ are linearly disjoint over $\mathbb{Q}^{ab}$. Then $K \otimes_{\mathbb{Q}^{ab}} \mathbb{Q}^{ab}(t)$ is an extension of constants with respect to the indeterminate t and thus $(K \otimes_{\mathbb{Q}^{ab}} \mathbb{Q}^{ab}(t)) \otimes_{\mathbb{Q}^{ab}(t)} \tilde{M}$ is a Galois extension of $K(t)$ with Galois group G that is regular over K. □

This last corollary extends the result of J. Sonn that every nilpotent group can be realized regularly over $\mathbb{Q}^{solv}(t)$ as given in [Sonn1].

3.4 Outlook: The arithmetic lifting property for solvable groups

In 1954 I. R. Shafarevich gave the proof that every solvable group can be realized as a Galois group over $\mathbb{Q}$. In the first step of his proof, done in [Shafarevich1], he showed that every p-group, and hence every nilpotent group, can be realized over $\mathbb{Q}$ using central embedding problems. Unsurprisingly the proof for the arithmetic lifting property of nilpotent groups given in the last sections shares many common ideas with Shafarevich's proof given in [Shafarevich1]. Hence it is natural to ask if the results obtained in this chapter can be generalized to hold for solvable groups. There is, at least, no obvious answer to this question.

The final part of Shafarevich's proof, done in [Shafarevich2], is concerned with the solvability of split embedding problems with nilpotent kernel. He shows that every split-embedding problem with nilpotent kernel is solvable over $\mathbb{Q}$. Using that every solvable group G is a factor group of a nilpotent group by a solvable group of lower order than G, he can then proof by induction on the order of solvable groups that every solvable group occurs as Galois group over $\mathbb{Q}$.

Unfortunately not very much is known about split embedding problems and the arithmetic lifting property besides Theorem 1.3.2. The most far-reaching results in this direction can be found in [Black4]. We need the following definition to state them:

Definition: Let H and G be finite groups. The *wreath* product of G by H is the semi-direct product $N \rtimes G$, where $N := H_1 \times ... \times H_n$, $n = \text{ord } G$, each H_i is a copy of H and G acts on N by permutation of the indices $1, ..., n$.

We then have

Theorem 3.4.1. ([Black4], Theorem 1.1) *Assume that a finite group G has the arithmetic lifting property over a Hilbertian field K and assume that there exist generic polynomials for another finite group H over the same field K. In this situation the wreath product $H \wr G$ has the arithmetic lifting property over K.*

E. Black uses this Theorem to obtain some results on the arithmetic lifting property and the formation of semi-direct products: If in addition to the assumptions of the theorem above H is abelian and the orders of H and G are relatively prime, it is shown in [Black4] *Cor.*1.3 that the semi-direct product $H \rtimes G$ has the arithmetic lifting property as well. The central arguments of the proof of this corollary are that if H is abelian then $H \rtimes G$ is a factor group of $H \wr G$ and if the orders of H and G are relatively prime the group extension given by $(H \wr G)/(H \rtimes G)$ splits.

The condition $\mathrm{ord}(H)$ and $\mathrm{ord}(G)$ being relatively prime can be omitted if we assume that K has cohomological dimension ≤ 1 by Theorem 3.1.2. It remains however a crucial part that there have to exist generic polynomials for H for the proof to work. As noted in the introduction, there exist generic polynomials for an abelian group H precisely if H does not contain an element of order 8.

So, for now there is not even a way known, to infer from the fact that a group G has the arithmetic lifting property, that general split group extensions of G with abelian kernel have the arithmetic lifting property as well. With regard to this, even though it may seem likely that every solvable group has the arithmetic lifting property over $\mathbb{Q}^{ab}$, there appears to be no obvious way to proof this conjecture.

Chapter 4

Some other results on the arithmetic lifting property

4.1 Other results on the arithmetic lifting property

The two results presented in this section are neither concerned with p-groups nor used anywhere in the text but arise as corollaries to Theorem 3.1.2.

Definition: A group G is called *semiabelian* if it can be constructed in finitely many steps, starting from the trivial group, by taking semidirect products with finite abelian kernel and by taking factor groups. (For further characterizations and properties see [Malle&Matzat1] Chapter IV, Section 2.3.)

Corollary 4.1.1. *Let K be a Hilbertian field of cohomological dimension ≤ 1 that contains all roots of unity. Every semiabelian group has the arithmetic lifting property over K.*

Proof. Every semiabelian group G is factor group of an iterated wreath product of cyclic groups according to [Stoll1], i.e.

$$G \;\simeq\; C_m^{\wr n}/N \;=\; \underbrace{C_m \wr \ldots \wr C_m}_{n-times}/N$$

for suitable $m, n \in \mathbb{N}$ and a suitable normal subgroup $N \lhd C_m^{\wr n}$. Such wreath products have the arithmetic lifting property over Hilbertian fields according to [Black3], Cor. 4.5. Hence by Theorem 3.1.2 G has the arithmetic lifting property over K. □

Corollary 4.1.2. *Let A be an abelian group and let G be a group which has the arithmetic lifting property over a Hilbertian field K of cohomological dimension ≤ 1 such that the following conditions are satisfied: The characteristic of K is prime to the order of A and the extension $K(\zeta_q)/K$ is cyclic, when ζ_q denotes a primitive q-th root of unity and q is the exponent of the 2-Sylow subgroup of A. (The field $\mathbb{Q}^{ab}$, for example, satisfies all those conditions.)*
Then the semidirect product $A \rtimes G$ has the arithmetic lifting property over K.

Proof. The semidirect product $A \rtimes G$ is a factor group of the wreath product $A \wr G$ according to [Huppert1] Ch.2 Thm. 10.10. By [Black3], Cor. 4.5 the group $A \wr G$ has the arithmetic lifting property over any Hilbertian field K satisfying the conditions of the corollary. □

4.2 Lists of groups having the arithmetic lifting property

For certain groups, the arithmetic lifting property or the existence of generic polynomials have been verified over certain algebraic number fields or even over $\mathbb{Q}$. The next two tables give an overview of some of these groups or group products. The list is restricted to fields of characteristic zero.
In the last column of each line of the tables a reference for each group or group product is given.

4.2.1 List of groups having the arithmetic lifting property

For the groups of this list either there exist no generic polynomials or the existence of generic polynomials is unknown.

Group	**Field K**	**Reference**
A_n, the alternating group	char $K = 0$	[Black3]
Abelian groups	number field	[Beckmann1], *Cor. 2.4*
$H_1 \times H_2$ $H_1,\ H_2$ have the arithmetic lifting property	K Hilbertian	[Black3], *Cor. 2.2*
$C \rtimes H$ C cyclic, H has arithm. lifting property, ord C and ord H prime to each other	K Hilbertian, char $K \nmid$ ord C,	[Black3], *Cor. 4.4*
$A \rtimes H$ A abelian, there are generic polynomials for A, H has arithm. lifting property	K Hilbertian, ord A and ord H prime to each other	[Black3], *Cor. 4.4*

Group	**Field** K	**Reference**
$A \wr H$ A abelian, H has arithm. lifting property	K Hilbertian, char $K \nmid$ ord A, $K(\mu_q)/K$ cyclic	[Black3], *Cor. 4.5*
$G \wr H$ there are generic polynomials for G, H has arithm. lifting property	K Hilbertian	[Black4], *Cor. 1.2*

4.2.2 List of groups with generic polynomials

For these groups the existence of generic polynomials is known. Hence they have the arithmetic lifting property by [Jensen1], *Proposition 3.3.8* to *Theorem 3.3.10.* This list is just a selection with emphasis on p-groups.

Group	**Field** K	**Reference**
S_n, the symmetric group	arbitrary	[Jensen1], p. 11
A_4, A_5, alternating groups	arbitrary	[Jensen1], p. 11
$C_2,\ C_4,\ C_n$, n odd	arbitrary	[Jensen1], p. 11
Abelian groups not containing an element of order 8	$\mathbb{Q}$	[Lenstra1]
D_{2^d}, dihedral groups of order 2^{d+1}	char K $\neq 2$, 2^d-th roots of unity contained in K	[Black2], *Cor. 3.4*
$H_1 \times H_2$ there are generic polynomials for $H_1,\ H_2$	number field	[Saltman1]

Bibliography

[Basten1] S. Basten: *Die Arithmetische Liftungseigenschaft für Gruppen der Ordnung p^4*, Diplomarbeit Universität Heidelberg (2006)

[Beckmann1] S. Beckmann: *Is every extension of $\mathbb{Q}$ the specialization of a branched covering*, Journal of Algebra 164 (1994)

[Black1] E. Black: *Arithmetic lifting of dihedral extensions*, Journal of Algebra 203 (1998)

[Black2] E. Black: *Deformations of dihedral 2-group extensions of fields*, Trans. Am. Math. Soc. 351 (1999)

[Black3] E. Black: *On semidirect products and the arithmetic lifting property*, J. London Math. Soc. 60 (1999)

[Black4] E. Black: *Lifting wreath product extensions*, Proc. Am. Math. soc. 129 (2000)

[DiGiacomo1] R. E. Di Giacomo: *Die Arithmetische Liftungseigenschaft für Gruppen der Ordnung 32 und für nicht-semiabelsche Gruppen der Ordnung 64*, Diplomarbeit Universität Heidelberg (2008)

[Harbater1] D. Harbater: *Galois coverings of the arithmetic line*, Lecture Notes in Math. 1240 (1987), 165-195, Springer-Verlag, New York

[Huppert1] B. Huppert: *Endliche Gruppen*, Springer-Verlag (1967)

[Jensen1] C. Jensen, A. Ledet, N. Yui: *Generic Polynomials*, Cambridge University Press (2000)

[Lang1] S. Lang: *Algebra*, Springer-Verlag Berlin Heidelberg (1999)

[Leedham1] C.R. Leedham-Green, S. McKay: *The structure of Groups of Prime Power Order*, Oxford Science Publications (2002)

[Ledet1] A. Ledet: *Brauer Type Embedding Problems*, American Mathematical Society (2005)

[Ledet2] A. Ledet: *Generic polynomials for quasi-dihedral, dihedral and modular extension of order 16*, Proc. Amer. Math. Soc 128 (2000)

[Lenstra1] H.W. Lenstra: *Rational functions invariant under a finite group*, Invent. Math. 25 (1974)

[McKay1] S. McKay: *Finite p-groups*, Queen Mary maths notes (2000)

[Malle&Matzat1] G. Malle, B.H. Matzat: *Inverse Galois Theory*, Springer-Verlag Berlin Heidelberg (1999)

[Massy1] R. Massy: *Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p*, Journal of Algebra 109 (1987)

[Neukirch1] J. Neukirch: *Algebraische Zahlentheorie*, Springer-Verlag Berlin Heidelberg (1992)

[Noether1] E. Noether: *Gleichungen mit vorgeschriebener Gruppe*, Math.Ann 78 (1916)

[Pop1] F. Pop: *Etale Galois covers of affine smooth curves*, Invent. Math. 120 (1995)

[Rotman1] J.J. Rotman: *An Introduction to the Theory of Groups, 4th edition*, Springer-Verlag New York (1995)

[Shafarevich1] I. R. Shafarevich: *On the construction of fields with a given Galois group of order l^α* , Izv. Akad. Nauk SSSR Ser. Mat., 18:3 (1954)

[Shafarevich2] I. R. Shafarevich: *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR Ser. Mat., 18:6 (1954)

[Saltman1] D. Saltman: *Generic Galois extensions and problems in field theory*, Adv. Math. 43 (1982)

[Saltman2] D. Saltman: *Noether's problem over an algebraically closed field*, Invent. Math. 77 (1984)

[Sonn1] J. Sonn: *Brauer groups, embedding problems and nilpotent groups as Galois groups*, Israel Journal of Mathematics 85 (1994)

[Smith1] L. Smith: *Polynomial invariants of finite groups*, Research Notes in Mathematics Vol. 6, B & T (1995)

[Stoll1] M. Stoll: *Construction of semiabelian Galois extensions*, Glasgow Math. Journal 37 (1995)

[Swan1] R.G. Swan: *Invariant rational functions and a problem of Steenrod*, Invent. Math (1969)

[Swallow1] R.G. Swallow: *Central p-extensions of (p,p,...,p)-type Galois groups*, Journal of Algebra 186 (1996)

[Weissauer1] R. Weissauer: *Der Hilbertsche Irreduzibilitätssatz*, J. reine angew. Math. 334 (1982)