On the structure of the absolute Galois group of local fields with residue characteristic 2

Dissertation zur Erlangung des Doktorgrades
der Naturwissenschaften (Dr. rer. nat.)
der Fakultät für Mathematik
der Universität Regensburg

vorgelegt von
Franziska Schneider
aus Heidelberg

im Jahr 2016

Promotionsgesuch eingereicht am: 10. Oktober 2016

Die Arbeit wurde angeleitet von Prof. Dr. Uwe Jannsen.

Prüfungsausschuss:

Vorsitzender: Prof. Dr. Helmut Abels

Erst-Gutachter: Prof. Dr. Uwe Jannsen

Zweit-Gutachter: Prof. Dr. Walter Gubler

weiterer Prüfer: Prof. Dr. Klaus Künnemann

Ersatzprüferin: Prof. Dr. Clara Löh

Contents

Introduction **1**

1 Preliminaries **4**

1.1 Classification of Demuškin groups 4

1.2 Relation structure, cup product and Hilbert Symbol 8

1.2.1 Relation structure and cup product 8

1.2.2 Connection between cup product and Hilbert symbol 10

1.3 Construction of a certain profinite group 11

2 The maximal extension without simple ramification of a local field **14**

2.1 Symplectic spaces 15

2.2 The symplectic structure of $K(i)^*/(K(i)^*)^q$ 18

2.3 The group G_k 23

2.4 Maximal extension without simple ramification 40

3 Conjecture on the absolute Galois group of a local field with residue characteristic 2 **43**

References **49**

Introduction

A central object in number theory is the absolute Galois group $G = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ of a p-adic number field $k/\mathbb{Q}_p$. For example, these groups occur as decomposition groups in the absolute Galois group of a global field $K/\mathbb{Q}$.

For $p \neq 2$ the structure of the absolute Galois group G was determined by Jannsen and Wingberg in [JW]. Their description of G is based on the characterization as a so-called Demuškin formation. The abstract profinite group defined through generators and relations, as well as G, are Demuškin formations with the same numerical invariants, and a uniqueness theorem shown by Wingberg in [W] says that two Demuškin formations with the same invariants are isomorphic.

For $p = 2$ Diekert [D] adapted the method from above and described the Galois group of a 2-adic number field k, whose maximal tamely ramified extension contains the fourth roots of unity, the same way as for $p \neq 2$. Generators and relations were before already used by Zelvenskii to describe the maximal extension without simple ramification of such a field k, but his work [Z2] is based on a paper by Jakovlev [Jak], which contains several mistakes.

In the remaining case, i.e. $p = 2$ and k a 2-adic number field with $k(i)/k$ ramified, the absolute Galois group is still unknown. In this thesis we will not solve this problem, but make a few steps towards a solution. Unfortunately, in this case there is no sensible notion of a Demuškin formation and we have to use a different approach. Nevertheless, in [Z1] Zelvenskii was able to describe the Galois group of the maximal extension without simple ramification k^{wsr} of k as a profinite group with $m+2$ generators and one defining relation, if the degree m of $k/\mathbb{Q}_2$ is odd. He did so by giving three conditions which characterize a group up to isomorphism and showing that they are satisfied for both, a certain group defined by generators and relations and the Galois group $\mathrm{Gal}(K(2)/k)$, where K is an unramified extension of k having odd degree f and $K(2)$ the maximal 2-extension of K. Since k^{wsr} is equal to the union of all such fields $K(2)$, one obtains

the Galois group $\mathrm{Gal}(k^{\mathrm{wsr}}, k)$ as an inverse limit over all these groups. In addition, he claims that for fields k of even degree over $\mathbb{Q}_2$ these three conditions can be shown in an analogous manner.

Overview: In the first section of this thesis we start with some known facts about pro-p groups, in particular Demuškin groups.
The second section concentrates on the paper by Zelvenskii [Z1] and we explain in detail, how he obtained the description of the maximal extension without simple ramification of k, if the degree $k/\mathbb{Q}_2$ is odd. And we prove the following theorem

Theorem. *(Theorem 2.20)*
Let k be an extension of the field of 2-adic numbers having even degree m, such that the maximal unramified extension of k does not contain a primitive 4-th root of unity. Further, let k' denote the intersection of k with the extension $\mathbb{Q}_{2^\infty}$ of the field $\mathbb{Q}_2$, and let $q \geq 4$ denote the largest power of 2 such that the q-th roots of unity belong to $k(i)$.
If k' is not contained in the real subfield of $\mathbb{Q}_{2^\infty}$, then the Galois group of the maximal extension without simple ramification of the field k is isomorphic to the profinite group with $m+2$ generators $x_1, \ldots, x_{m+2}$ subject to the relation

$$x_1^{2+q/2}[x_1, x_2] \ldots [x_{m+1}, x_{m+2}] = 1$$

and the relation $x^{\Delta(2)} = 1$ on the normal subgroup generated by the elements $x_1, x_2, x_4, x_5, \ldots, x_{m+2}$.

We conclude the last section with an idea how one could use the results from section 2 to compute the whole absolute Galois group of k in case $k(i)/k$ is ramified. To this end we approximate the absolute Galois group by its subquotients corresponding to the maximal 2-extensions of all finite tamely ramified extensions L/k. We subdivide L/k into a totally ramified part l/k and an unramified part L/l. We define an abstract group by generators and relations, which we conjecture to be isomorphic to $\mathrm{Gal}(k^{\mathrm{sep}}/k)$. We

identify a subquotient of this abstract group, which under the conjectured isomorphism should correspond to $\mathrm{Gal}(L(2)/l)$. An isomorphism between the latter two groups could be shown following the strategy of Zelvenskii, by showing that each group satisfies the three conditions mentioned above, which characterize a group up to isomorphism. We were able to establish one of these conditions.

Acknowledgment

I would like to express my sincere gratitude to my advisor Professor Uwe Jannsen for the continuous support of my Ph.D study. Thank you for always being available and your motivation, enthusiasm, and immense knowledge.

1 Preliminaries

1.1 Classification of Demuškin groups

Definition 1.1. *Let j and n be non-negative integers and G a profinite group. Then we define the normal subgroups $G^{(j,n)}$ inductively as follows:*

If $j = 0$, let $G^{(0,n)} = G$.

If $j \geq 1$, let $G^{(j,n)} = (G^{(j-1,n)})^n [G^{(j-1,n)}, G]$.

Definition 1.2. *i) A pro-p group (for some prime number p) is a profinite group G such that for any open normal subgroup $N \triangleleft G$ the quotient group G/N is a p-group. (Note that, as profinite groups are compact, the open subgroups are exactly the closed subgroups of finite index.)*

ii) A closed subgroup H of a profinite group G is called a p-Sylow subgroup of G, if for every open normal subgroup N of G, the group HN/N is a p-Sylow subgroup of G/N.

In the rest of this section G will denote a pro-p group.

Proposition 1.3. *([NSW] Proposition 3.9.1)*

i) A convergent subset $S \subset G$ (by convergent we mean every open subgroup of G contains almost all elements of S) generates G as topological group if and only if the set $\overline{S}$ of residue classes modulo $G^{(1,p)}$ generates $G/G^{(1,p)}$. S is a minimal set of generators if and only if $\overline{S}$ is.

ii) For the rank $n(G)$ of G, which is defined as the infimum over the cardinalities of minimal generator systems of G, we have the equality

$$n(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z}).$$

iii) Let S be a set of generators of G. For the relation rank $r(G)$ of G, which is defined as the cardinality of a minimal relation system with respect to S of G, we have the equality

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

Definition 1.4. *Let p be a prime number. A pro-p-group G is called a Demuškin group if*

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

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

iii) the cup product $H^1(G, \mathbb{Z}/p\mathbb{Z}) \times H^1(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z}/p\mathbb{Z})$ is a non-degenerate bilinear form.

Remark 1.5. If G is a Demuškin group, then the following holds:

a) G is a finitely generated topological group with $n(G) = \dim H^1(G, \mathbb{Z}/p\mathbb{Z})$ as the minimal number of generators.

b) There is only one relation among a minimal system of generators for G. This means that G is isomorphic to a quotient $F/(r)$, where F is a free pro-p-group of rank $n = n(G)$ and (r) is the closed normal subgroup of F generated by an element $r \in F^{(1,p)}$.

c) $G/[G,G]$ is isomorphic to $(\mathbb{Z}_p)^{n-1} \times (\mathbb{Z}_p/q'\mathbb{Z}_p)$, where $q' = q'(G)$ is a uniquely determined power of p.

d) $\dim_{\mathbb{F}_p} H^2(N, \mathbb{Z}/p\mathbb{Z}) = 1$ and $n(N) - 2 = (G : N)(n(G) - 2)$ for every open subgroup N of G (see [NSW] Theroem 3.9.15).

In his work [L], Labute classifies pro-2 Demuškin groups by using two invariants. Let G be a pro-2 Demuškin group with $n = \dim H^1(G, \mathbb{F}_2)$. Labute has shown that there

exists a unique continuous homomorphism $\chi\colon G \to U_2$, U_2 the group of units of $\mathbb{Z}_2$, such that, if $I_j(\chi)$ denotes the G-module obtained by letting G act on $\mathbb{Z}/2^j\mathbb{Z}$ by means of χ, the homomorphism $H^1(G, I_j(\chi)) \to H^1(G, I_1(\chi))$ is surjective for all $j \geq 1$. Then in fact, $q' = q'(G)$ is the highest power of 2 such that $\mathrm{Im}(\chi) \subset 1 + q'\,\mathbb{Z}_2$ (see [L] Corollary 4).

Theorem 1.6. *([L] Theorem 2)*
Two Demuškin groups with the same invariants n and $\mathrm{im}(\chi)$ are isomorphic.

Theorem 1.7. *([L] Theorem 3)*
Let $G = F/(r)$ be a Demuškin group with invariants $n = n(G)$, $q' = q'(G)$ and $Im(\chi) = A$.

1) If $q' \neq 2$, there exists a basis $x_1, \ldots, x_n$ of F such that

$$r = x_1^{q'}[x_1, x_2]\ldots[x_{n-1}, x_n] \quad \textit{and} \quad Im(\chi) = 1 + q'\,\mathbb{Z}_2\,.$$

2) If $q' = 2$ and n is odd, there exists a basis $x_1, \ldots, x_n$ of F such that

$$r = x_1^2 x_2^{2^f}[x_2, x_3]\ldots[x_{n-1}, x_n] \quad \textit{and} \quad Im(\chi) = \{\pm 1\} \times U_2^{(f)},$$

for some $f \geq 2$ and $U_2^{(f)} = 1 + 2^f\,\mathbb{Z}_2$.

3) If $q' = 2$ and n is even, there exists a basis $x_1, \ldots, x_n$ of F such that

$$r = x_1^2[x_1, x_2]x_3^{2^f}[x_3, x_4]\ldots[x_{n-1}, x_n] \quad \textit{if } (A : A^2) = 4,$$

$$\textit{and then} \quad Im(\chi) = \pm 1 \times U_2^{(f)},$$

or

$$r = x_1^{2+2^f}[x_1, x_2][x_3, x_4]\ldots[x_{n-1}, x_n] \quad \textit{if } (A : A^2) = 2,$$

$$\textit{and then} \quad Im(\chi) = \langle -1 + 2^f \rangle \subset U_2,$$

for some $f \geq 2$.

Remark 1.8. (see [S] or [L])

For any relation r of the form

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

with n odd and $f \geq 2$ an integer, the group $G = F/(r)$ is a Demuškin group with $n(G) = n$ and $\mathrm{Im}(\chi) = \pm 1 \times U_2^{(f)}$.

Example 1.9. ([L] §5)

Let k be a finite extension of $\mathbb{Q}_2$ of degree m such that k does not contain the 4th roots of unity and $k(2)/k$ the maximal 2-extension of k, e.g. the compositum of all normal (separabel) extensions of k, whose degree is a power of 2. Then $G = \mathrm{Gal}(k(2)/k)$ is a Demuškin group with $n(\mathrm{Gal}(k(2)/k)) = m + 2$ and $q'(\mathrm{Gal}(k(2)/k)) = 2$.

The Galois group of $\mathbb{Q}_{2^\infty} = \bigcup_{i=1}^{\infty} \mathbb{Q}_2(\zeta_{2^i})$ over $\mathbb{Q}_2$ is canonically isomorphic to U_2 under the map $a \mapsto \rho_a$, where $\rho_a(\zeta) = \zeta^a$ for all roots of unity ζ. We get continuous homomorphisms

$$\mathrm{Gal}(k(2)/k) \to \mathrm{Gal}(\mathbb{Q}_{2^\infty}/k') \hookrightarrow \mathrm{Gal}(\mathbb{Q}_{2^\infty}/\mathbb{Q}_2),$$

where the first homomorphism is surjective and $k' = k \cap \mathbb{Q}_{2^\infty}$. Since $\mathbb{Q}_{2^\infty} \subset k(2)$, we obtain a continuous homomorphism $\chi' \colon G \to U_2$, where $\mathrm{Im}(\chi')$ is the Galois group of $\mathbb{Q}_{2^\infty}/k'$. The Galois group $\mathrm{Gal}(\mathbb{Q}_{2^\infty}/k')$ is either isomorphic to the subgroup $\{\pm 1\} \times U_2^{(f)}$ or $\langle -1 + 2^f \rangle \subset U_2$ with $f \geq 2$. Using the exact sequence

$$0 \to \mu_{2^d} \to k(2)^* \xrightarrow{2^d} k(2)^* \to 0,$$

we obtain a commutative diagram

$$\begin{array}{ccccc} k^*/(k^*)^{2d} & \longrightarrow & H^1(G, \mu_{2^d}) & \longrightarrow & H^1(G, I/2^d I) \\ \downarrow & & \downarrow & & \downarrow \\ k^*/(k^*)^2 & \longrightarrow & H^1(G, \mu_2) & \longrightarrow & H^1(G, I/2I) \end{array}$$

for all $d \geq 1$, where $I = I_1(\chi')$ is the profinite G-module defined above. Since the horizontal arrows are all isomorphisms (for the leftmost see [S3] §5, Prop. 20, Lemma

2) and $k^*/(k^*)^{2d} \to k^*/(k^*)^2$ is surjective for all $d \geq 1$, we get that $H^1(G, I/2^dI) \to H^1(G, I/2I)$ is surjective. Thus $\chi = \chi'$, since it is unique and

- if m is odd, then $k = k'$ and $\mathrm{Im}(\chi) = \{\pm 1\} \times U_2^{(2)}$,
- if m is even and $\mathrm{Gal}(\mathbb{Q}_{2^\infty}/k') \cong \{\pm 1\} \times U_2^{(f)}$, then $\mathrm{Im}(\chi) = \{\pm 1\} \times U_2^{(f)}$,
- if m is even and $\mathrm{Gal}(\mathbb{Q}_{2^\infty}/k') \cong \langle -1 + 2^f \rangle$, then $\mathrm{Im}(\chi) = \langle -1 + 2^f \rangle$.

1.2 Relation structure, cup product and Hilbert Symbol

1.2.1 Relation structure and cup product

Let G be a pro-2 group with $\{s_1, \ldots, s_d\}$ a minimal system of generators and

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

a minimal presentation of G with $R = \langle r \rangle$, e.g. $d = \dim_{F_2} H^1(G, \mathbb{F}_2)$ and $\dim_{F_2} H^2(G, \mathbb{F}_2) = 1$. Assume that the orders of the elements $s_\nu[G,G]$, $\nu = 1, \ldots, d$ are multiples of q, a power of 2, or ∞. Then the map $F/[F,F]^q \to G/[G,G]^q$ is an isomorphism and $R \subset F^{(1,q)}$. Furthermore, the inflation

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

with G acting trivially on $\mathbb{Z}/q$ and the transgression

$$\mathrm{tra}\colon H^1(R, \mathbb{Z}/q)^G \to H^2(G, \mathbb{Z}/q)$$

are isomorphisms. The latter follows from the five term exact sequence and because F is free and therefore $H^2(F, \mathbb{Z}/q) = 0$ (see also [K2] Theorem 3.14 and 4.12).
Thus we can define a homomorphism

$$\varphi\colon H^2(G, \mathbb{Z}/q) \to \mathbb{Z}/q \tag{1.2.1}$$

by setting

$$\varphi\alpha = \mathrm{tra}^{-1}\alpha(r).$$

By assumption, G is a one-relator group, hence φ is injective (see [NSW] Proposition 3.9.12).

Let $\{\chi_1, \ldots, \chi_d\}$ be a basis of $H^1(G, \mathbb{Z}/q)$ corresponding to $\{s_1, \ldots, s_d\}$ via

$$\chi_\nu(s_\mu) = \delta_{\nu\mu}, \quad \nu, \mu = 1, \ldots, d.$$

Theorem 1.10. *([K2] Theorem 7.22)*

Every element $g \in G^{(1,q)}$ can be written in the form

$$g = \prod_{\nu=1}^{d} s_\nu^{a_{\nu}q} \prod_{\nu<\mu} [s_\nu, s_\mu]^{a_{\nu\mu}} g', \quad g' \in G^{(2,q)},\ 0 \leq a_\nu, a_{\nu\mu} < q. \tag{1.2.2}$$

Theorem 1.11. *([K2] Theorem 7.23)*

Assume that r is written according to Theorem 1.10, then

$$\varphi(\chi_\nu \cup \chi_\mu) = \begin{cases} -\overline{a}_{\nu\mu} & \text{for } \nu < \mu, \\ -\binom{q}{2}\overline{a}_\nu & \text{for } \nu = \mu, \end{cases} \tag{1.2.3}$$

for $\nu, \mu = 1, \ldots, d$. Here $\cup$ denotes the cup product $H^1(G, \mathbb{Z}/q) \times H^1(G, \mathbb{Z}/q) \to H^2(G, \mathbb{Z}/q)$.

As a result of the theorem above, we obtain the following corollary for the case $q = 2$:

Corollary 1.12. *([JW] Lemma 1)*

Let G be a pro-2 group with $dim H^1(G, \mathbb{F}_2) = d$, $dim H^2(G, \mathbb{F}_2) = 1$ and $\{s_1, \ldots, s_d\}$ a minimal system of generators of G. If the following relation holds in G

$$\prod_{\nu} s_\nu^{a_\nu 2} \prod_{\nu<\mu} [s_\nu, s_\mu]^{a_{\nu\mu}} \equiv 1 \mod G^{(2,2)}$$

with $a_\nu, a_{\nu\mu} \in \mathbb{Z}_2$ and at least one a_ν or $a_{\nu\mu}$ not divisible by 2, then there exists a generator ξ of $H^2(G, \mathbb{F}_2)$, such that for the dual basis $\{\chi_1, \ldots, \chi_d\}$ of $H^1(G, \mathbb{F}_2)$ corresponding to $\{s_1, \ldots, s_d\}$,

$$\chi_\nu \cup \chi_\mu = -a_{\nu\mu}\xi \quad \text{for } \nu < \mu.$$

Proof. See [JW] Lemma 1. The proof there works exactly the same way if $p = 2$. □

1.2.2 Connection between cup product and Hilbert symbol

Now if G is the Galois group of the maximal 2-extension $K(2)$ of a field K and K contains the q-th roots of unity (q a power of 2), the cup product $H^1(G,\mathbb{Z}/q)\times H^1(G,\mathbb{Z}/q)\to H^2(G,\mathbb{Z}/q)$ corresponds to the qth Hilbert symbol $K^*/(K^*)^q\times K^*/(K^*)^q\to\mu_q$ denoted by (a,b) (see also [S2] Proposition 5), which we explain now:
To each $a\in K^*$ we associate an element $\chi_a\in H^1(G,\mathbb{Z}/q)$ by

$$g(\sqrt[q]{a})=\zeta_q^{\chi_a(g)}\sqrt[q]{a},\ g\in G.$$

This defines an injective homomorphism

$$\phi\colon K^*/(K^*)^q\to H^1(G,\mathbb{Z}/q), \tag{1.2.4}$$

and since $H^1(G,\mathbb{Z}/q)\cong H^1(G/G^{(1,q)},\mathbb{Z}/q)\cong H^1(\mathrm{Gal}(K(\sqrt[q]{K^*})/K),\mathbb{Z}/q)$, where $K(\sqrt[q]{K^*})$ is the maximal abelian extension of K of exponent q, Kummer theory tells us that ϕ is an isomorphism (see [N1] ch.V §3).
On the other hand, the reciprocity map of local class field theory gives an injective group homomorphism

$$\theta_K\colon K^*\to G^{\mathrm{ab}}.$$

The q-th Hilbert symbol of the field K is then given by the pairing

$$(\ ,\ )\colon K^*/(K^*)^q\times K^*/(K^*)^q\to\mu_q\ ,\ (a,b)=\phi(a)(\theta_K(b)).$$

It is a nondegenerate, anti-symmetric bilinear form and if K/k is a Galois extension, then the pairing is $\mathrm{Gal}(K/k)$-invariant, i.e.

$$(ga,gb)=(a,b)^g \text{ for } g\in\mathrm{Gal}(K/k).$$

We now consider the exact Kummer sequence

$$0\to\mathbb{Z}/q\xrightarrow{\lambda}K(2)^*\xrightarrow{q}K(2)^*\to 0,$$

where $\mathbb{Z}/q$ has been identified with the group μ_q of q-th roots of unity and the map q stands for raising to the q-th power. As $H^1(G, K(2)^*) = 0$ ([S3] §1 Prop. 1), by taking cohomology we get the exact sequence

$$0 \to H^2(G, \mathbb{Z}/q) \to H^2(G, K(2)^*) \xrightarrow{q} H^2(G, K(2)^*).$$

By local class field theory, we have

$$H^2(G, K(2)^*) = \mathbb{Q}_2 / \mathbb{Z}_2$$

(see [S3] §5 Prop. 20, Lemma 2). Hence by the above sequence we get an isomorphism

$$\psi\colon H^2(G, \mathbb{Z}/q) \longrightarrow \mathbb{Z}/q,$$

which coincides with the homomorphism φ in (1.2.1), since G is a pro-2 group.

Theorem 1.13. *([S2] Proposition 5)*
For all $a, b \in K^*$ we have

$$(a, b) = \psi(\chi_a \cup \chi_b).$$

1.3 Construction of a certain profinite group

The following construction will play a role in the description of the maximal extension without simple ramification as well as in the general case.
Let $\mathscr{G}$ be the profinite group with generators σ and τ and the defining relation

$$\sigma\tau\sigma^{-1} = \tau^{2^s}\ , \quad s \in \mathbb{N}\,.$$

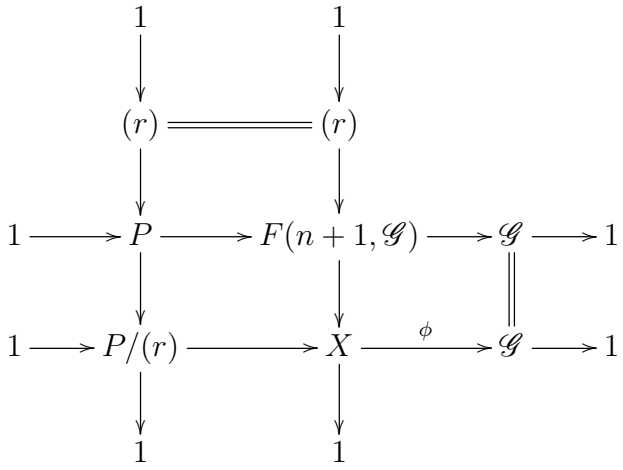
Let F_{n+1} be the free profinite group with basis $z_0, \ldots, z_n$. Then the kernel of the canonical projection from the free profinite product $\phi\colon F_{n+1} * \mathscr{G} \to \mathscr{G}$ is the normal subgroup $Z = (z_0, \ldots, z_n)$ ([N2], 1.2). Let I be the normal subgroup of Z such that Z/I is the maximal pro-2 factor group and set

$$F(n+1, \mathscr{G}) = (F_{n+1} * \mathscr{G})/I,$$
$$P = Z/I.$$

If $x_i = z_i \mod I$, $i = 0, \ldots, n$, then $F(n+1, \mathscr{G})$ is generated by $\sigma, \tau, x_0, \ldots, x_n$ and defined by the two properties, namely that σ and τ fulfill the relation of $\mathscr{G}$ and that the normal subgroup generated by $x_0, \ldots, x_n$ is a pro-2-group. We now define the group

$$X = X(\mathscr{G}, n) = F(n+1, \mathscr{G})/(r),$$

where (r) is the (closed) normal subgroup generated by some fixed r with $r \equiv 1 \mod P$. The map ϕ induces a surjection $X \to \mathscr{G}$ which we will also call ϕ. Therefore we have the commutative diagram



with exact rows and columns. Now let $\mathcal{H}$ be an open normal subgroup of $\mathscr{G}$, $U = U_{\mathcal{H}}$ the preimage of $\mathcal{H}$ in $F(n+1, \mathscr{G})$, $X_{\mathcal{H}} = \phi^{-1}(\mathcal{H})$ the preimage of $\mathcal{H}$ in X and $G = \mathscr{G}/\mathcal{H}$. The theorem for subgroups of free products ([B]) tells us that the preimage U' of $\mathcal{H}$ in $F_{n+1} * \mathscr{G}$ is isomorphic to

$$U' \cong (*_{\rho \in R} F_{n+1}^{\rho}) * \mathcal{H},$$

where R is a set of representatives for $\mathscr{G}/\mathcal{H}$. This is used in ([J]) to prove that $P/[P,U]$ is a free $\mathbb{Z}_2[G]$-module with basis $x_0[P,U], \ldots, x_n[P,U]$.

We will also need the following definition. The element $\pi \in \hat{\mathbb{Z}}$ with $\pi\hat{\mathbb{Z}} = \mathbb{Z}_2$ can be defined as follows: For every $m \in \mathbb{N}$ we choose $a_m, b_m \in \mathbb{Z}$ such that

$$1 = a_m 2^m + b_m p_1^m p_2^m \ldots p_m^m$$

where $\{p_1, p_2, \dots\}$ is the set of all odd prime numbers and set

$$\Delta(2) = \lim_{m\to\infty} a_m 2^m \in \hat{\mathbb{Z}},$$
$$\pi = \pi(2) = \lim_{m\to\infty} b_m p_1^m p_2^m \dots p_m^m \in \hat{\mathbb{Z}}.$$

Remark 1.14. (see [Z2])
A profinite group is a pro-2 group if and only if the equality $x^{\Delta(2)} = 1$ ($x^{\pi(2)} = x$) holds for every element in the group.

We recall that raising to a power with exponent in $\hat{\mathbb{Z}}$ is defined as follows in a profinite group H: Let $x \in H$ and $a = \lim a_n$ an element of $\hat{\mathbb{Z}}$ ($a_n \in \mathbb{Z}$). The sequence $x^{a_1}, x^{a_2}, \dots$ converges in H. Its limit, which does not depend on the choice of the sequence $a_1, a_2, \dots$ converging (in $\hat{Z}$) to a, will be denoted by x^a.

2 The maximal extension without simple ramification of a local field

Let k be a finite extension of $\mathbb{Q}_2$. In [Z2] Zelvenskii describes the maximal extension without simple ramification of the field k under the assumption that the maximal unramified extension of this field contains i, and in [Z1] the remaining case, e.g. that the extension $k(i)/k$ is totally ramified. We are interested in the latter one, where Zelvenskii proves everything only for fields k of odd degree over $\mathbb{Q}_2$ and claims that for fields of even degree it can be proven in an analogous manner. We expand Zelvenskiis very short explanations of the case of odd degree. In particular we provide the omitted proof for fields having even degree and one further property.

We give an outline of the content of this section. In subsection 2.3 we will define certain groups G_k by generators and relations. In order to show that these are isomorphic to certain subquotients of the Galois groups we are interested in, we want to use Lemma 2.16, which gives three conditions characterizing a group up to isomorphism. In the main part of this section we establish these three conditions for the groups G_k and their Galois counterparts. The desired result follows in subsection 2.4 by passage to an inverse limit.

For the remainder of this section, we use the following definitions and notations. Let G be a profinite group. $\tilde{G}$ will denote the 2-Sylow subgroup of G and for any $a, b \in G$ set $[a, b] = a^{-1}b^{-1}ab = a^{-1}a^b$.

Lemma 2.1. *Let G be a profinite group. Then for any $a, b, c \in G$ and any integer $k \in \mathbb{Z}$ one has the following congruences modulo $G^{(2,n)} = (G^n[G, G])^n[G^n[G, G], G]$:*

(i) $[a, bc] \equiv [a, b][a, c]$ *and* $[ab, c] \equiv [a, c][b, c]$,

(ii) $[a^k, b] \equiv [a, b^k] \equiv [a, b]^k$,

(iii) $(ab)^k \equiv a^k b^k [a, b]^{-k(k-1)/2}$.

Proof. See [De]. □

Let k be a 2-adic number field of degree m over $\mathbb{Q}_2$ such that $k(i)/k$ is ramified. We now divide such fields into three classes $\mathfrak{L}$, $\mathfrak{N}_\alpha$ and $\mathfrak{M}_\alpha$ with $\alpha \geq 2$ an integer. The class $\mathfrak{L}$ consists of all k of odd degree m. If m is even, let k' denote the intersection of k with the extension $\mathbb{Q}_{2^\infty}$ of $\mathbb{Q}_2$. As seen in the preliminaries, $\mathrm{Gal}(\mathbb{Q}_{2^\infty} / \mathbb{Q}_2)$ is isomorphic to U_2, the group of units of the ring of 2-adic integers $\mathbb{Z}_2$. We consider k to be in the class $\mathfrak{M}_\alpha$ (respectively, $\mathfrak{N}_\alpha$) if the Galois group $\mathrm{Gal}(\mathbb{Q}_{2^\infty} /k')$ is isomorphic to the subgroup $\{\pm 1\} \times (1 + 2^\alpha \mathbb{Z}_2) \subset U_2$ (respectively, to the closed subgroup of U_2 generated by the element $-1 + 2^\alpha$ (see Example (1.9)). Summarized we have

$$\begin{aligned} &m \text{ odd} && \Rightarrow k \in \mathfrak{L} \\ &m \text{ even, } \mathrm{Gal}(\mathbb{Q}_{2^\infty} /k') \cong \{\pm 1\} \times (1 + 2^\alpha \mathbb{Z}_2) && \Rightarrow k \in \mathfrak{M}_\alpha \\ &m \text{ even, } \mathrm{Gal}(\mathbb{Q}_{2^\infty} /k') \cong \langle -1 + 2^\alpha \rangle && \Rightarrow k \in \mathfrak{N}_\alpha \,. \end{aligned}$$

Remark 2.2. [De2]

1) The fields in the classes $\mathfrak{L}, \mathfrak{M}_\alpha, \mathfrak{N}_\alpha$ exhaust all fields whose maximal unramified extension does not contain i.

2) α has the following meaning: if $k \in \mathfrak{M}_\alpha$, then the field $k(i)$ contains a 2^αth root of unity but not a $2^{\alpha+1}$th root of unity; if $k \in \mathfrak{N}_\alpha$, then $k(i)$ contains a $2^{\alpha+1}$th root of unity but not a $2^{\alpha+2}$th root of unity.

3) A field k of even degree m belongs to the class $\mathfrak{M} = \bigcup_\alpha \mathfrak{M}_\alpha$, if k' is contained in the real subfield of $\mathbb{Q}_{2^\infty}$, otherwise k belongs to $\mathfrak{N} = \bigcup_\alpha \mathfrak{N}_\alpha$.

Throughout the remaining sections let q denote the largest power of 2 such that $K(i)$ contains a q-th root of unity and let $k(2)$ denote the maximal 2-extension of k.

2.1 Symplectic spaces

Let R be a commutative ring (with unit) and A an associative R-algebra.

Definition 2.3. *An involution anti-automorphism of A is a R-linear endomorphism $^*\colon A \to A$ satisfying the following conditions:*

$$1^* = 1 \ , \ (a^*)^* = a \text{ and } (ab)^* = b^*a^* \text{ for any } a, b \in A.$$

Moreover, if A is commutative the terms involution anti-automorphism and automorphism coincide.

Definition 2.4. *Let M be a (left) A-module, * an involution anti-automorphism on A and $\phi\colon M \times M \to R$ an R-bilinear form on M.*

i) ϕ is called A-invariant if for all $x, y \in M$ and $a \in A$

$$\phi(ax, y) = \phi(x, a^*y).$$

ii) ϕ defines an A-homomorphism

$$g_\phi\colon M \to Hom_R(M, R), \quad g_\phi(x)(y) = \phi(x, y),$$

where A acts on $Hom_R(M, R)$ by the rule $(af)(x) = f(a*x)$ for $x \in M$ and $a \in A$. We say ϕ is nondegenerate on the left if g_ϕ is an isomorphism. (The notion of nondegenerate on the right is defined in an analogous manner.)

Since for our purposes left- and right-nondegeneracy are equivalent, we will just say nondegenerate.

Definition 2.5. *A symplectic A-space is a pair (M, ϕ) consisting of an A-module M and a nondegenerate, antisymmetric A-invariant R-bilinear form ϕ on M.*

Remark 2.6. Two symplectic A-spaces (M, ϕ) and (N, ψ) are called isomorphic if there exists an A-isomorphism $\varphi\colon M \to N$ such that for every $x, y \in M$

$$\phi(x, y) = \psi(\varphi(x), \varphi(y)).$$

The case we are interested in is $A = \mathbb{Z}/q\,\mathbb{Z}[F](= \mathbb{Z}/q[F])$, where F is the product of a group of order two with generator ρ and a finite commutative group T of odd order $f > 1$. The map

$$*\colon F \to F, \quad \rho^\kappa\tau \mapsto (\rho^\kappa\tau)^* = c^\kappa\rho^\kappa\tau^{-1}$$

($\kappa = 0$ or 1, $\tau \in T$ and $c \in \mathbb{Z}/q$, $c^2 = 1$), extended by linearity to the group algebra $\mathbb{Z}/q[F]$, is an involution automorphism of this algebra.

Definition 2.7. *Let M be a $\mathbb{Z}/q[F]$-module and ϕ a $\mathbb{Z}/q$-bilinear form on M. Then ϕ is said to be F-invariant, if there exists a group homomorphism $\chi\colon F \to (\mathbb{Z}/q)^*$ such that for any $g \in F$ and $x, y \in M$ one has*

$$\phi(gx, gy) = \chi(g)\phi(x, y).$$

Remark 2.8. For the involution automorphism $^{(*)}\colon \mathbb{Z}/q[F] \to \mathbb{Z}/q[F]$ defined by

$$\left(\sum_{g\in F} a_g g\right)^{(*)} = \sum_{g\in F} a_g\chi(g)g^{-1},$$

the F-invariant forms coincide with the $\mathbb{Z}/q[F]$-invariant forms defined in (2.4 i)). For $\chi\colon F \to (\mathbb{Z}/q)^*$ defined by $\chi(\rho^\kappa\tau) = c^\kappa$ the involutions *, from above (2.7), and $^{(*)}$ coincide.

We identify the free $\mathbb{Z}/q[F]$-module of rank 1 with the additive group of the algebra $\mathbb{Z}/q[F]$ and assume that a bilinear, antisymmetric, nondegenerate and F-invariant form ϕ is given on it. In $\mathbb{Z}/q[F]$ we consider the subalgebra $\mathcal{A} = \mathcal{A}(F, q, c)$ generated by the idempotent $1 - e = 1 - f^{-1}\sum_{g\in T} g$. Then $\mathcal{A}$ is in a natural way a $\mathbb{Z}/q[F]$-module with automorphism $*$. Since the idempotents $1 - e = 1 - f^{-1}\sum_{g\in T} g$ and $e = f^{-1}\sum_{g\in T} g$ are symmetric ($e^* = e$, $(1 - e)^* = 1 - e$) and orthogonal, we have the decomposition $\mathbb{Z}/q[F] = \mathcal{A} \oplus e\,\mathbb{Z}/q[F]$ and $\mathcal{A}$ is a complete subspace of the symplectic space $\mathbb{Z}/q[F]$, where complete means, that the restriction of ϕ to $\mathcal{A}$ is nondegenerate.

Theorem 2.9. *([Z1] Theorem 1)*
On any free $\mathcal{A}$-module of finite rank there exists a symplectic $\mathbb{Z}/q[F]$-space structure, which is unique up to isomorphism.

2.2 The symplectic structure of $K(i)^*/(K(i)^*)^q$

Let K be an unramified extension of k having odd degree f, with $f \equiv 1 \mod 4$ if $k \in \mathfrak{L}$, $f \equiv 1 \mod 2^{2\alpha-1}$ if $k \in \mathfrak{M}_\alpha$ and $f \equiv 1 \mod 2^{2(\alpha+1)}$ if $k \in \mathfrak{N}_\alpha$ (just for technical reasons).

We write $F = \mathrm{Gal}(K(i)/k)$, which is a cyclic group of order $2f$ generated by an element ω. Since $K \cap k(i) = k$, K/k unramified and f odd, one has

$$\mathrm{Gal}(K(i)/k) = \mathrm{Gal}(K/k) \times \mathrm{Gal}(k(i)/k) = \mathbb{Z}/f\,\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z} = \mathbb{Z}/2f\,\mathbb{Z}\,.$$

Let $F_1 = \mathrm{Gal}(K(i)/K)$ denote the subgroup of F generated by ω^f. q is the largest power of 2 such that $K(i)$ contains a primitive q-th root ζ of unity, e.g. $q = 4$ if $k \in \mathfrak{L}$, $q = 2^\alpha$ if $k \in \mathfrak{M}_\alpha$ and $q = 2^{\alpha+1}$ if $k \in \mathfrak{N}_\alpha$. We let $(\ ,\ )$ denote the q-th Hilbert symbol on $K(i)^*/(K(i)^*)^q$, which makes $K(i)^*/(K(i)^*)^q$ into a symplectic space. Furthermore, let $S(\omega^2) = \sum_{\nu=0}^{f-1} \omega^{2\nu}$ and $\mathcal{O} = \mathcal{A}(F, q, c)$, where $c = -1$, if $k \in \mathcal{L}$ or $k \in \mathfrak{M}_\alpha$, and $c = -(1 + 2^\alpha) \in (\mathbb{Z}/2^{\alpha+1}\,\mathbb{Z})^*$ if $k \in \mathfrak{N}_\alpha$.

The following theorem has been proven by Zelvenskii just in the case $k \in \mathfrak{L}$. We also prove the remaining two cases.

Theorem 2.10. *The symplectic space $K(i)^*/(K(i)^*)^q$ splits into a direct sum of the full subspaces*

$$(K(i)^*/(K(i)^*)^q)^{1-S(\omega^2)} \text{ and } (K(i)^*/(K(i)^*)^q)^{S(\omega^2)}.$$

The $\mathbb{Z}/q[F]$-module $(K(i)^*/(K(i)^*)^q)^{1-S(\omega^2)}$ is isomorphic to a free $\mathcal{O}$-module of rank m. In the $\mathbb{Z}/q[F_1]$-module $(K(i)^*/(K(i)^*)^q)^{S(\omega^2)}$ we can choose $2m+2$ $\mathbb{Z}/q$-generators

a) $k \in \mathfrak{L}$: $\epsilon_1, \ldots, \epsilon_{2m+2}$ such that

$$(\epsilon_{2i-1}, \epsilon_{2i}) = (\epsilon_{2i}, \epsilon_{2i-1})^{-1} = \zeta^{-1} \quad \text{for } i = 1, 2, \ldots, m+1$$
$$(\epsilon_1, \epsilon_1) = -1$$
$$(\epsilon_{m+2}, \epsilon_{m+2}) = -1$$

and all other values of the Hilbert symbol on these generators are equal to $\zeta^0 = 1$.

b) $k \in \mathfrak{M}_\alpha$*:* $\epsilon_1, \ldots, \epsilon_{2m+2}$ *such that*

$$(\epsilon_{2i-1}, \epsilon_{2i}) = (\epsilon_{2i}, \epsilon_{2i-1})^{-1} = \zeta^{-1} \quad \textit{for } i = 1, 2, \ldots, m+1$$
$$(\epsilon_3, \epsilon_3) = -1$$
$$(\epsilon_{m+3}, \epsilon_{m+3}) = -1.$$

and all other values of the Hilbert symbol on these generators are equal to $\zeta^0 = 1$.

c) $k \in \mathfrak{N}_\alpha$*:* $\epsilon_1, \ldots, \epsilon_{2m+2}$ *such that*

$$(\epsilon_{2i-1}, \epsilon_{2i}) = (\epsilon_{2i}, \epsilon_{2i-1})^{-1} = \zeta^{-1} \quad \textit{for } i = 1, 2, \ldots, m+1$$
$$(\epsilon_1, \epsilon_1) = -1$$

and all other values of the Hilbert symbol on these generators are equal to $\zeta^0 = 1$.

Proof. Since the element $S(\omega^2)$ is idempotent, we have for $a, b \in K(i)^*$

$$(a^{S(\omega^2)}, b^{1-S(\omega^2)}) = (a, b^{(1-S(\omega^2))S(\omega^2)}) = (a, b^0) = (a, 1) = 1.$$

Hence $(K(i)^*/(K(i)^*)^q)^{1-S(\omega^2)}$ and $(K(i)^*/(K(i)^*)^q)^{S(\omega^2)}$ are orthogonal and thus full subspaces. For $(K(i)^*/(K(i)^*)^q)^{1-S(\omega^2)}$ being isomorphic to a free $\mathcal{O}$-module of rank m, see [Z1] Theorem 3.
By the choice of f, we have for $a, b \in k(i)^*$

$$(a, b)_{K(i)} = (N_{K(i)/k(i)}a, b)_{k(i)} = (a^f, b)_{k(i)} = (a, b)_{k(i)}^f = (a, b)_{k(i)},$$

(where $N_{K(i)/k(i)}$ is the usual field norm).
Since $\mathrm{Gal}(K(i)/k(i)) = \langle\omega^2\rangle$, it follows that $(K(i)^*)^{\langle\omega^2\rangle} = k(i)^*$. Because f is odd, we obtain

$$(K(i)^*/(K(i)^*)^q)^{\langle\omega^2\rangle}/(K(i)^*/(K(i)^*)^q)^{S(\omega^2)} = 0$$

and hence the equality

$$(K(i)^*/(K(i)^*)^q)^{S(\omega^2)} = k(i)^*/(k(i)^*)^q.$$

We now explain the structure of $(K(i)^*/(K(i)^*)^q)^{S(\omega^2)}$ for the three classes of fields $\mathfrak{L}$, $\mathfrak{M}_\alpha$ and $\mathfrak{N}_\alpha$:

a) Type $\mathfrak{L}$: Following Serre [S] and Labute [L], the Galois group of $k(2)/k$ is isomorphic to the pro-2 group with $m+2$ generators $x_1, \ldots, x_{m+2}$ and defining relation

$$r = x_1^2 x_2^4 [x_2, x_3] \ldots [x_{m+1}, x_{m+2}] = 1 \tag{2.2.1}$$

and the field $k(i)$ is the fixed field of the normal subgroup D of index 2 generated by the elements $x_1^2, x_2, \ldots, x_{m+2}$. The group D has $2m+2$ generators, connected by a single relation.

In D we have the relation (2.2.1) above and this relation conjugated by x_1

$$r^{x_1} = x_1^2 x_2^{4x_1} [x_2^{x_1}, x_3^{x_1}] \ldots [x_{m+1}^{x_1}, x_{m+2}^{x_1}] = 1.$$

Modulo $D^{(2,0)} = [[D,D],D]$ (and clearly also modulo $D^{(2,4)}$) we get by eliminating x_1^2 the relation

$$x_2^{4(-1+x_1)} \underbrace{[x_2^{x_1}, x_3^{x_1}] \ldots [x_{m+1}^{x_1}, x_{m+2}^{x_1}]}_{m+1 \text{ generators}} \underbrace{[x_2, x_3^{-1}] \ldots [x_{m+1}, x_{m+2}^{-1}]}_{m+1 \text{ generators}} \equiv 1.$$

Using the correspondence between the relation structure, the cup product and the Hilbert symbol explained in 1.2, we can choose a basis $\epsilon_1, \ldots, \epsilon_{2m+2}$ in $k(i)^*/(k(i)^*)^4$ which corresponds under the isomorphism ϕ (1.2.4) to

$$\epsilon_i \mapsto x_{i+1}^{x_1} \text{ for } 1 \le i \le m+1 \quad \text{and} \quad \epsilon_i \mapsto x_{i-m}^{(-1)^{i-m}} \text{ for } m+2 \le i \le 2m+2$$

such that (using the formula of Theorem 1.11)

$$\begin{aligned} (\epsilon_{2i-1}, \epsilon_{2i}) &= \zeta^{-1} \quad \text{for } i = 1, 2, \ldots, m+1 \\ (\epsilon_1, \epsilon_1) &= \zeta^{-\binom{4}{2}1} = \zeta^2 = -1 \quad \text{since } \zeta \text{ is a primitive 4th root of unity} \\ (\epsilon_{m+2}, \epsilon_{m+2}) &= \zeta^{-\binom{4}{2}(-1)} = \zeta^2 = -1 \end{aligned}$$

and all other values of the Hilbert symbol on these generators are equal to $\zeta^0 = 1$.

b) Type $\mathfrak{M}_\alpha$: In this case $k(2)/k$ has $m+2$ generators $x_1, \ldots, x_{m+2}$ and defining relation

$$r = x_1^2[x_1, x_2]x_3^{2^\alpha}[x_3, x_4]\ldots[x_{m+1}, x_{m+2}] = 1. \tag{2.2.2}$$

The subgroup D is the normal subgroup generated by $x_1, x_2^2, \ldots, x_{m+2}$. In D we have the relation (2.2.2) and this relation conjugated by x_2

$$\begin{aligned} r^{x_2} &= x_1^{2x_2}[x_1^{x_2}, x_2](x_3^{x_2})^{2^\alpha}[x_3^{x_2}, x_4^{x_2}]\ldots[x_{m+1}^{x_2}, x_{m+2}^{x_2}] = 1 \\ &= x_1^{x_2}x_1^{x_2^2}(x_3^{x_2})^{2^\alpha}[x_3^{x_2}, x_4^{x_2}]\ldots[x_{m+1}^{x_2}, x_{m+2}^{x_2}] \end{aligned}$$

Transforming equation (2.2.2) we get

$$x_1x_1^{x_2}x_3^{2^\alpha}[x_3, x_4]\ldots[x_{m+1}, x_{m+2}] = 1$$

and thus

$$x_1^{x_2} = x_1^{-1}x_3^{-2^\alpha}[x_3, x_4]^{-1}\ldots[x_{m+1}, x_{m+2}]^{-1}.$$

Inserting this into r^{x_2}, we obtain the following relation modulo $D^{(2,0)}$

$$\begin{aligned} &x_1^{-1}x_3^{-2^\alpha}x_1^{x_2^2}(x_3^{x_2})^{2^\alpha}[x_3^{x_2}, x_4^{x_2}]\ldots[x_{m+1}^{x_2}, x_{m+2}^{x_2}][x_3, x_4]^{-1}\ldots[x_{m+1}, x_{m+2}]^{-1} \\ \equiv &x_3^{2^\alpha(-1+x_2)}\underbrace{[x_1, x_2^2x_3^{2^\alpha}]}_{2 \text{ generators}}\underbrace{[x_3^{x_2}, x_4^{x_2}]\ldots[x_{m+1}^{x_2}, x_{m+2}^{x_2}]}_{m \text{ generators}}\underbrace{[x_3, x_4^{-1}]\ldots[x_{m+1}, x_{m+2}^{-1}]}_{m \text{ generators}}, \end{aligned}$$

since

$$\begin{aligned} x_1^{-1}x_3^{-2^\alpha}x_1^{x_2^2}(x_3^{x_2})^{2^\alpha} &\equiv x_3^{-2^\alpha}x_1^{-1}[x_1^{-1}, x_3^{-2^\alpha}]x_1^{x_2^2}(x_3^{x_2})^{2^\alpha} \\ &\equiv x_3^{-2^\alpha}[x_1, x_2^2][x_1, x_3^{2^\alpha}](x_3^{x_2})^{2^\alpha} \\ &\equiv x_3^{2^\alpha(-1+x_2)}[x_1, x_2^2x_3^{2^\alpha}]. \end{aligned}$$

Thus we can choose a basis $\epsilon_1, \ldots, \epsilon_{2m+2}$ in $k(i)^*/(k(i)^*)^{2^\alpha}$ which corresponds under the isomorphism ϕ (1.2.4) to

$$\epsilon_1 \mapsto x_1 \ , \ \epsilon_2 \mapsto x_2^2x_3^{2^\alpha}$$

$$\epsilon_i \mapsto x_i^{x_2} \text{ for } 3 \le i \le m+2 \quad \text{and} \quad \epsilon_i \mapsto x_{i-m}^{(-1)^{i+1-m}} \text{ for } m+3 \le i \le 2m+2$$

such that

$$\begin{aligned}(\epsilon_{2i-1},\epsilon_{2i}) &= \zeta^{-1} \quad \text{for } i=1,2,\dots,m+1\\ (\epsilon_3,\epsilon_3) &= \zeta^{-\binom{2^\alpha}{2}1} = \zeta^{2^{\alpha-1}} = -1 \quad \text{since } (\zeta^{2^{\alpha-1}})^2 = 1\\ (\epsilon_{m+3},\epsilon_{m+3}) &= \zeta^{\binom{2^\alpha}{2}1} = -1.\end{aligned}$$

and all other values of the Hilbert symbol on these generators are equal to $\zeta^0 = 1$.

c) Type $\mathfrak{N}_\alpha$: In this case $k(2)/k$ has $m+2$ generators $x_1,\dots,x_{m+2}$ and defining relation

$$r = x_1^{2+2^\alpha}[x_1,x_2]\dots[x_{m+1},x_{m+2}] = 1. \tag{2.2.3}$$

The subgroup D is the normal subgroup generated by $x_1, x_2^2, \dots, x_{m+2}$. In D we have the relation (2.2.3) and this relation conjugated by x_2

$$\begin{aligned}r^{x_2} =&(x_1^{2+2^\alpha})^{x_2}[x_1^{x_2},x_2]\dots[x_{m+1}^{x_2},x_{m+2}^{x_2}] = 1\\ =&(x_1^{x_2})^{1+2^\alpha}x_1^{x_2^2}[x_3^{x_2},x_4^{x_2}]\dots[x_{m+1}^{x_2},x_{m+2}^{x_2}.]\end{aligned}$$

Transforming equation (2.2.3), we get

$$x_1^{1+2^\alpha}x_1^{x_2}[x_3,x_4]\dots[x_{m+1},x_{m+2}] = 1$$

and thus

$$x_1^{x_2} = x_1^{-(1+2^\alpha)}[x_3,x_4]^{-1}\dots[x_{m+1},x_{m+2}]^{-1}.$$

Inserting this into r^{x_2}, we obtain the following relation modulo $D^{(2,0)}$

$$\begin{aligned}&(x_1^{-(1+2^\alpha)}[x_3,x_4]^{-1}\dots[x_{m+1},x_{m+2}]^{-1})^{1+2^\alpha}x_1^{x_2^2}[x_3^{x_2},x_4^{x_2}]\dots[x_{m+1}^{x_2},x_{m+2}^{x_2}]\\ \equiv&x_1^{-(1+2^\alpha)(1+2^\alpha)}x_1^{x_2^2}[x_3^{x_2},x_4^{x_2}]\dots[x_{m+1}^{x_2},x_{m+2}^{x_2}][x_3,x_4]^{-(1+2^\alpha)}\dots[x_{m+1},x_{m+2}]^{-(1+2^\alpha)}\\ \equiv&(x_1^{-(1+2^{\alpha-1})})^{2^{\alpha+1}}[x_1,x_2^2][x_3^{x_2},x_4^{x_2}]\dots[x_{m+1}^{x_2},x_{m+2}^{x_2}][x_3,x_4^{-(1+2^\alpha)}]\dots[x_{m+1},x_{m+2}^{-(1+2^\alpha)}.]\end{aligned}$$

The last equation holds since

$$\begin{aligned}x_1^{-(1+2^\alpha)(1+2^\alpha)}x_1^{x_2^2} &\equiv x_1^{-(2^{\alpha+1}+2^{2\alpha})}x_1^{-1}x_1^{x_2^2}\\ &\equiv x_1^{-(2^{\alpha+1}+2^{\alpha-1}2^{\alpha+1})}[x_1,x_2^2]\\ &\equiv (x_1^{-(1+2^{\alpha-1})})^{2^{\alpha+1}}[x_1,x_2^2].\end{aligned}$$

Since $-(1+2^{\alpha})$ and $-(1+2^{\alpha-1})$ are units in $\mathbb{Z}_2$ (and in $\mathbb{Z}/q$ $(-(1+2^{\alpha-1}))^4 = ((1+2^{\alpha-1})^2)^2 = (1+2^{\alpha}+2^{2\alpha-2})^2 = (1+2^{\alpha})^2 = 1+2^{\alpha+1}+2^{2\alpha} = 1$), we can choose $x_i^{-(1+2^{\alpha})}$ as generators. Setting $\overline{x_1} = x_1^k$ with $k = -(1+2^{\alpha-1})$, we finally have the relation

$$\overline{x_1}^{2^{\alpha+1}} \underbrace{[\overline{x_1}, x_2^{2k^{-1}}]}_{2 \text{ generators}} \underbrace{[x_3^{x_2}, x_4^{x_2}] \dots [x_{m+1}^{x_2}, x_{m+2}^{x_2}]}_{m \text{ generators}} \underbrace{[x_3, x_4^{-(1+2^{\alpha})}] \dots [x_{m+1}, x_{m+2}^{-(1+2^{\alpha})}]}_{m \text{ generators}} \equiv 1$$

with $2m+2$ generators.

Thus we can choose a basis $\epsilon_1, \dots, \epsilon_{2m+2}$ in $k(i)^*/(k(i)^*)^{2^{\alpha+1}}$ which corresponds under the isomorphism ϕ (1.2.4) to

$$\epsilon_1 \mapsto \overline{x_1}\ ,\ \epsilon_2 \mapsto x_2^{2k^{-1}}$$

$$\epsilon_i \mapsto x_i^{x_2} \text{ for } 3 \leq i \leq m+2 \quad \text{and} \quad \epsilon_i \mapsto x_{i-m}^{(-(1+2^{\alpha}))^{i+1-m}} \text{ for } m+3 \leq i \leq 2m+2$$

such that

$$(\epsilon_{2i-1}, \epsilon_{2i}) = \zeta^{-1} \quad \text{for } i = 1, 2, \dots, m+1$$
$$(\epsilon_1, \epsilon_1) = \zeta^{-\binom{2^{\alpha+1}}{2}1} = \zeta^{2^{\alpha}} = -1 \quad \text{since } (\zeta^{2^{\alpha}})^2 = 1.$$

and all other values of the Hilbert symbol on these generators are equal to $\zeta^0 = 1$.

□

2.3 The group G_k

Let G_k be the profinite group with $m+2$ generators and a single defining relation depending on the field k.

- If $k \in \mathfrak{L}$, then the generators of G_k are connected by the relation

$$x_1^2 x_2^4 [x_1, x_2] \dots [x_{m+1}, x_{m+2}] = 1$$

and the identical relation $x^{\Delta(2)} = 1$ on the normal subgroup B_k generated by the elements $x_1 x_2^2, x_2^f, x_3, \dots, x_{m+2}$.

- If $k \in \mathfrak{M}_\alpha$, then the generators are connected by the relation

$$x_1^2[x_1, x_2]x_3^{2^\alpha}[x_3, x_4] \dots [x_{m+1}, x_{m+2}] = 1$$

and the identical relation $x^{\Delta(2)} = 1$ on the normal subgroup B_k generated by the elements $x_1 x_3^{2^{\alpha-1}}, x_2, x_3^f, x_4, \dots, x_{m+2}$.

- If $k \in \mathfrak{N}_\alpha$, then the generators are connected by the relation

$$x_1^{2+2^\alpha}[x_1, x_2] \dots [x_{m+1}, x_{m+2}] = 1$$

and the identical relation $x^{\Delta(2)} = 1$ on the normal subgroup B_k generated by the elements $x_1, x_2, x_3^f, x_4, \dots, x_{m+2}$.

The next two theorems give a description of certain subgroups of G_k. Both theorems were proven by Zelvenskii with almost no explanations and only in the case $k \in \mathfrak{L}$. He also proved the second theorem for $k \in \mathfrak{N}_\alpha$, but the proof is incomprehensible and incomplete. We will explain the first case in more detail and prove the case $k \in \mathfrak{N}_\alpha$. Theorem 2.12 below claims that G_k has a subgroup isomorphic to $\mathrm{Gal}(K(2)/k(i))$. For the proof we will need Zelvenskiis description of the maximal extension without simple ramification of a 2-adic number field containing the fourth roots of unity (see [Z2]):

Theorem 2.11. *([Z2] Theorem 5)*
Let l be a finite extension of degree n of the field of 2-adic numbers and let q be the greatest power of 2 such that ς, a primitive qth root of unity, belongs to the maximal unramified extension of the field l. If $q \geq 4$, then n is even and the Galois group of the maximal extension without simple ramification of the field l is isomorphic to the profinite group with $n+2$ generators x and $y_0, \dots, y_n$ which are connected by the relation

$$x^{-1}y_0x = y_1^q[y_1, y_2] \dots [y_{n-1}, y_n]y_0$$

and by the identity relation $y^{\Delta(2)} = 1$ on the normal subgroup generated by the elements $y_0, \dots, y_n$.

Theorem 2.12. *The normal subgroup H_k of G_k generated by the elements $x_1^2, x_2, \ldots, x_{m+2}$ (if $k \in \mathfrak{L}$) and $x_1, x_2^2, x_3, \ldots, x_{m+2}$ (if $k \in \mathfrak{M}_\alpha$ or $\mathfrak{N}_\alpha$) is isomorphic to the group* $\mathrm{Gal}(K(2)/k(i))$.

Proof. We will show that H_k is generated by $2m+2$ generators $z_1, \ldots, z_{2m+2}$ subject to the single relation

$$z_1^q[z_1, z_2] \ldots [z_{2m+1}, z_{2m+2}] \equiv 1 \mod H_k^{(2,0)}.$$

$k \in \mathfrak{L}$**:** As shown in the proof of (2.10), we get a relation modulo $H_k^{(2,0)}$ of the form

$$x_2^{4(-1+x_1)}[x_2^{x_1}, x_3^{x_1}] \ldots [x_{m+1}^{x_1}, x_{m+2}^{x_1}][x_2, x_3^{-1}] \ldots [x_{m+1}, x_{m+2}^{-1}] \equiv 1,$$

which we can transform by using the following equivalences

$$\begin{aligned} x_2^{4(-1+x_1)}[x_2^{x_1}, x_3^{x_1}][x_2, x_3^{-1}] &\equiv (x_2^{(-1+x_1)})^4[x_2^{-1}, x_2^{x_1}]^{4(4-1)/2}[x_2^{-1+x_1}, x_3^{x_1}][x_2, x_3^{x_1}][x_2, x_3^{-1}] \\ &\equiv (x_2^{(-1+x_1)})^4[x_2, x_2^{x_1}]^{-6}[x_2^{-1+x_1}, x_3^{x_1}][x_2, x_3^{x_1-1}] \\ &\equiv (x_2^{(-1+x_1)})^4[x_2^{-1+x_1}, x_3^{x_1}][x_2, x_2^{-6x_1}x_3^{x_1-1}][x_2, x_2^6] \\ &\equiv (x_2^{(-1+x_1)})^4[x_2^{-1+x_1}, x_3^{x_1}][x_2, x_2^{6(1-x_1)}x_3^{x_1-1}]. \end{aligned}$$

Hence we get the relation

$$z_1^q[z_1, z_2] \ldots, [z_{2m+1}, z_{2m+2}] \equiv 1 \mod H_k^{(2,0)},$$

where

$$z_1 = x_2^{-1+x_1}\ , \quad z_2 = x_3^{x_1}\ , \quad z_3 = x_2\ , \quad z_4 = x_2^{6(1-x_1)}x_3^{x_1-1}$$

$$z_{4i-3} = x_{2i}x_1\ , \quad z_{4i-2} = x_{2i+1}^{x_1}$$

$$z_{4i-1} = x_{2i}\ , \quad z_{4i} = x_{2i+1}^{-1} \quad (i = 2, 3, \ldots, (m+1)/2).$$

Here $z_1, z_2, z_3^f, z_4, \ldots, z_{2m+2}$ belong to the normal subgroup $B_k \cap H_k$, because $z_1 = x_2^{-1+x_1} = (x_1x_2^2)^{-x_2^{-1}+x_2^2} \in B_k \cap H_k$ (all others are obvious). Now we are in the situation of 2.11 with $z_3 = x$ and the theorem is proven for $k \in \mathfrak{L}$.

$k \in \mathfrak{N}_\alpha$**:** Again from (2.10), we get a relation modulo $H_k^{(2,0)}$ of the form

$$\overline{x_1}^{2^{\alpha+1}}[\overline{x_1}, x_2^{2k^{-1}}][x_3^{x_2}, x_4^{x_2}] \dots [x_{m+1}^{x_2}, x_{m+2}^{x_2}][x_3, x_4^{-(1+2^\alpha)}] \dots [x_{m+1}, x_{m+2}^{-(1+2^\alpha)}] \equiv 1$$

which we can transform by using the following equivalence

$$\begin{aligned}[x_3^{x_2}, x_4^{x_2}][x_3, x_4^{-(1+2^\alpha)}] &\equiv [x_3^{x_2-1}, x_4^{x_2}][x_3, x_4^{x_2}][x_3, x_4^{-(1+2^\alpha)}] \\ &\equiv [x_3^{x_2-1}, x_4^{x_2}][x_3, x_4^{x_2-(1+2^\alpha)}].\end{aligned}$$

Hence we get the relation

$$z_1^q[z_1, z_2] \dots [z_{2m+1}, z_{2m+2}] \equiv 1 \mod H_k^{(2,0)},$$

where

$$z_1 = \overline{x_1}\ , \quad z_2 = x_2^{2k^{-1}}\ , \quad z_3 = x_3^{x_2-1}\ , \quad z_4 = x_4^{x_2}\ , \quad z_5 = x_3\ , \quad z_6 = x_4^{x_2-(1+2^\alpha)}$$

$$z_{4i-1} = x_{2i+1}^{x_2}\ , \quad z_{4i} = x_{2i+2}^{x_2}$$

$$z_{4i+1} = x_{2i+1}\ , \quad z_{4i+2} = x_{2i+2}^{-(1+2^\alpha)} \quad (i = 2, \dots, m/2).$$

Here $z_1, z_2, z_3, z_4, z_5^f, z_6, \dots, z_{2m+2}$ belong to $B_k \cap H_k$, which is generated as normal subgroup by $x_1, x_2^2, x_3^f, x_4, \dots, x_{m+2}$, because $H_k \ni x_3^{x_2-1} = z_3 = x_2^{-1}x_2^{x_3^{-1}} \in B_k$ (all others are obvious). Hence we can apply (2.11) again. □

Theorem 2.13. *The 2-Sylow subgroup $\tilde{G}_k$ of G_k is isomorphic to* $\mathrm{Gal}(K(2)/K)$.

Proof. Let $k \in \mathfrak{L}$: The group $\tilde{G}_k$ is generated as normal subgroup by the elements $x_1x_2^2, x_2^f, x_3, \dots, x_{m+2}$. We will use the following notation

$$\begin{aligned} y_i &= (x_1x_2^2)^{x_2^i} \quad 0 \le i \le f-1, \\ t_i &= [x_3, x_2]^{x_2^i} \quad 0 \le i \le f-2, \\ u_{i,j} &= x_j^{x_2^i} \quad 0 \le i \le f-1\ ,\ 4 \le j \le m+2, \\ M_i &= \prod_{j=2}^{(m+1)/2} [u_{i,2j}, u_{i,2j+1}]. \end{aligned}$$

Then the relations conjugated to the defining relation r of G_k using x_2^i are as follows:

$$y_i y_{i+2} t_i^{-1} M_i = 1 \quad 0 \le i \le f-3,$$

$$y_{f-2} x_2^{-f} y_0 x_2^f t_{f-2}^{-1} M_{f-2} = 1,$$

$$y_{f-1} x_2^{-f} y_1 x_2^f [x_2^f, x_3] \Big(\prod_{i=0}^{f-2} t_i\Big) M_{f-1} = 1.$$

Eliminating $y_1, \ldots, y_{f-1}$ from these relations, we obtain

$$y_0 \Big(\prod_{j=0}^{(f-5)/4} M_{4j+2}^{-1} t_{4j+2} \Big) x_2^{-f} \Big(\prod_{j=0}^{(f-5)/4} M_{4j+1}^{-1} t_{4j+1} \Big) x_2^{-f} y_0 x_2^f \Big(\prod_{j=0}^{(f-5)/4} M_{4j+3}^{-1} t_{4j+3} \Big)^{-1}$$

$$\times\, x_2^f [x_2^f, x_3] \Big(\prod_{i=0}^{f-2} t_i\Big) M_{f-1} \Big(\prod_{j=0}^{(f-5)/4} M_{4j}^{-1} t_{4j} \Big)^{-1} = 1. \tag{2.3.4}$$

The calculations above are explained in detail in the master thesis of D. Meier [M]. But only up to this point, then it got more complicated. For the proof we need the relation above in a special form, but neither Zelvenskii nor Meier explained how to obtain this special form from relation (2.3.4). We will show this now. For this let

$$u = y_0 \Big(\prod_{j=0}^{(f-5)/4} t_{4j+1} \Big) \Big(\prod_{j=0}^{(f-5)/4} t_{4j+2} \Big) x_2^{-2f},$$

$$v_i = \prod_{j=0}^{[i/4]} t_{4j+\lambda} \quad \text{for } 0 \le i \le f-2,\ \lambda = i - 4[i/4].$$

Next we look at equation 2.3.4 modulo $\tilde{G}_k^{(2,0)}$

$$
\begin{aligned}
& y_0\Big(\prod_{j=0}^{(f-5)/4} M_{4j+2}^{-1}t_{4j+2}\Big)x_2^{-f}\Big(\prod_{j=0}^{(f-5)/4} M_{4j+1}^{-1}t_{4j+1}\Big)x_2^{-f}y_0x_2^f\Big(\prod_{j=0}^{(f-5)/4} M_{4j+3}^{-1}t_{4j+3}\Big)^{-1}x_2^f[x_2^f,x_3] \\
& \times\Big(\prod_{i=0}^{f-2}t_i\Big)M_{f-1}\Big(\prod_{j=0}^{(f-5)/4} M_{4j}^{-1}t_{4j}\Big)^{-1} \\
\equiv & \underbrace{y_0\Big(\prod_{j=0}^{(f-5)/4} t_{4j+2}\Big)x_2^{-f}\Big(\prod_{j=0}^{(f-5)/4} t_{4j+1}\Big)x_2^{-f}y_0x_2^f\Big(\prod_{j=0}^{(f-5)/4} t_{4j+3}\Big)^{-1}x_2^f[x_2^f,x_3]\Big(\prod_{i=0}^{f-2}t_i\Big)\Big(\prod_{j=0}^{(f-5)/4} t_{4j}\Big)^{-1}}_{(2)} \\
& \times\underbrace{\Big(\prod_{j=0}^{(f-5)/4} M_{4j+2}^{-1}\prod_{j=0}^{(f-5)/4} M_{4j+1}^{-1}\prod_{j=0}^{(f-5)/4} M_{4j+3}M_{f-1}\prod_{j=0}^{(f-5)/4} M_{4j}\Big)}_{(1)} \mod \tilde{G}_k^{(2,0)}.
\end{aligned}
$$

and simplify the terms (1) and (2):

$$
\begin{aligned}
(1): & \prod_{j=0}^{(f-5)/4} M_{4j+2}^{-1}\prod_{j=0}^{(f-5)/4} M_{4j+1}^{-1}\prod_{j=0}^{(f-5)/4} M_{4j+3}M_{f-1}\prod_{j=0}^{(f-5)/4} M_{4j} \\
\equiv & M_2^{-1}M_6^{-1}M_{10}^{-1}\cdots M_{f-3}^{-1}\cdot M_1^{-1}M_5^{-1}\cdots M_{f-4}^{-1}\cdot M_3M_7\cdots M_{f-2}\cdot M_{f-1}\cdot M_0M_4\cdots M_{f-5} \\
\equiv & M_0\prod_{j=1}^{(f-1)/2}(M_{2j-1}M_{2j})^{(-1)^j} \mod \tilde{G}_k^{(2,0)}
\end{aligned}
$$

$$
\begin{aligned}
(2):\ & y_0\big(\prod_{j=0}^{(f-5)/4} t_{4j+2}\big)x_2^{-f}\big(\prod_{j=0}^{(f-5)/4} t_{4j+1}\big)x_2^{-f}y_0x_2^f\big(\prod_{j=0}^{(f-5)/4} t_{4j+3}\big)^{-1}x_2^f[x_2^f,x_3]\big(\prod_{i=0}^{f-2} t_i\big)\big(\prod_{j=0}^{(f-5)/4} t_{4j}\big)^{-1}\\
\equiv & y_0\big(\prod_{j=0}^{(f-5)/4} t_{4j+2}\prod_{j=0}^{(f-5)/4} t_{4j+1}\big)x_2^{-f}[x_2^{-f},\prod_{j=0}^{(f-5)/4} t_{4j+1}]x_2^{-f}y_0x_2^f\big(\prod_{j=0}^{(f-5)/4} t_{4j+3}\big)^{-1}x_2^f[x_2^f,x_3]\\
& \times\big(\prod_{i=0}^{f-2} t_i\big)\big(\prod_{j=0}^{(f-5)/4} t_{4j}\big)^{-1}\\
\equiv & \big(y_0\prod_{j=0}^{(f-5)/4} t_{4j+2}\prod_{j=0}^{(f-5)/4} t_{4j+1}x_2^{-2f}\big)^2x_2^{2f}\big(\prod_{j=0}^{(f-5)/4} t_{4j+1}\big)^{-1}\big(\prod_{j=0}^{(f-5)/4} t_{4j+2}\big)^{-1}x_2^{2f}\big(\prod_{j=0}^{(f-5)/4} t_{4j+3}\big)^{-1}\\
& \times[x_2^f,\prod_{j=0}^{(f-5)/4} t_{4j+3}][x_2^f,\big(\prod_{j=0}^{(f-5)/4} t_{4j+1}\big)^{-1}][x_2^f,x_3]\big(\prod_{i=0}^{f-2} t_i\big)\big(\prod_{j=0}^{(f-5)/4} t_{4j}\big)^{-1}\\
\equiv & u(x_2^f)^4[\big(\prod_{j=0}^{(f-5)/4} t_{4j+1}\big)^{-1}\big(\prod_{j=0}^{(f-5)/4} t_{4j+2}\big)^{-1},x_2^{2f}][x_2^f,x_3\prod_{j=0}^{(f-5)/4} t_{4j+3}\big(\prod_{j=0}^{(f-5)/4} t_{4j+1}\big)^{-1}]\\
& \times\big(\prod_{j=0}^{(f-5)/4} t_{4j+1}\big)^{-1}\big(\prod_{j=0}^{(f-5)/4} t_{4j+2}\big)^{-1}\big(\prod_{j=0}^{(f-5)/4} t_{4j+3}\big)^{-1}\big(\prod_{i=0}^{f-2} t_i\big)\big(\prod_{j=0}^{(f-5)/4} t_{4j}\big)^{-1}\\
\equiv & u(x_2^f)^4[x_2^f,x_3\big(\prod_{j=0}^{(f-5)/4} t_{4j+3}\big)\big(\prod_{j=0}^{(f-5)/4} t_{4j+1}\big)\big(\prod_{j=0}^{(f-5)/4} t_{4j+2}\big)^2]\big(\prod_{j=0}^{(f-5)/4} t_{4j+1}\big)^{-1}\big(\prod_{j=0}^{(f-5)/4} t_{4j+2}\big)^{-1}\\
& \times\big(\prod_{j=0}^{(f-5)/4} t_{4j+3}\big)^{-1}\big(\prod_{i=0}^{f-2} t_i\big)\big(\prod_{j=0}^{(f-5)/4} t_{4j}\big)^{-1}\\
\equiv & u(x_2^f)^4[x_2^f,x_3v_{f-2}v_{f-4}v_{f-3}^2]\underbrace{v_{f-4}^{-1}v_{f-3}^{-1}v_{f-2}^{-1}\underbrace{\big(\prod_{i=0}^{f-2} t_i\big)}_{(3)}v_{f-5}^{-1}}_{(4)}.
\end{aligned}
$$

Next we rewrite (3) and (4):

$$\begin{aligned}(3):\ \prod_{i=0}^{f-2} t_i &= [t_0, t_1t_2t_3]t_1t_2t_3t_0t_4\cdots t_{f-2}\\ &= [v_0, v_1v_2v_3][t_1, t_2t_3t_0t_4]t_2t_3t_0t_4t_1t_5\cdots t_{f-2}\\ &= [v_0, v_1v_2v_3][v_1, v_2v_3v_4][t_2, t_3t_0t_4t_1t_5]t_3t_0t_4t_1t_5t_2t_6\cdots t_{f-2}\\ &\vdots\\ &= \prod_{i=0}^{f-5}[v_i, v_{i+1}v_{i+2}v_{i+3}]v_{f-4}v_{f-3}v_{f-2}v_{f-5}\end{aligned}$$

$$\begin{aligned}(4):\ & v_{f-4}^{-1}v_{f-3}^{-1}v_{f-2}^{-1}(\prod_{i=0}^{f-2} t_i)v_{f-5}^{-1}\\ \equiv& v_{f-4}^{-1}v_{f-3}^{-1}v_{f-2}^{-1}\prod_{i=0}^{f-5}[v_i, v_{i+1}v_{i+2}v_{i+3}]v_{f-4}v_{f-3}v_{f-2}v_{f-5}v_{f-5}^{-1}\\ \equiv& v_{f-4}^{-1}v_{f-3}^{-1}v_{f-2}^{-1}v_{f-4}v_{f-3}v_{f-2}\prod_{i=0}^{f-5}[v_i, v_{i+1}v_{i+2}v_{i+3}]\\ \equiv& [v_{f-4}, v_{f-3}v_{f-2}]v_{f-3}^{-1}v_{f-2}^{-1}v_{f-3}v_{f-2}\prod_{i=0}^{f-5}[v_i, v_{i+1}v_{i+2}v_{i+3}]\\ \equiv& [v_{f-4}, v_{f-3}v_{f-2}][v_{f-3}, v_{f-2}]\prod_{i=0}^{f-5}[v_i, v_{i+1}v_{i+2}v_{i+3}] \mod \tilde{G}_k^{(2,0)}.\end{aligned}$$

Hence we finally find that $\tilde{G}_k$ is generated by the $mf+2$ elements u, x_2^f, x_3, v_i $(0 \le i \le f-2)$ and $u_{i,j}$ $(0 \le i \le f-1,\ 4 \le j \le m+2)$, which are connected by the single relation

$$u(x_2^f)^4[x_2^f, x_3v_{f-2}v_{f-4}v_{f-3}^2][v_{f-4}, v_{f-3}v_{f-2}][v_{f-3}, v_{f-2}]\prod_{i=0}^{f-5}[v_i, v_{i+1}v_{i+2}v_{i+3}]$$

$$\times M_0\prod_{j=1}^{(f-1)/2}(M_{2j-1}M_{2j})^{(-1)^j} \equiv 1 \mod \tilde{G}_k^{(2,0)}. \tag{2.3.5}$$

Using Demuškins algorithm [De] to transform the generators v_i $(0 \le i \le f-2)$, we see that the relation above cannot be replaced by an equivalent relation ($\mod \tilde{G}_k^{(2,0)}$),

which leaves out even one generator. Hence Remark (1.8) tells us that $\tilde{G}_k$ is a pro-2 Demuškin group with $n(\tilde{G}_k) = mf + 2$ and $\mathrm{Im}(\chi) = \pm 1 \times U_2^{(2)}$. The same holds for $\mathrm{Gal}(K(2)/K)$ (see (1.9)), which implies the theorem for $k \in \mathfrak{L}$.

Let $k \in \mathfrak{N}_\alpha$: First we will show, that $\tilde{G}_k$ is a pro-2 Demuškin group with the two invariants $n(\tilde{G}_k) = \dim H^1(\tilde{G}_k, \mathbb{F}_2) = mf + 2$ and $\mathrm{Im}(\chi) = \langle -1 + 2^\alpha \rangle$ (see the preliminaries (1.1)). By definition, $\tilde{G}_k$ is generated as normal subgroup by the elements $x_1, x_2, x_3^f, x_4, \ldots, x_{m+2}$. We introduce the following notation as in the setting of section (1.3):

let P be generated by $x_1, x_2, x_4, \ldots, x_{m+2}$ as normal subgroup of G_k, $\mathscr{G} = \langle x_3 \rangle$, $\mathcal{H} = \langle x_3^f \rangle$ and $G = \mathscr{G}/\mathcal{H}$ (x_3 plays the role of σ and $\tau = 1$).

Then P is a pro-2 group and

$$\begin{aligned} r &\equiv x_1^{2+2^\alpha} x_4^{-x_3} x_4 \mod [P, U] \qquad (\star) \\ &\equiv (x_1^{1+2^\alpha})^2 x_4^{-x_3} x_4 \mod [P, U], \end{aligned}$$

where U is the preimage of $\mathcal{H}$ in G_k.

Since the results from [J] apply in general, the statements in [JW] 2.4-2.7 are also true for $p = 2$, which proves that

$$\begin{aligned} \dim H^2(\tilde{G}_k, \mathbb{F}_2) &= 1, \\ \dim H^1(\tilde{G}_k, \mathbb{F}_2) &= (\mathscr{G} : \mathcal{H})m + 2 = fm + 2, \\ \mathrm{Tor}(\tilde{G}_k^{\mathrm{ab}}) &\cong \mathbb{Z}/2\mathbb{Z} \quad \text{as G-module.} \end{aligned}$$

Hence what is left to show is that the cup product $H^1(\tilde{G}_k, \mathbb{F}_2) \times H^1(\tilde{G}_k, \mathbb{F}_2) \to H^2(\tilde{G}_k, \mathbb{F}_2)$ is a nondegenerate bilinear form: in $\tilde{G}_k$ we have the relation r conjugated by x_3^i, $0 \leq i \leq f - 1$:

$$(x_1^{x_3^i})^{2+2^\alpha} [x_1^{x_3^i}, x_2^{x_3^i}][x_3, x_4^{x_3^i}][x_5^{x_3^i}, x_6^{x_3^i}] \ldots [x_{m+1}^{x_3^i}, x_{m+2}^{x_3^i}] = 1,$$

so in particular

$$[x_4^{x_3^i}, x_3] = [x_5^{x_3^i}, x_6^{x_3^i}] \ldots [x_{m+1}^{x_3^i}, x_{m+2}^{x_3^i}] (x_1^{x_3^i})^{2+2^\alpha} [x_1^{x_3^i}, x_2^{x_3^i}]. \tag{2.3.6}$$

Using

$$[x_3, x_4^{x_3^{f-1}}] = [x_3^f, x_4][x_4, x_3^{f-1}] = [x_3^f, x_4]\prod_{i=0}^{f-2}[x_4^{x_3^i}, x_3],$$

we can rewrite the relation $r^{x_3^{f-1}}$ to

$$\begin{aligned}&(x_1^{x_3^{f-1}})^{2+2^\alpha}[x_1^{x_3^{f-1}}, x_2^{x_3^{f-1}}][x_3, x_4^{x_3^{f-1}}][x_5^{x_3^{f-1}}, x_6^{x_3^{f-1}}]\dots[x_{m+1}^{x_3^{f-1}}, x_{m+2}^{x_3^{f-1}}]\\ =&(x_1^{x_3^{f-1}})^{2+2^\alpha}[x_1^{x_3^{f-1}}, x_2^{x_3^{f-1}}][x_3^f, x_4]\prod_{i=0}^{f-2}[x_4^{x_3^i}, x_3][x_5^{x_3^{f-1}}, x_6^{x_3^{f-1}}]\dots[x_{m+1}^{x_3^{f-1}}, x_{m+2}^{x_3^{f-1}}] = 1.\end{aligned}$$

Into this we now insert the equations (2.3.6) and obtain the following equivalence modulo $\tilde{G}_k^{(2,0)}$

$$\begin{aligned}&(x_1^{x_3^{f-1}})^{2+2^\alpha}[x_1^{x_3^{f-1}}, x_2^{x_3^{f-1}}]\prod_{i=0}^{f-2}(x_1^{x_3^i})^{2+2^\alpha}[x_1^{x_3^i}, x_2^{x_3^i}][x_3^f, x_4]\\ &\times\prod_{i=0}^{f-1}[x_5^{x_3^i}, x_6^{x_3^i}]\dots[x_{m+1}^{x_3^i}, x_{m+2}^{x_3^i}] \equiv 1 \mod \tilde{G}_k^{(2,0)}.\end{aligned} \tag{2.3.7}$$

For abbreviation, we define

$$\begin{aligned}y_i &= \prod_{\nu=0}^{i} x_1^{x_3^\nu} \text{ for } 0 \le i \le f-1\\ z_i &= x_2^{x_3^i} \text{ for } 0 \le i \le f-1\\ u_{i,\nu} &= x_\nu^{x_3^i} \text{ for } 0 \le i \le f-1 \text{ and } 5 \le \nu \le m+2.\end{aligned}$$

Furthermore, we have the following equivalences (using Lemma 2.1)

- $$\begin{aligned}(x_1^{x_3^{f-1}})^{2+2^\alpha}\prod_{i=0}^{f-2}(x_1^{x_3^i})^{2+2^\alpha} &\equiv \prod_{i=0}^{f-1}(x_1^{x_3^i})^{2+2^\alpha}[(x_1^{x_3^{f-1}})^{2+2^\alpha}, y_{f-2}^{2+2^\alpha}]\\ &\equiv \prod_{i=0}^{f-1}(x_1^{x_3^i})^{2+2^\alpha}[y_{f-2}, y_{f-1}]^{-(2+2^\alpha)^2} \mod \tilde{G}_k^{(2,0)},\end{aligned}$$

- $$\begin{aligned}\prod_{i=0}^{f-1}(x_1^{x_3^i})^{2+2^\alpha} &\equiv (y_{f-1})^{2+2^\alpha}[y_0, x_1^{x_3}]^{(1+2^{\alpha-1})(1+2^\alpha)}\\ &\quad\times[y_1, x_1^{x_3^2}]^{(1+2^{\alpha-1})(1+2^\alpha)}\dots[y_{f-2}, x_1^{x_3^{f-1}}]^{(1+2^{\alpha-1})(1+2^\alpha)}\\ &\equiv (y_{f-1})^{2+2^\alpha}\prod_{i=0}^{f-2}[y_i, y_{i+1}^{(1+2^{\alpha-1})(1+2^\alpha)}] \mod \tilde{G}_k^{(2,0)},\end{aligned}$$

- $\prod_{i=0}^{f-1}[x_1^{x_3^i}, x_2^{x_3^i}] \equiv [x_1,x_2]\prod_{i=1}^{f-1}[y_i,z_i][y_{i-1},z_i^{-1}] \equiv \prod_{i=0}^{f-2}[y_i, z_{i+1}^{-1}z_i][y_{f-1},z_{f-1}] \mod \tilde{G}_k^{(2,0)}$,

which we use to transform equation (2.3.7). We obtain

$$(y_{f-1})^{2+2^\alpha}[y_{f-1},z_{f-1}][x_3^f,x_4]\Big(\prod_{i=0}^{f-3}[y_i, z_{i+1}^{-1}z_i y_{i+1}^{(1+2^{\alpha-1})(1+2^\alpha)}]\Big)$$

$$\times [y_{f-2}, z_{f-1}^{-1}z_{f-2}y_{f-1}^{(1+2^{\alpha-1})(1+2^\alpha)-(2+2^\alpha)^2}]\prod_{i=0}^{f-1}\Big(\prod_{\nu=3}^{(m+2)/2}[u_{i,2\nu-1},u_{i,2\nu}]\Big) \equiv 1 \mod \tilde{G}_k^{(2,0)}. \tag{2.3.8}$$

Hence the $fm+2$ elements y_i $(0 \le i \le f-1)$, z_{f-1}, $z_{i+1}^{-1}z_i$ $(0 \le i \le f-2)$, x_3^f, x_4, $u_{i,\nu}$ $(0 \le i \le f-1\ ,\ 5 \le \nu \le m+2)$ form a minimal system of generators of $\tilde{G}_k$ and are connected by the single relation above.

Let $\eta_1, \ldots, \eta_{m+2}$ denote the corresponding dual basis of $H^1(\tilde{G}_k, \mathbb{F}_2)$. If we now look at the relation (2.3.8) modulo $\tilde{G}_k^{(2,2)}$, then Corollary 1.12 tells us that

$$\rho\eta_i \cup \rho\eta_{i+1} = -\xi, \quad i = 1, \ldots, m+2$$
$$\eta_1 \cup \eta_1 = -\xi,$$

and all other values of the cup product on these generators are zero (ξ is a generator of $H^2(\tilde{G}_k, \mathbb{F}_2)$). Hence the cup product for $\tilde{G}_k$ is nondegenerate. Thus $\tilde{G}_k$ is a Demuškin group with $n = n(\tilde{G}_k) = mf+2$ even and $q' = q'(\tilde{G}_k) = 2$, since $\mathbb{Z}/2\mathbb{Z} \cong \mathrm{Tor}(\tilde{G}_k^{\mathrm{ab}}) \cong \mathrm{Tor}((\mathbb{Z}_2)^{n-1} \times (\mathbb{Z}_2/q'\mathbb{Z})) = \mathbb{Z}_2/q'\mathbb{Z}$.

We still have to calculate the invariant $\mathrm{Im}(\chi)$ of $\tilde{G}_k$. It is equal to $\langle -1+2^\alpha \rangle$: we define a continuous homomorphism $\chi\colon F \to U_2$, where F is the free pro-2 group with basis y_i $(0 \le i \le f-1)$, z_{f-1}, $z_{i+1}^{-1}z_i$ $(0 \le i \le f-2)$, x_3^f, x_4, $u_{i,\nu}$ $(0 \le i \le f-1\ ,\ 5 \le \nu \le m+2)$, by

$$\chi(z_{f-1}) = (-1-2^\alpha)^{-1}, \quad \text{and } \chi \text{ of any other element of the basis is equal to 1.}$$

Then $\chi(r) = 0$ and χ induces a continuous homomorphism $\chi\colon \tilde{G}_k \to U_2$.

To show the surjectivity of $H^1(\tilde{G}_k, I_j(\chi)) \to H^1(\tilde{G}_k, I_1(\chi))$ for all $j \ge 1$, let $\tilde{G}_k \to I_1(\chi)$

be a cocycle. Since F is free, we can lift the homomorphism $F \to \tilde{G}_k \to I_1(\chi)$ to a cocycle $D\colon F \to I_j(\chi)$ for $j \geq 1$. Using the formula

$$D([x,y]) = x^{-1}y^{-1}(D(x) - yD(x) + xD(y) - D(y)),$$

we find

$$D(r) = (2^\alpha + \chi(z_{f-1})^{-1} + 1)D(y_{f-1}) = 0.$$

It follows that D induces a derivation of $\tilde{G}_k$ into $I_j(\chi)$ for $j \geq 1$ and because χ is unique, we obtain the invariant $\mathrm{Im}(\chi) = \langle -1 + 2^\alpha \rangle$.
But $\mathrm{Gal}(K(2)/K)$ also is a pro-2 Demuškin group with invariants $n(\mathrm{Gal}(K(2)/K)) = [K : \mathbb{Q}_2] + 2 = mf + 2$, $q' = 2$ (since K does not contain the 4th roots of unity) and $\mathrm{Im}(\chi) = \langle -1 + 2^\alpha \rangle$ (see Example 1.9).
The theorem now follows from the fact that two Demuškin groups with the same invariants n and $\mathrm{Im}(\chi)$ are isomorphic (Theorem 1.6). □

For the next lemma, we have to define a symplectic $\mathbb{Z}/q[F]$-space structure on $A_k = \tilde{H}_k/\tilde{H}_k^{(1,q)}$. The 2-Sylow subgroup $\tilde{H}_k = \tilde{G}_k \cap H_k$ is a normal subgroup of index 2 in $\tilde{G}_k$ and isomorphic to $\mathrm{Gal}(K(2)/K(i))$ (see Theorem 2.13).

Lemma 2.14. *The maps*

$$\omega \mapsto x_1 x_2^{(f+5)/2} \tilde{H}_k \quad \textit{for } k \in \mathfrak{L}$$

and

$$\omega \mapsto x_2 x_3^{(f+1)/2} \tilde{H}_k \quad \textit{for } k \in \mathfrak{M}_\alpha \ \textit{ or } \ \mathfrak{N}_\alpha$$

give isomorphisms from F to $G_k/\tilde{H}_k$.

Proof. $G_k/\tilde{H}_k$ has order $2f$ and since f is odd we have

$$\mathbb{Z}/2f = \mathbb{Z}/2 \times \mathbb{Z}/f = \mathrm{Gal}(K(i)/K) \times \mathrm{Gal}(K(i)/k(i)) = \tilde{G}_k/\tilde{H}_k \times H_k/\tilde{H}_k = G_k/\tilde{H}_k.$$

Thus $G_k/\tilde{H}_k$ is cyclic of order $2f$ and

- has $x_1 x_2^{(f+5)/2} \tilde{H}_k$ as generator if $k \in \mathfrak{L}$: clearly $G_k/\tilde{H}_k$ is generated by x_1, x_2 mod $\tilde{H}_k$ and

$$(x_1 x_2^{(f+5)/2})^2 \equiv x_1^2 x_2^{f+5} \equiv x_2 \mod \tilde{H}_k,$$

$$\begin{aligned}(x_1 x_2^{(f+5)/2})^{f-4} &\equiv x_1 x_2^{(f+5)/2} ((x_1 x_2^{(f+5)/2})^2)^{(f-5)/2} \\ &\equiv x_1 x_2^{(f+5)/2} x_2^{(f-5)/2} \equiv x_1 \mod \tilde{H}_k\end{aligned}$$

since $x_2^f \in \tilde{H}_k$ and $1 \equiv r \equiv x_1^2 x_2^4 \mod \tilde{H}_k$.

- has $x_2 x_3^{(f+1)/2} \tilde{H}_k$ as generator if $k \in \mathfrak{N}_\alpha$: in this case $G_k/\tilde{H}_k$ is generated by x_2, x_3 mod $\tilde{H}_k$ and

$$(x_2 x_3^{(f+1)/2})^2 \equiv x_2^2 x_3^{f+1} \equiv x_3 \mod \tilde{H}_k,$$

$$\begin{aligned}(x_2 x_3^{(f+1)/2})^f &\equiv ((x_2 x_3^{(f+1)/2})(((x_2 x_3^{(f+1)/2})^2)^{(f-1)/2} \\ &\equiv x_2 x_3^{(f+1)/2} x_3^{(f-1)/2} \equiv x_2 \mod \tilde{H}_k\end{aligned}$$

since $x_2^2, x_3^f \in \tilde{H}_k$.

- has $x_2 x_3^{(f+1)/2} \tilde{H}_k$ as generator if $k \in \mathfrak{M}_\alpha$: in this case $G_k/\tilde{H}_k$ is generated by $x_1, x_2, x_3 \mod \tilde{H}_k$ and

$$x_3^{f-q/2} \equiv x_1 \quad \text{since} \quad x_1 x_3^{q/2} \in \tilde{G}_k \cap H_k = \tilde{H}_k$$

(x_2, x_3 are analogous to the case $k \in \mathfrak{N}_\alpha$). □

In addition, $G_k/\tilde{H}_k$ is via conjugation a group of operators for the abelian group $A_k = \tilde{H}_k/\tilde{H}_k^{(1,q)}$. Hence we can consider A_k as an F-module. Since $\tilde{H}_k \cong \mathrm{Gal}(K(2)/K(i))$, we can choose generators $\overline{h}_1, \ldots, \overline{h}_{2mf+2}$ in $\overline{H}_k = \tilde{H}_k/\tilde{H}_k^{(2,q)}$ (where $\overline{h}_v$ is the image of $h_v \in \tilde{H}_k$ in $\overline{H}_k$) in such a way that they are connected by the single relation (see [De])

$$\overline{h}_1^q [\overline{h}_1, \overline{h}_2] \ldots [\overline{h}_{2mf+1}, \overline{h}_{2mf+2}] = 1. \tag{2.3.9}$$

Then Theorem 1.11 tells us that if $\chi_1, \ldots, \chi_{2mf+2} \in H^1(\tilde{H}_k, \mathbb{Z}/q) = H^1(A_k, \mathbb{Z}/q)$ denotes a dual basis of $\overline{h}_1, \ldots, \overline{h}_{2mf+2}$, the cup product induces an antisymmetric, nondegenerate and F-invariant bilinear form $\langle\ ,\ \rangle\colon H^1(A_k, \mathbb{Z}/q) \times H^1(A_k, \mathbb{Z}/q) \to \mu_q$ with

$$\langle \chi_1, \chi_1 \rangle = \eta^{q/2} \quad , \quad \langle \chi_{2v-1}, \chi_{2v} \rangle = \langle \chi_{2v}, \chi_{2v-1} \rangle^{-1} = \eta$$

$(1 \leq v \leq mf+1)$, where η is a generator of μ_q and all other values of the form $\langle \ldots, \ldots \rangle$ on the basis elements $\chi_1, \ldots, \chi_{2mf+2}$ are equal to 1. Let $\tilde{h}_v$ be the image of h_v in A_k, then we can define a bilinear form on A_k by $(\tilde{h}_i, \tilde{h}_j) = \langle \chi_i, \chi_j \rangle$ for $0 \leq i, j \leq 2mf+2$. Thus A_k is a symplectic $\mathbb{Z}/q[F]$-space.

Lemma 2.15. *The symplectic $\mathbb{Z}/q[F]$-spaces $\tilde{H}_k/\tilde{H}_k^{(1,q)}$ and $K(i)^*/(K(i)^*)^q$ are isomorphic.*

Proof. If $k \in \mathfrak{L}$ see [Z1] Lemma 9. The other two cases are omitted in [Z1].
Let $k \in \mathfrak{N}_\alpha$. We described in Theorem 2.10 the symplectic structure of $K(i)^*/(K(i)^*)^q$ and showed that it splits into a direct product of two full subspaces. We show that A_k splits in the same way.
$\tilde{H}_k = \tilde{G}_k \cap H_k$ is generated as normal subgroup by the elements $x_1, x_2^2, x_3^f, x_4, \ldots, x_{m+2}$. Let $\tilde{z}$ denote the image of $z \in \tilde{H}_k$ in A_k. Recall that the group $\tilde{G}_k$ is generated by the elements $y_i = \prod_{j=0}^{i} x_1^{x_3^j}$, $x_2^{x_3^{f-1}}$, x_3^f, $[x_3, x_2]^{x_3^\nu}$, x_4, $u_{i,k} = x_k^{x_3^i}$ for $0 \leq i \leq f-1$, $0 \leq \nu \leq f-2$ and $5 \leq k \leq m+2$, where $(x_2^2)^{x_3^{f-1}}$ as well as all other generators lie in $\tilde{H}_k$. The group H_k has $2m+2$ generators $z_1', \ldots, z_4', x_3, z_6', \ldots, z_{2m+2}'$ with $z_i', x_3^f \in \tilde{G}_k$.
We split A_k into a direct product of the two modules $A_k' = A_k^{1-S(\omega^2)}$ and $A_k'' = A_k^{S(\omega^2)}$. Under the isomorphism in Lemma 2.14, ω^2 corresponds to the element x_3 in $G_k/\tilde{H}_k$, so the elements $\widetilde{[x_3, x_2]}^{1-S(\omega^2)}, \widetilde{[x_4, x_3]}, \tilde{x_5}^{1-S(\omega^2)}, \ldots, \tilde{x}_{m+2}^{1-S(\omega^2)}$ form a $\mathbb{Z}/q[F]$-basis of A_k', because of the following:

- Since $\widetilde{[x_2^2, x_3]}$ and $\tilde{x_2^2}$ commute, and $(\tilde{x_2^2})^{f-1} = 1$ ($f \equiv 1 \mod 2^{2(\alpha+1)}$) and $x_2^{x_3} =$

$x_2^2[x_2^2, x_3]$ we get

$$(\tilde{x_2^2})^{-1+S(\omega^2)} = (\tilde{x_2^2})^{-1}\tilde{x_2^2}\prod_{i=1}^{f-1}\tilde{x_2^2}\prod_{j=1}^{i}\widetilde{[x_2^2, x_3]}^{x_3^{j-1}} = (\tilde{x_2^2})^{f-1}\prod_{i=1}^{f-1}\prod_{j=1}^{i}\widetilde{[x_2^2, x_3]}^{x_3^{j-1}}$$
$$= \prod_{i=1}^{f-1}\prod_{j=1}^{i}\widetilde{[x_2^2, x_3]}^{x_3^{j-1}},$$

and therefore $((\tilde{x_2^2})^{x_3^{f-1}})^{1-S(\omega^2)}$ lies in the submodule spanned by $\widetilde{[x_3, x_2]}$ as $\widetilde{[x_3, x_2^2]} = \widetilde{[x_3, x_2]}\widetilde{[x_3, x_2]}^{x_2}$.

- Analogously to the first point we can show that $x_4^{1-S(\omega^2)}$ lies in the submodule spanned by $\widetilde{[x_4, x_3]}$. Furthermore, we have

$$\widetilde{[x_4, x_3]}^{-1+S(\omega^2)} = \widetilde{[x_4, x_3]}^{-1}\prod_{i=0}^{f-1}\widetilde{[x_4, x_3]}^{x_3^i} = \widetilde{[x_4, x_3]}^{-1}[\tilde{x_4}, \tilde{x_3^f}] = \widetilde{[x_3, x_4]}.$$

- $(\tilde{x_3^f})^{1-S(\omega^2)} = \tilde{x_3^f}(\tilde{x_3^f})^f = \tilde{x_3^f}$.

- $\widetilde{y_{f-1}}^{1-S(\omega^2)} = (\tilde{x_1}^{S(\omega^2)})^{1-S(\omega^2)} = 1$ and hence $\tilde{y_i}^{1-S(\omega^2)} = 1$ for all $0 \leq i \leq f-1$, since $\tilde{y_i}\tilde{y_i}^{-x_3^i} = \tilde{y_{i-1}}$, and $\tilde{y_j}^{x_3^l}$ and $\tilde{y_j}^{x_3^k}$ commute for all $j, l, k = 0, \ldots, f-1$.

Thus A_k' is a free $\mathcal{O}$-module of rank m ($\mathcal{O}$ is the subalgebra of $\mathbb{Z}/q[F]$ generated by $1 - S(\omega^2)$) and by Theorem 2.9 the symplectic spaces A_k' and $K(i)^*/((K(i)^*)^q)^{1-S(\omega^2)}$ are isomorphic.

The $\mathbb{Z}/q[F_1]$-module A_k'' is generated by the elements

$$\tilde{y_0}, \tilde{x_3^f}, \widetilde{[x_3, x_2]}^{S(\omega^2)}, \tilde{x_5}^{S(\omega^2)}, \ldots, \widetilde{x_{m+2}}^{S(\omega^2)}.$$

Let P_k be the subgroup of $\tilde{H}_k$ spanned by the elements

$$\widetilde{[x_3, x_2]}^{1-\sum_{i=0}^{f-1} x_3^i} \quad , \quad \widetilde{[x_4, x_3]} \quad , \quad u_{0,k}^{1-\sum_{i=0}^{f-1} x_3^i} \quad (5 \leq k \leq m+2)$$

and their conjugates with x_2 and x_3. We now define a symplectic structure on the module A_k' the same way as on A_k explained before this theorem. Since

$$A_k^{S(\omega^2)} = (\tilde{H}_k/\tilde{H}_k^{(1,q)})/(P_k/P_k \cap \tilde{H}_k^{(1,q)}) = \tilde{H}_k/(\tilde{H}_k^{(1,q)}P_k) = (\tilde{H}_k/P_k)/(\tilde{H}_k/P_k)^{(1,q)})$$

and

$$\tilde{H}_k^{(2,q)}[\tilde{H}_k, P_k] \twoheadrightarrow \tilde{H}_k^{(2,q)} P_k$$

$$\tilde{H}_k/\tilde{H}_k^{(2,q)} P_k = (\tilde{H}_k/P_k)/(\tilde{H}_k/P_k)^{(2,q)}),$$

we have to look at the relation imposed on the generators of $\tilde{H}_k$, but we must only write out the necessary relation modulo $\tilde{H}_k^{(2,2^{\alpha+1})}[\tilde{H}_k, P_k]$. We start as in the proof of 2.12 and get the relation (using that $[x_3, x_4] \in P_k$)

$$\begin{aligned}
&(x_1^{-(1+2^\alpha)}[x_3,x_4]^{-1}\dots[x_{m+1},x_{m+2}]^{-1})^{1+2^\alpha} x_1^{x_2^2}[x_3^{x_2},x_4^{x_2}]\dots[x_{m+1}^{x_2},x_{m+2}^{x_2}]\\
\equiv& x_1^{-(1+2^\alpha)(1+2^\alpha)} x_1^{x_2^2}[x_3,x_4]^{-(1+2^\alpha)}[x_3^{x_2},x_4^{x_2}][x_5,x_6]^{x_2-(1+2^\alpha)}\dots[x_{m+1},x_{m+2}]^{x_2-(1+2^\alpha)}\\
\equiv&(x_1^{-(1+2^{\alpha-1})})^{2^{\alpha+1}}[x_1,x_2^2][x_3,x_4]^{-(1+2^\alpha)}[x_3^{x_2},x_4^{x_2}]\\
&\times[x_5,x_6]^{x_2-(1+2^\alpha)}\dots[x_{m+1},x_{m+2}]^{x_2-(1+2^\alpha)} \mod \tilde{H}_k^{(2,2^{\alpha+1})}[\tilde{H}_k,P_k].
\end{aligned}$$

We now have to conjugate this relation with x_3^i for $0 \le i \le f-1$ and follow the methods used in the proof of 2.10. We obtain the relation

$$\begin{aligned}
&(x_1^{x_3^{f-1}})^{-(1+2^{\alpha-1})2^{\alpha+1}}[x_1,x_2^2]^{x_3^{f-1}}[x_3^f,x_4]^{-(1+2^\alpha)}[(x_3^f)^{x_2},x_4^{x_2}]\prod_{i=0}^{f-2}([x_3,x_4]^{-x_3^i(1+2^\alpha)}[x_3^{x_2},x_4^{x_2}]^{x_3^i})\\
&\times\prod_{i=0}^{f-1}\prod_{j=3}^{(m+2)/2}([x_{2j-1},x_{2j}]^{x_3^i})^{x_2-(1+2^\alpha)}\\
\equiv& y_{f-1}^{-(1+2^{\alpha-1})2^{\alpha+1}}[y_{f-1},z_{f-1}][x_3^f,x_4^{-(1+2^\alpha)}][(x_3^f)^{x_2},x_4^{x_2}]\prod_{i=0}^{f-2}\underbrace{[y_i,z_{i+1}^{-1}z_i y_{i+1}^{2^\alpha}]}_{(1)}\\
&\times\prod_{j=3}^{(m+2)/2}\underbrace{\prod_{i=0}^{f-1}([x_{2j-1},x_{2j}]^{x_3^i})^{x_2-(1+2^\alpha)}}_{(2)} \mod \tilde{H}_k^{(2,2^{\alpha+1})}[\tilde{H}_k,P_k],
\end{aligned}$$

where $z_i = x_2^{x_3^i}$ for $0 \le i \le f-1$. We can simplify terms (1) and (2):
(1) : these terms are $\equiv 1 \mod \tilde{H}_k^{(2,2^{\alpha+1})}[\tilde{H}_k, P_k]$, because

$$(z_{i+1}^{-1}z_i)^{-1+\sum_{i=0}^{f-1}x_3^i} = (z_{i+1}^{-1}z_i)^{-1}\prod_{i=0}^{f-1}[x_3,x_2^2]^{x_3^i} = (z_{i+1}^{-1}z_i)^{-1}[x_3^f,x_2^2]$$

and hence

$$\begin{aligned}
[y_i, z_{i+1}^{-1} z_i y_{i+1}^{2^\alpha}] &\equiv [y_i, y_{i+1}]^{2^\alpha} \equiv [y_i^{\sum_{i=0}^{f-1} x_3^i}, y_{i+1}^{\sum_{i=0}^{f-1} x_3^i}]^{2^\alpha} \\
&\equiv [(x_1^{i+1} \prod_{j=0}^{i} [x_1, x_3^j])^{\sum_{i=0}^{f-1} x_3^i}, (x_1^{i+2} \prod_{j=1}^{i+1} [x_1, x_3^j])^{\sum_{i=0}^{f-1} x_3^i}]^{2^\alpha} \\
&\equiv [(x_1^{\sum_{i=0}^{f-1} x_3^i})^{i+1} \prod_{j=0}^{i} [x_1, (x_3^f)^j], (x_1^{\sum_{i=0}^{f-1} x_3^i})^{i+2} \prod_{j=1}^{i+1} [x_1, (x_3^f)^j]]^{2^\alpha} \\
&\equiv [(x_1^{\sum_{i=0}^{f-1} x_3^i})^{(i+1)2^\alpha}, (x_1^{\sum_{i=0}^{f-1} x_3^i})^{(i+2)2^\alpha}] \equiv 1 \mod \tilde{H}_k^{(2,2^{\alpha+1})} [\tilde{H}_k, P_k].
\end{aligned}$$

(2) :

$$\begin{aligned}
\prod_{i=0}^{f-1} [x_{2j-1}, x_{2j}]^{x_3^i} &\equiv \prod_{i=0}^{f-1} [x_{2j-1}, x_{2j}^{-1+\sum_{i=0}^{f-1} x_3^i}]^{x_3^i} \equiv \prod_{i=0}^{f-1} [x_{2j-1}^{x_3^i}, x_{2j}^{\sum_{i=0}^{f-1} x_3^i}] \\
&\equiv [x_{2j-1}^{\sum_{i=0}^{f-1} x_3^i}, x_{2j}^{\sum_{i=0}^{f-1} x_3^i}] \mod \tilde{H}_k^{(2,2^{\alpha+1})} [\tilde{H}_k, P_k].
\end{aligned}$$

Thus we finally get that the generators of $\tilde{H}_k$ are connected by the single relation

$$\begin{aligned}
&y_{f-1}^{-(1+2^{\alpha-1})2^{\alpha+1}} [y_{f-1}, z_{f-1}][x_3^f, x_4^{(1+2^\alpha)}][(x_3^f)^{x_2}, x_4^{x_2}] \\
&\times \Big(\prod_{j=3}^{(m+2)/2} [x_{2j-1}^{\sum_{i=0}^{f-1} x_3^i}, x_{2j}^{\sum_{i=0}^{f-1} x_3^i}]^{x_2-(1+2^\alpha)} \mod \tilde{H}_k^{(2,2^{\alpha+1})} [\tilde{H}_k, P_k].
\end{aligned}$$

If we define a map by

$$\begin{aligned}
&\epsilon_1 \mapsto \tilde{y_{f-1}}^{-(1+2^{\alpha-1})}, \quad \epsilon_2 \mapsto \tilde{z_{f-1}}^{-(1+2^{\alpha-1})^{-1} S(\omega^2)}, \\
&\epsilon_3 \mapsto (\tilde{x_3^f})^{\omega^f}, \quad \epsilon_i \mapsto \tilde{x_i}^{\omega^f S(\omega^2)} \ (4 \le i \le m+2) \\
\epsilon_{m+3} \mapsto \tilde{x_3^f}, \quad &\epsilon_i \mapsto \tilde{x}_{i-m}^{(-(1+2^\alpha))^{i+1-m} S(\omega^2)} \ (m+4 \le i \le 2m+2),
\end{aligned}$$

it gives us an isomorphism of the symplectic $\mathbb{Z}/q[F]$-spaces $(K(i)^*/(K(i)^*)^q)^{S(\omega^2)}$ and A_k''. □

2.4 Maximal extension without simple ramification

Lemma 2.16. *[Z1] (§5, Lemma 10)*

Any two profinite groups C_j, $j = 1, 2$, which satisfy the following conditions are isomorphic:

(1) C_j contains a subgroup D_j of index 2 isomorphic to $\mathrm{Gal}(K(2)/k(i))$,

(2) the 2-Sylow subgroup $\tilde{C}_j$ of C_j is isomorphic to $\mathrm{Gal}(K(2)/K)$,

(3) the symplectic $\mathbb{Z}/q[F]$-spaces $\tilde{D}_j/\tilde{D}_j^{(1,q)}$ and $K(i)^*/(K(i)^*)^q$ are isomorphic.

Remark 2.17. If a profinite group C satisfies condition (1) and (2) it is obvious that the 2-Sylow subgroup $\tilde{D}$ of D is isomorphic to $\mathrm{Gal}(K(2)/K(i))$ and we identify the cyclic group $C/\tilde{D}$ of order $2f$ with F. We can now consider the abelian group $\tilde{D}/\tilde{D}^{(1,q)}$ as an F-module. The unique relation connecting the generators of $\tilde{D}/\tilde{D}^{(2,q)}$ induces a symplectic $\mathbb{Z}/q[F]$-structure on $\tilde{D}/\tilde{D}^{(1,q)}$ (this works analogue to the symplectic space structure on A_k, which we explained in the section before).

Let again G_k be the profinite group with $m+2$ generators $x_1, \ldots, x_{m+2}$, subject to a single relation which depends on k, and $k \in \mathfrak{L}$ or $\mathfrak{N}_\alpha$. We now use the above lemma to prove the following theorem:

Theorem 2.18. *The groups G_k and* $\mathrm{Gal}(K(2)/k)$ *are isomorphic.*

Proof. The two Theorems 2.12, 2.13 and the Lemma 2.15, prove that the group G_k satisfies the conditions (1) to (3) in Lemma 2.16. If $k \in \mathfrak{L}$, this is due to Zelvenskii and we proved the case $k \in \mathfrak{N}_\alpha$. Furthermore, the Hasse norm residue symbol (class field theory) gives an F-isomorphism from $K(i)^*/(K(i)^*)^q$ to $\mathrm{Gal}(K(2)/K(i))/\mathrm{Gal}(K(2)/K(i))^{(1,q)}$ and thus also the group $\mathrm{Gal}(K(2)/k)$ satisfies the three conditions. □

The next step is to choose a cofinal subset W in the set of all odd natural numbers consisting of numbers congruent to $1 \mod 2^\kappa$, where $\kappa = 2$ if $k \in \mathfrak{L}$ and $\kappa = 2(\alpha+1)$

if $k \in \mathfrak{N}_\alpha$. Let $S = \{K \supseteq k \mid K/k \text{ unramified, } [K:k] \in W\}$. Since the maximal extension of k without simple ramification is equal to $\cup_{K \in S} K(2)$, we get a description of its Galois group as an inverse limit of the groups defined in terms of generators and relations at the beginning of section 2.3.

Theorem 2.19. *[Z1] (Theorem 4)*
Let k be an extension of the field of 2-adic numbers having odd degree m. The Galois group of the maximal extension without simple ramification of the field k is isomorphic to the profinite group with $m+2$ generators $x_1, \ldots, x_{m+2}$ subject to the relation

$$x_1^2 x_2^4 [x_1, x_2] \ldots [x_{m+1}, x_{m+2}] = 1$$

and the relation $x^{\Delta(2)} = 1$ on the normal subgroup generated by the elements $x_1 x_2^2, x_3, \ldots, x_{m+2}$.

Theorem 2.20. *Let k be an extension of the field of 2-adic numbers having even degree m, such that the maximal unramified extension of k does not contain a primitive 4-th root of unity. Further, let k' denote the intersection of k with the extension $\mathbb{Q}_{2^\infty}$ of the field $\mathbb{Q}_2$, and let $q \geq 4$ denote the largest power of 2 such that the q-th roots of unity belong to $k(i)$.*
If k' is not contained in the real subfield of $\mathbb{Q}_{2^\infty}$, then $q \geq 8$, and the Galois group of the maximal extension without simple ramification of the field k is isomorphic to the profinite group with $m+2$ generators $x_1, \ldots, x_{m+2}$ subject to the relation

$$x_1^{2+q/2} [x_1, x_2] \ldots [x_{m+1}, x_{m+2}] = 1$$

and the relation $x^{\Delta(2)} = 1$ on the normal subgroup generated by the elements $x_1, x_2, x_4, x_5, \ldots, x_{m+2}$.

Remark 2.21. Zelvenskii also claims that one has the following description for the Galois group of the maximal extension without simple ramification of the field k if $k \in \mathfrak{M}_\alpha$:
If k' is contained in the real subfield of $\mathbb{Q}_{2^\infty}$, then the Galois group of the maximal

extension without simple ramification of the field k is isomorphic to the profinite group with $m+2$ generators $x_1, \ldots, x_{m+2}$ subject to the relation

$$x_1^2[x_1, x_2]x_3^q[x_3, x_4] \ldots [x_{m+1}, x_{m+2}] = 1$$

and the relation $x^{\Delta(2)} = 1$ on the normal subgroup generated by the elements $x_1 x_3^{q/2}, x_2, x_4, \ldots, x_{m+2}$.

Zelvenskii wrote that one could prove the claim above in an analogous manner as for $k \in \mathfrak{L}$. But all our attempts to calculate the defining relations of H_k and $\tilde{G}_k$ in the case $k \in \mathfrak{M}_\alpha$ needed in the proofs of theorem (2.12) and (2.13) failed. In principle this problem is tractable with the methods of computer algebra. But even the simplest case is too complex to be solved by a computer program such as GAP. Indeed, finding such a presentation for H_k and $\tilde{G}_k$ is essentially an isomorphism test. According to computer algebra developer Derek Holt, there is no known algorithm for isomorphism testing of finite groups that has complexity better than $\mathcal{O}(|G|^{d(G)})$, where $d(G)$ is the number of generators of G.

3 Conjecture on the absolute Galois group of a local field with residue characteristic 2

Let k be a 2-adic number field over $\mathbb{Q}_2$ having even degree n, such that the maximal tamely ramified extension of k does not contain a primitive 4-th root of unity. As mentioned in the introduction, we can not use the same method for describing the absolute Galois group of k as in the $p \neq 2$ case and it turns out to be very difficult to find a different approach. But after working several years on this topic, we have an idea what the absolute Galois group of a field $k \in \mathfrak{N}_\alpha$ might look like.
So we also require that $k \in \mathfrak{N}_\alpha$. Then $q = 2^{\alpha+1}$ denotes the largest power of 2 such that the q-th roots of unity belong to the field $k(i)$.
Furthermore, let T be the maximal tamely ramified extension of k and 2^s, $s \in \mathbb{N}$, the number of elements in the residue field of k. Hasse and Iwasawa have shown that the Galois group $\mathscr{G} = \mathrm{Gal}(T/k)$ has two generators σ and τ with the defining relation

$$\sigma\tau\sigma^{-1} = \tau^{2^s}.$$

The group μ_T of roots of unity of 2-power order in T is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and the operation of $\mathscr{G}$ on μ_T is trivial.

Conjecture 3.1. *The absolute Galois group* $\mathrm{Gal}(k^{sep}/k)$ *is isomorphic to the profinite group* X *with* $n+3$ *generators* σ, τ, $x_0, \ldots, x_n$ *and the following defining conditions:*

(i) the normal subgroup generated by $x_0, \ldots, x_n$ *is a pro-2-group,*

(ii) the elements σ *and* τ *fulfill the relation* $\sigma\tau\sigma^{-1} = \tau^{2^s}$,

(iii) the generators satisfy the relation

$$x_0^{2+\frac{q}{2}}[x_0, x_1]x_2^{-\sigma}(x_2, \tau)[x_3, x_4]\ldots[x_{n-1}, x_n] = 1,$$

where $(x_2, \tau) = (x_2\tau)^\pi$ *and* $\pi \in \hat{\mathbb{Z}}$ *with* $\pi\hat{\mathbb{Z}} = \mathbb{Z}_2$ *(as in 1.3).*

The profinite group X is constructed as in (1.3). Thus

$$X = X(\mathscr{G}, n) = F(n+1, \mathscr{G})/(r),$$

where (r) is the (closed) normal subgroup generated by the following element r:

$$r = x_0^{2+\frac{q}{2}}[x_0, x_1]x_2^{-\sigma}(x_2, \tau)[x_3, x_4]\dots[x_{n-1}, x_n].$$

P is the normal subgroup generated by $x_0, \dots, x_n$, so

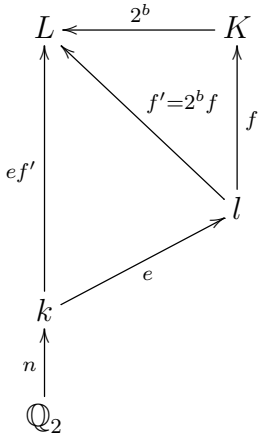
$$r \equiv (x_2, \tau) \equiv (\tau)^{\pi} \equiv 1 \mod P,$$

since the order of τ is prime to 2.

To describe the absolute Galois group of k it is enough to describe the Galois groups $\mathrm{Gal}(L(2)/k)$ of all tamely ramified extensions L/k. Let $L \subset T$ be a finite tamely ramified Galois extension of k with degree ef'. Then e is odd (e divides $2^s - 1$) and the Galois group $\mathrm{Gal}(L/k)$ is generated by σ and τ with the relations (see [I])

$$\sigma^{f'} = 1\ , \quad \tau^e = 1\ , \quad \sigma\tau\sigma^{-1} = \tau^{2^s},$$

where f' is the inertia degree and e the ramification index of L/k. Then $Gal(k^{\mathrm{sep}}/T)$ is a pro-2 group and k^{sep} is equal to $\bigcup_{k \subset L \subset T} L(2)$.
For each L we consider the diagram



where the integers denote the degree of the extensions and l is the fixed field of the subgroup of $\mathrm{Gal}(L/k)$ generated by σ. Therefore $\mathrm{Gal}(L/l)$ is cyclic of order $f' = 2^b f$ with $b \geq 0$ and f odd. Additionally K/l is an unramified extension and since e is odd, $l(i)/l$ is ramified and $q = 2^{\alpha+1}$ is still the largest power of 2 such that the q-th roots of unity belong to $l(i)$. The degree of l over $\mathbb{Q}_2$ is even and $\mathrm{Gal}(\mathbb{Q}_{2^\infty}/k \cap \mathbb{Q}_{2^\infty}) = \mathrm{Gal}(\mathbb{Q}_{2^\infty}/l \cap \mathbb{Q}_{2^\infty})$ (again since f is odd), thus $l \in \mathfrak{N}_\alpha$.
The next step is to define a special subgroup X_e of X. Let $\mathcal{H}$ be the normal subgroup of $\mathcal{G}$ generated by σ and τ^e and let $X_e = \phi^{-1}(\mathcal{H})$ denote the preimage of $\mathcal{H}$ in X ($\phi\colon X \to \mathcal{G}$ is the surjection defined by $\phi(\sigma) = \sigma,\ \phi(\tau) = \tau,\ \phi(x_i) = 1$ (see 1.3)).

The idea to prove the conjecture above is to start by showing that $X_e/(\tau^e)$ is isomorphic to the maximal extension without simple ramification of l. To obtain this isomorphism we can follow Zelvenskiis argument, which we explained in the previous section. So if $X_{e,f}$ denotes the factor group $X_e/(\tau^e)$ of X_e with one further relation, namely the relation $x^{\Delta(2)} = 1$ on the normal subgroup generated by σ^f, it is enough to show that $X_{e,f}$ is isomorphic to $\mathrm{Gal}(K(2)/l) = \mathrm{Gal}(L(2)/l)$. For this it suffices that both groups $X_{e,f}$ and $\mathrm{Gal}(K(2)/l)$ fulfill the three conditions of the following lemma:

Lemma 3.2. *[Z1] (§5, Lemma 10)*
Any two profinite groups C_j, $j = 1, 2$, which satisfy the following conditions are isomorphic:

(1) C_j contains a subgroup D_j of index 2 isomorphic to $\mathrm{Gal}(K(2)/l(i))$,

(2) the 2-Sylow subgroup $\tilde{C}_j$ of C_j is isomorphic to $\mathrm{Gal}(K(2)/K)$,

(3) the symplectic $\mathbb{Z}/q[F]$-spaces $\tilde{D}_j/\tilde{D}_j^{(1,q)}$ and $K(i)^*/(K(i)^*)^q$ are isomorphic.

We already know that $\mathrm{Gal}(K(2)/l)$ satisfies all three conditions. We are able to show the second requirement for $X_{e,f}$:

Theorem 3.3. *The 2-Sylow subgroup $\widetilde{X_{e,f}}$ of $X_{e,f}$ is isomorphic to* $\mathrm{Gal}(K(2)/K)$.

Proof. As in Theorem 2.13 we show that both groups $\widetilde{X_{e,f}}$ and $\mathrm{Gal}(K(2)/K)$ are Demuškin pro-2 groups with the same two invariants $n(\widetilde{X_{e,f}}) = n(\mathrm{Gal}(K(2)/K)) = efn+2$ and $\mathrm{Im}(\chi) = \langle -1+2^\alpha \rangle$. For $\mathrm{Gal}(K(2)/K)$ this is clear, hence we will prove the claim for $\widetilde{X_{e,f}}$: In the setting of (1.3), let $\mathcal{H}$ be the normal subgroup of $\mathscr{G}$ generated by τ^e and σ^f, $G = \mathscr{G}/\mathcal{H}$ and U the preimage of $\mathcal{H}$ in $F(n+1, \mathscr{G})$. Denote by $\overline{X}_{\mathcal{H}}$ the maximal pro-2 factor group of $X_{\mathcal{H}}$. Then $\widetilde{X_{e,f}} = \overline{X}_{\mathcal{H}}$ and if $\widetilde{\sigma^f}$ denotes the image of σ^f under the projection from U to $\widetilde{X_{e,f}}$, $\widetilde{X_{e,f}}$ is generated as normal subgroup by the elements $x_0, \ldots, x_n, \widetilde{\sigma^f}$ (the order of τ is prime to 2).
Let $\lambda = \frac{1}{e}\sum_{i=0}^{e-1} \tau^i$, then we obtain the following equivalences $(\star)$ modulo $[P,U]$:

$$\begin{aligned}(x_2,\tau) &\equiv (x_2\tau)^\pi \equiv (x_2\tau)^{e\frac{\pi}{e}} \equiv (x_2\tau x_2\tau^{-1}\tau^2 x_2 \ldots x_2\tau^{e-1}x_2\tau^{-(e-1)}\tau^e)^{\frac{\pi}{e}} \\ &\equiv (x_2 x_2^{\tau^{-1}} x_2^{\tau^{-2}} \ldots x_2^{\tau^{-(e-1)}}\tau^e)^{\frac{\pi}{e}} \equiv (x_2^{e\lambda}\tau^e)^{\frac{\pi}{e}} \\ &\equiv (x_2^\lambda)^\pi \equiv x_2^\lambda \mod [P,U].\end{aligned}$$

The last equivalences hold since $y^\pi = y$ for any $y \in P$ and $\tau^e \in U$. As a result, we have

$$\begin{aligned}r &\equiv x_0^{2+2^\alpha} x_2^{-\sigma}(x_2,\tau) \mod [P,U] \qquad (\star\star) \\ &\equiv (x_0^{1+2^\alpha})^2 x_2^{-\sigma} x_2^\lambda \mod [P,U].\end{aligned}$$

The statements in [JW] 2.4-2.7 show that

$$\begin{aligned}\dim H^2(\widetilde{X_{e,f}}, \mathbb{F}_2) &= 1, \\ \dim H^1(\widetilde{X_{e,f}}, \mathbb{F}_2) &= (\mathscr{G}:\mathcal{H})m + 2 = efn+2, \\ \mathrm{Tor}(\widetilde{X_{e,f}}^{\mathrm{ab}}) &\cong \mathbb{Z}/2\mathbb{Z} \quad \text{as G-module.}\end{aligned}$$

It is left to show that the cup product $H^1(\widetilde{X_{e,f}}, \mathbb{F}_2) \times H^1(\widetilde{X_{e,f}}, \mathbb{F}_2) \to H^2(\widetilde{X_{e,f}}, \mathbb{F}_2)$ is a nondegenerate bilinear form:
As $[P/N, X_{\mathcal{H}}] \subset X_{\mathcal{H}}^{(1,2)}$, it follows from $(\star\star)$ that

$$x_2^\sigma \equiv x_2^\lambda \mod \tilde{X}_{e,f}^{(1,2)}. \tag{3.0.1}$$

Let I be the closed two-sided ideal in $\mathbb{Z}_2[\![\mathscr{G}]\!]$ generated by 2 and $\tau^e - 1$, then

$$\sigma\lambda \equiv \lambda\sigma \mod I \qquad \text{and} \qquad \tau\lambda \equiv \lambda \mod I.$$

Therefore we get from (3.0.1)

$$x_2^\tau \equiv x_2^\lambda \equiv x_2^\sigma \equiv x_2 \mod \tilde{X}_{e,f}^{(1,2)} \tag{3.0.2}$$

and from that

$$[x_2^{a\rho}, x_2^{b\rho'}] \equiv \mod \tilde{X}_{e,f}^{(2,2)}, \tag{3.0.3}$$

for all $a, b \in \mathbb{Z}_2$ and $\rho, \rho' \in \mathscr{G}$. Consequently, the equivalences $(\star)$ also hold modulo $\tilde{X}_{e,f}^{(2,2)}$ since $\widetilde{\tau^e} = 1$, i.e.

$$\widetilde{(x_2, \tau)} \equiv x_2^\lambda \mod \tilde{X}_{e,f}^{(2,2)}.$$

Let $\kappa = \sum_{i=0}^{f-1} \sigma^i$. Then in the group ring $\mathbb{Z}_2[\![\mathscr{G}]\!]$

$$\begin{aligned} \kappa\lambda(\lambda - \sigma) &\equiv \kappa(1-\sigma)\lambda \\ &\equiv (1-\sigma^f)\lambda \mod I, \end{aligned}$$

and for a $v \in \mathbb{Z}_2[\![\mathscr{G}]\!]$ it follows from (3.0.2) that

$$x_2^{2v} \equiv x_2^{2a} \mod \tilde{X}_{e,f}^{(2,2)}$$

with $a \in \mathbb{Z}_2$.

As a result from the above, we get the equivalence

$$\begin{aligned} (x_2^{-\sigma}(\widetilde{x_2, \tau}))^{e\lambda\kappa} &\equiv x_2^{\kappa\lambda(\lambda-\sigma)e} \\ &\equiv (x_2^\lambda)^{(1-\sigma^f)e} x_2^{2a} \\ &\equiv [x_2, \widetilde{\sigma^f}]^e x_2^{2a} \mod \tilde{X}_{e,f}^{(2,2)}. \end{aligned}$$

Finally, by applying $e\lambda\kappa$ to the relation r we obtain

$$1 \equiv x_0^{(2+2^\alpha)\kappa\lambda e} x_2^{2a} [x_2, \widetilde{\sigma^f}]^e ([x_0, x_1][x_3, x_4] \dots [x_{n-1}, x_n])^{\kappa\lambda e} \mod \tilde{X}_{e,f}^{(2,2)}.$$

The $efn+2$ elements $\tilde{\sigma^f}, x_2, x_i^\rho,\ i=0,1,3,\ldots,n$, where $\rho \in G$ runs through a set of representatives of $\mathscr{G}/\mathcal{H}$, form a minimal system of generators of $\tilde{X}_{e,f}$. Analogously as in the proof of Theorem 2.13 we now can show that the cup product for $\tilde{X}_{e,f}$ is nondegenerate and calculate the invariant $\mathrm{Im}(\chi)$. For the calculation of the latter, we write $r^{e\lambda_\kappa} = r'g$ with $g \in \tilde{X}_{e,f}^{(2,2)}$ and define $\chi\colon \tilde{X}_{e,f} \to U_2$ by

$$\chi(x_1^\rho) = (-1-2^\alpha)^{-1}, \quad \chi(\tilde{\sigma^f}) = \chi(x_2) = \chi(x_i^\rho) = 1 \quad \text{for } \rho \in G,\ i = 0,3,\ldots,n,$$

which allows the lifting argument from the proof of Theorem 2.13.
Then for any crossed homomorphism D

$$D(r) = D(r') + \chi(r')D(g) = D(r') = \sum_{\rho\in G}(2^\alpha + \chi(x_1^\rho)^{-1} + 1)D(x_0^\rho) = 0.)$$

Consequently, $\tilde{X}_e$ is a Demuškin group with the required invariants. □

The idea how to prove the first condition, i.e. that the normal subgroup H of $X_{e,f}$ generated by the elements $x_0, x_1^2, x_2, \ldots, x_n, \sigma$ is isomorphic to the group $\mathrm{Gal}((K(2)/l(i))$, would be to show that the normal subgroup of X generated by $x_0, x_1^2, x_2, \ldots, x_n, \sigma, \tau$ is a so called Demuškin formation over the maximal tamely ramified extension of $k(i)$ defined by Diekert in [D] with methods similar to the ones he used. However, the computations are complicated and we have not succeeded so far.

References

[B] E. Binz, J. Neukirch and G.H. Wenzel, *A subgroup theorem for free products of pro-finite groups*, J. Algebra **19** (1971), 104-109.

[De] S.P. Demuškin, *On 2-extensions of a local field*, Sibirsk. Mat. Z. **4** (1963), 951-955; English transl. in Amer. Math. Soc. Transl. (2) **50** (1966).

[De2] S. P. Demuškin: *Topological 2-groups with an even number of generators and one complete defining relation*, Amer. Math. Soc. Transl. (2) **66** (1968).

[D] V. Diekert, *Über die absolute Galoisgruppe dyadischer Zahlkörper*, J. reine angew. Math. **350** (1984), 152-172.

[I] K. Iwasawa, *On Galois Groups of Local Fields*, Trans. Am. Math. Soc. **80** (1955), 448-469.

[Jak] A. V. Jakovlev, *The Galoisgroup of the algebraic closure of a local field*, Math. USSR Izv. **2** (1968), 1231-1269.

[J] U. Jannsen, *Über Galoisgruppen lokaler Körper*, Invent. math. **70** (1982), 53-69.

[JW] U. Jannsen and K. Wingberg, *Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper*, Invent. math. **70** (1982), 71-89.

[K1] H. Koch, *Über das Normrestsymbol einer lokalen unverzweigten Erweiterung von 2-Potenzgrad*, Math. Nachr. **52** (1972), 355-369.

[K2] H. Koch, *Galoissche Theorie der p-Erweiterungen*, VEB Deutsche Verlag der Wissenschaften, Berlin (1970).

[K3] H. Koch, *The Galois group of a p-closed extension of a local field*, Soviet. Math. Dokl. **19** (1978), 10-13.

[L] J. P. Labute, *Classification of Demuškin groups*, Canad. J. Math. **19** (1967), 106-132.

[M] D. Meier, *On two papers of I. G. Zelvenskii on Local Galois Groups*, Universität Regensburg (2016).

[N1] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin (1992).

[N2] J. Neukirch, *Freie Produkte pro-endlicher Gruppen und ihre Kohomologie*, Arch. d. Math. **12** (1971), 337-357.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology Of Number Fields*, Springer, Berlin, (2000).

[S] J. P. Serre, *Structure de certains pro-p-groupes*, Sem. Bourbaki **252** (1962/63).

[S2] J. P. Serre, *Local fields*, Springer, New York (1979).

[S3] J. P. Serre, *Galois Cohomology*, Springer, Berlin (1997).

[Si1] L. Simons, *The Structure of the Hilbert Symbol for Unramified Extensions of 2-adic Number Fields*, Ph. D. Thesis (1986), McGill University.

[Si2] L. Simons, *The Hilbert symbol for tamely ramified Abelian extensions of 2-adic number fields*, manuscripta math. **58** (1987), 345-362.

[Si3] L. Simons, *The Galois-equivariant Structure of the Norm Residue Symbol in Tamely Ramified extensions of 2-adic Number Fields*, Math. Nachr. **169** (1994), 267-277.

[W] K. Wingberg, *Der Eindeutigkeitssatz für Demuškinformationen*, Invent. math. **70** (1982), 99-113.

[Z1] I. G. Zelvenskii, *Maximal extension without simple ramification of a local field*, Math. USSR Izv. **13** (1979) No. 3, 647-661.

[Z2] I. G. Zelvenskii, *On the algebraic closure of a local field for p=2*, Math. USSR Izv. **6** (1972).