Algebra & Number Theory

Volume 12

2018

No. 10

Realizing 2-groups as Galois groups following Shafarevich and Serre

Peter Schmid

ALGEBRA AND NUMBER THEORY 12:10 (2018)
dx.doi.org/10.2140/ant.2018.12.2387

Realizing 2-groups as Galois groups following Shafarevich and Serre

Peter Schmid

Let G be a finite p-group for some prime p, say of order p^n. For odd p the inverse problem of Galois theory for G has been solved through the (classical) work of Scholz and Reichardt, and Serre has shown that their method leads to fields of realization where at most n rational primes are (tamely) ramified. The approach by Shafarevich, for arbitrary p, has turned out to be quite delicate in the case $p = 2$. In this paper we treat this exceptional case in the spirit of Serre's result, bounding the number of ramified primes at least by an integral polynomial in the rank of G, the polynomial depending on the 2-class of G.

1. Introduction

Let p be prime and G a finite p-group. By [Scholz 1937; Reichardt 1937] there is a Galois extension $K\,|\,\mathbb{Q}$ with group G provided p is odd. The general case, allowing $p = 2$, has been treated by Shafarevich [1954] in a different and somehow more complicated way. Actually the $p = 2$ case led to controversial discussions some years ago, because Shafarevich used in his proof "something on free groups (and their p-filtration) which is false for $p = 2$" (Serre in a letter of May 10, 1988). Shafarevich [1989] corrected this by suggesting to use a refined filtration. The proof of Shafarevich's theorem (for solvable groups) given in [Neukirch et al. 2000] is based on this filtration; it employs deep results and techniques in cohomology of number fields.

The Scholz–Reichardt method has been explained further by Serre. In a letter of September 6, 1988 he wrote: "I have now looked into Reichardt's 1937 paper in Crelle, and it is quite nice. The proof gives a rather surprising result, namely: if G has order p^n, $p \neq 2$, then G can be realized as $\mathrm{Gal}(K\,|\,\mathbb{Q})$ where K is ramified at most n primes. However, $p \neq 2$ seems indeed essential." This was elaborated in [Serre 1992, Chapter 2]. A slight improvement was given in [Plans 2004]; see also [Geyer and Jarden 1998].

The field K in Serre's letter refers to so-called *Scholz fields* (Section 2). Only tame ramification happens in these fields, so that the inertia groups are all cyclic. This implies that the cardinality of the set $\mathrm{Ram}(K)$ of rational primes ramified in K must be at least equal to the rank $d(G)$ of the p-group $G = \mathrm{Gal}(K\,|\,\mathbb{Q})$, its minimum number of generators (in view of Burnside's basis theorem and the Hermite–Minkowski theorem). Indeed at least $d(G)$ primes must ramify in the socle $\mathfrak{S}(K)$ of K, the fixed field of the Frattini subgroup $\Phi(G)$ of G (where $G/\Phi(G)$ is an $\mathbb{F}_p$-vector space of dimension $d(G)$).

MSC2010: primary 11R32; secondary 20D15.
Keywords: Galois 2-groups, Scholz fields, tame ramification, Shafarevich, Serre.

The *p-class* (sometimes also called Frattini class) of the p-group G is the least positive integer c such that G has a central series of length c with all factors being elementary.

Theorem. *Let G be a nontrivial finite 2-group with rank d and 2-class c. There exist infinitely many Scholz fields K with pairwise coprime (absolute) discriminants realizing G as Galois group over $\mathbb{Q}$ and satisfying* $\mathrm{Ram}(K) \subseteq 1 + 2^c\mathbb{Z}$ *and* $|\mathrm{Ram}(K)| \leq f_c(d)$ *for some integral polynomial f_c of degree* $(c+3)!/24$.

The upper bound on the cardinality of $\mathrm{Ram}(K)$ is rather weak (compared with the odd case). This is primarily due to the (inductive) shrinking process needed (see below). The polynomial $f_c \in \mathbb{Z}[X]$ will be defined recursively ($f_1 = X,\ f_2 = 2X^5 + X^2, \dots$).

For any number field K_0 there is a field K as above having discriminant coprime to that of K_0. Then the compositum K_0K (in $\mathbb{C}$) is Galois over K_0 and admits G. Reichardt [1937] proved a corresponding result in the odd case.

The proof of the theorem utilizes ideas from Scholz, Reichardt and Serre, as well as from Shafarevich. Up to isomorphism there is a unique p-group $G_d^c(p)$ of minimal order with rank d and p-class c which has every (finite) p-group of rank d and p-class c as epimorphic image. We will have to consider, like Shafarevich [1954], this so-called *disposition p-group* (for $p = 2$). In order to eliminate certain (*Scholz*) *obstructions* we also use a *shrinking process*, a technique also developed in [Shafarevich 1954]. However, avoiding Shafarevich's "graded functions on canonical homomorphisms", this will be based on the Chevalley–Warning theorem, in a manner as proposed in [Meshulam and Sonn 1999; Neukirch et al. 2000, Proposition (9.5.4)]. It is possible to derive upper bounds on $|\mathrm{Ram}(K)|$ following the lines of proof given by Shafarevich; e.g., see [Rabayev 2013].

The "minimal ramification problem" for a p-group G is the question whether G can be realized as the group of a tamely ramified Galois extension of $\mathbb{Q}$ in which exactly $d(G)$ primes are ramified. Kisilevsky, Neftin and Sonn [Kisilevsky et al. 2010] answered this question to the affirmative in the case where G is semiabelian. At present a general answer seems to be out of reach; no counterexample is known so far.

2. Scholz fields

In this section G is a finite p-group for some prime p. As usual $G_{\mathbb{Q}}$ denotes the absolute Galois group of the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ contained in $\mathbb{C}$. Number fields are understood to be subfields of $\overline{\mathbb{Q}}$. For any rational prime q we fix one of the $G_{\mathbb{Q}}$-conjugate prime ideals $\mathfrak{Q}$ above q of the ring of algebraic integers in $\overline{\mathbb{Q}}$, and let $I_q \subset D_q$ denote the inertia and decomposition groups of $\mathfrak{Q}$ ($D_q/I_q \cong \mathrm{Gal}(\overline{\mathbb{F}}_q \,|\, \mathbb{F}_q) \cong \widehat{\mathbb{Z}}$).

Definition 1. Let N be a positive integer with $p^N \geq \exp(G)$, where $\exp(G)$ denotes the exponent of G. Suppose we have a (continuous) epimorphism $\varphi : G_{\mathbb{Q}} \twoheadrightarrow G$. The fixed field $K = \overline{\mathbb{Q}}^{\mathrm{Ker}(\varphi)}$ of $\mathrm{Ker}(\varphi)$ (having Galois group G over the rationals) is a *Scholz field* with respect to N provided:

(S1) Each $q \in \mathrm{Ram}(K)$ belongs to $1 + p^N\mathbb{Z}$.

(S2) Each $q \in \mathrm{Ram}(K)$ is *busy* in K (in German: "fleissig"); that is, $\varphi(I_q) = \varphi(D_q)$.

We say that K is a Scholz field (per se) if it is Scholz with respect to N for some N with $p^N \geq \exp(G)$. Normal subfields of Scholz fields obviously are Scholz fields. We also say that K is a *strong* Scholz field (with respect to N) if in addition the socle satisfies $\mathfrak{S}(K) = P_1 \cdots P_d$, where $d = d(G)$ and the sets $\operatorname{Ram}(P_i)$ for the (cyclic) fields P_i are pairwise disjoint and of the same cardinality.

By (S1) ramification in a Scholz field K is always tame, and by (S2) the residue class degrees of the primes of K ramified over $\mathbb{Q}$ are 1. Our definition of a Scholz field is in accordance with that given in [Scholz 1937; Reichardt 1937; Serre 1992] (for odd p), but differs from that in [Shafarevich 1954]. In the $p = 2$ case from (S1), with $N \geq 3$, it follows that 2 splits completely in $\mathfrak{S}(K)$ and that this is a (totally) real field, which just says that $\mathfrak{S}(K)$ is a Scholz field in the sense of Shafarevich.

Proposition 2.1. *Let $Z \rightarrowtail H \xrightarrow{\pi} G$ be a nonsplit central extension of the p-group G where $Z = Z_p$ is cyclic of order p. Assume that $K = \overline{\mathbb{Q}}^{\operatorname{Ker}(\varphi)}$ is a Scholz field with respect to N where $p^N \geq \exp(H)$. Then the embedding problem $(G_{\mathbb{Q}}, \varphi, \pi)$ has a proper solution $E = \overline{\mathbb{Q}}^{\operatorname{Ker}(\psi)}$, with $\psi : G_{\mathbb{Q}} \twoheadrightarrow H$ lifting φ, such that* $\operatorname{Ram}(E) = \operatorname{Ram}(K)$.

Since Z is contained in the Frattini subgroup of H, every solution of the embedding problem $(G_{\mathbb{Q}}, \varphi, \pi)$ is proper. Let $\rho \in H^2(G, Z)$ be the cohomology class of the extension. Recall that $(G_{\mathbb{Q}}, \varphi, \pi)$ has a solution if and only if the map $\varphi^* : H^2(G, Z) \to H^2(G_{\mathbb{Q}}, Z)$ induced by φ vanishes at ρ [Neukirch et al. 2000, Proposition (9.4.2)]. The existence of a solution then follows by using standard global-local techniques, as described in [Serre 1992, Lemma 2.1.5]. Actually Serre treats only the case where p is odd; see also [Scholz 1937; Reichardt 1937]. Let $p = 2$ (and $Z = Z_2$). The map $\tau \mapsto \tau^2$ is an epimorphism of $\overline{\mathbb{Q}}^*$ onto itself with kernel $\{\pm 1\} \cong Z$. Using that $H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*) = 0$ (Hilbert's Theorem 90) we get that $H^2(G_{\mathbb{Q}}, Z)$ is isomorphic to $\operatorname{Br}_2(\mathbb{Q})$, the 2-torsion of the Brauer group $\operatorname{Br}(\mathbb{Q}) = H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*)$ of $\mathbb{Q}$. Restriction to the decomposition groups $D_q \cong G_{\mathbb{Q}_q}$ gives rise to a map

$$\operatorname{Br}_2(\mathbb{Q}) \to \bigoplus_q \operatorname{Br}_2(\mathbb{Q}_q),$$

and this is injective when q varies over all (finite) rational primes (ignoring the infinite place ∞). This follows from the celebrated Brauer–Hasse–Noether theorem, which tells us that an element of $\operatorname{Br}(\mathbb{Q})$ is trivial provided it is locally trivial everywhere, except possibly at one place (*Hasse reciprocity*; see [Weil 1967, Chapter XIII, Theorem 2]). Now the arguments given in [Serre 1992] apply as in the odd case. (For odd p the archimedean places can be ignored, and by Hasse reciprocity one could allow that p is ramifying [Reichardt 1937].)

Having found a solution of the embedding problem $(G_{\mathbb{Q}}, \varphi, \pi)$ from [Serre 1992, Proposition 2.1.7] it follows that there is a solution E with $\operatorname{Ram}(E) = \operatorname{Ram}(K)$; see also [Scholz 1937, Section 5].

Usually the field $E = \overline{\mathbb{Q}}^{\operatorname{Ker}(\psi)}$ will not be a Scholz field, because condition (S2) may fail. It is the unique solution of $(G_{\mathbb{Q}}, \varphi, \pi)$ with $\operatorname{Ram}(E) = \operatorname{Ram}(K)$ only when $|\operatorname{Ram}(\mathfrak{S}(K))| = d(G)$. In fact, by the Kronecker–Weber theorem $\mathfrak{S}(K)$ is a subfield of a cyclotomic field. Let $q \in \operatorname{Ram}(\mathfrak{S}(K))$, and let P_q be the (unique) subfield of the q-th cyclotomic field $\mathbb{Q}(\zeta_q)$ of absolute degree p, which exists by (S1). Then

$\mathrm{Ram}(P_q) = \{q\}$. There is an epimorphism $\chi_q : G_{\mathbb{Q}} \twoheadrightarrow Z$ with $\overline{\mathbb{Q}}^{\mathrm{Ker}(\chi_q)} = P_q$, and $E_q = \overline{\mathbb{Q}}^{\mathrm{Ker}(\psi\chi_q)}$ is a solution of $(G_{\mathbb{Q}}, \varphi, \pi)$ with $\mathrm{Ram}(E_q) = \mathrm{Ram}(E) = \mathrm{Ram}(K)$. We have $E_q = E$ only when $P_q \subseteq \mathfrak{S}(K)$. Hence uniqueness happens only when $\mathfrak{S}(K) = \prod_{q \in \mathrm{Ram}(\mathfrak{S}(K))} P_q$.

Lemma 2.2. *For any positive integers N, d there exist infinitely many pairwise disjoint d-sets of primes $\{q_1, \dots, q_d\}$ such that each q_i is in $1 + p^N\mathbb{Z}$ and is a p^N-th power in $\mathbb{F}_{q_j}^* = (\mathbb{Z}/q_j\mathbb{Z})^*$ whenever $j \neq i$.*

Let q_1 be one of the infinitely many (Chebotarev) primes which split completely in the p^N-th cyclotomic field $K_1 = \mathbb{Q}(\zeta_{p^N})$. Let q_2 split completely in $K_2 = K_1(\zeta_{q_1}, \sqrt[p^N]{q_1})$, …, and let finally q_d split completely in $K_d = K_{d-1}(\zeta_{q_{d-1}}, \sqrt[p^N]{q_{d-1}})$. Each q_i is in $1 + p^N\mathbb{Z}$ as it splits completely in $\mathbb{Q}(\zeta_{p^N})$. In

$$K_{i+1} = \mathbb{Q}(\zeta_{p^N}; \zeta_{q_1}, \dots, \zeta_{q_i}; \sqrt[p^N]{q_1}, \dots, \sqrt[p^N]{q_i})$$

the prime q_{i+1} is completely split, whereas $q_1, \dots, q_i$ are ramified ($1 \le i < d$). For $1 \le j \le i$ we have $q_{i+1} \in 1 + q_j\mathbb{Z}$ since it is totally split in $\mathbb{Q}(\zeta_{q_j})$; in this case q_{i+1} obviously is a p^N-th power in $\mathbb{F}_{q_j}^*$. Since q_{i+1} splits completely in $\mathbb{Q}(\zeta_{p^N}, \sqrt[p^N]{q_j})$ for $j \le i$, the congruence $x^{p^N} \equiv q_j \pmod{q_{i+1}}$ is solvable in $\mathbb{Z}$ (Kummer's theorem).

Having found this d-set $\{q_1, \dots, q_d\}$ of primes, let q_{d+1} be a prime splitting totally in $K_{d+1} = K_d(\zeta_{q_d}, \sqrt[p^N]{q_d})$, and proceed in this manner.

Lemma 2.3. *Given positive integers N, d, let $\{q_1, \dots, q_d\}$ be a d-set of primes as constructed in the preceding lemma. Let also n_i be integers with $1 \le n_1 \le n_2 \le \dots \le n_d \le N$, and let G be abelian of type $(p^{n_1}, \dots, p^{n_d})$. For $i = 1, \dots, d$ let P_i be the (unique) subfield of $\mathbb{Q}(\zeta_{q_i})$ of absolute degree p^{n_i} (which exists). Then $K = P_1 \cdots P_d$ is a Scholz field with respect to N realizing G as Galois group over $\mathbb{Q}$, with* $\mathrm{Ram}(K) = \{q_1, \dots, q_d\}$.

By construction and the decomposition law in cyclotomic fields, for each $i = 1, \dots, d$ the prime q_i is in $1 + p^N\mathbb{Z}$, is totally ramified in P_i and is completely split in all P_j, $j \neq i$.

Remark. Let $S = \{q_1, \dots, q_d\}$ be as constructed in Lemma 2.2, and let $G_S(p)$ be the absolute Galois group of the maximal p-extension of $\mathbb{Q}$ unramified outside $S \cup \{\infty\}$. By [Fröhlich 1983, Theorem 4.11] $G_S(p)$ maps onto every p-group of rank d, exponent p^N and nilpotency class 2. This solves the minimal ramification problem for p-groups of nilpotency class at most 2 (varying d and N). However, it is easily seen that such groups are semiabelian (so that [Kisilevsky et al. 2010] applies).

By recursive definition a finite group G is *semiabelian* if either G is abelian or $G = AH$ for some normal abelian subgroup A of G and some *proper* semiabelian subgroup H. So G is an epimorphic image of a split group extension with abelian kernel. In an analogous manner finite solvable groups might be called *seminilpotent* (see Proposition 2.2.4 and Claim 2.2.5 in [Serre 1992], and the elegant proof of this claim in the case of abelian kernels).

The bound $|\mathrm{Ram}(K)| = d(G)$ can be diminished if one allows also wild ramification. Examples for $p = 2$ are the (semiabelian) dihedral, semidihedral and modular 2-groups, with $\mathrm{Ram}(K) = \{2\}$, whereas the (generalized) quaternion 2-groups require a further (odd) ramifying prime; e.g., see [Schmid 2014].

3. Disposition 2-groups

For subgroups X, Y of a group G we let $[X, Y]$ be the subgroup of G generated by the commutators $[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$ $(x \in X,\ y \in Y)$. We define recursively $[x_1, \dots, x_{n+1}] = [[x_1, \dots, x_n], x_{n+1}]$, and $\gamma_1(G) = G,\ \gamma_{n+1}(G) = [\gamma_n(G), G]$ describing the lower central series of G. As usual we write $G' = \gamma_2(G) = [G, G]$. We also denote by $Z(G)$ the centre of G, and we write $Z'(G) = Z(G) \cap G'$.

The lower (central Frattini) 2-series of the group G is defined inductively by $\lambda_1(G) = G$ and $\lambda_{n+1}(G) = [\lambda_n(G), G]\lambda_n(G)^2$. If $G \neq 1$ is a finite 2-group then $\Phi(G) = \lambda_2(G)$ is the Frattini subgroup of G, and G has 2-class c if $\lambda_{c+1}(G) = 1$ but $\lambda_c(G) \neq 1$. Letting F_d be "the" free group of finite rank $d \geq 1$, for any integer $c \geq 1$ the quotient

$$G_d^c = G_d^c(2) = F_d/\lambda_{c+1}(F_d)$$

is a finite 2-group of rank d and 2-class c, which will be called a "disposition group" (with respect to the prime $p = 2$; of course we could replace F_d by the free pro-2-group of rank d). Every (finite) 2-group G of rank $\leq d$ and 2-class $\leq c$ is an epimorphic image of G_d^c. In fact, by the universal property of free groups, and by Burnside's basis theorem, any epimorphism $F_d/\lambda_2(F_d) \twoheadrightarrow G/\lambda_2(G)$ lifts to an epimorphism $\pi : F_d \twoheadrightarrow G$, and $\lambda_{c+1}(G) = 1$ implies that $\lambda_{c+1}(F_d) \subseteq \operatorname{Ker}(\pi)$.

The disposition p-groups have been studied in the literature quite intensively (see for instance [Shafarevich 1989; Neukirch et al. 2000; Schmid 2017]). We summarize the basic facts (for the somewhat exceptional case $p = 2$).

Proposition 3.1. *Let $G = G_d^c$ for $d \geq 2$ and $c \geq 2$, and let*

$$\ell_d^\kappa = \frac{1}{k} \sum_{k|\kappa} \mu(k) d^{\kappa/k}$$

for $\kappa = 1, \dots, c$ (where $\mu(k)$ denotes the Möbius function). The group G has rank d, exponent 2^c and nilpotency class c, with centre $Z(G) = \lambda_c(G)$. So both $V = G/\Phi(G)$ and $Z(G)$ are $\mathbb{F}_2$-vector spaces (often written additively):

(a) *The assignment $x\Phi(G) \mapsto x^{2^{c-1}}$ for $x \in G$ is a well-defined injection of V into $Z(G)$. Fix a basis $\{x_i\Phi(G)\}_{i=1}^d$ of V $(x_i \in G)$, and let $z_i = x_i^{2^{c-1}}$ and $L_d^1 = \langle z_1, \dots, z_d \rangle$. Then $Z(G) = L_d^1 \oplus Z'(G)$, and $x_i\Phi(G) \mapsto z_i$ defines a linear isomorphism $\psi_d^1 : V \xrightarrow{\sim} L_d^1$.*

(b) *For $\kappa \in \{2, \dots, c\}$ the $2^{c-\kappa}$-th power map on $\gamma_\kappa(G)$ is a homomorphism with kernel $\gamma_{\kappa+1}(G)\gamma_\kappa(G)^2$ and image $L_d^\kappa = \gamma_\kappa(G)^{2^{c-\kappa}}$ in $Z'(G)$, and we have the (natural) direct decomposition*

$$Z'(G) = L_d^2 \oplus \cdots \oplus L_d^c.$$

The "Lie module" L_d^κ has the $\mathbb{F}_2$-dimension ℓ_d^κ, and the assignments $\bar{x}_1 \otimes \cdots \otimes \bar{x}_\kappa \mapsto [x_1, \dots, x_\kappa]^{2^{c-\kappa}}$, for $x_i \in G$ and $\bar{x}_i = x_i\Phi(G)$, define an epimorphism $\psi_d^\kappa : V^{\otimes\kappa} \twoheadrightarrow L_d^\kappa$.

Proposition 3.1 is contained in the (Main) Theorem of [Schmid 2017] (where one can also find an explanation of the notion "Lie module"). Actually we shall only use the $\mathbb{F}_2$-vector space decomposition

$Z(G_d^c) = \bigoplus_{\kappa=1}^{c} L_d^{\kappa}$, together with the epimorphisms ψ_d^{κ} described above. We emphasize that ψ_d^1 depends on the choice of a basis for $G_d^c/\Phi(G_d^c)$ (in the $p=2$ case).

Lemma 3.2. *Let $G_\delta^c = G_\delta^c$ and $G_d^c = G_d^c$ be disposition 2-groups with $\delta > d \geq 2$ and $c \geq 2$, and let $\alpha : G_\delta^c/\Phi(G_\delta^c) \twoheadrightarrow G_d^c/\Phi(G_d^c)$ be an epimorphism. Then all lifts of α to G_δ^c (which exist) restrict to the same epimorphism $\alpha_z : Z(G_\delta^c) \twoheadrightarrow Z(G_d^c)$, and α_z maps $Z'(G_\delta^c)$ onto $Z'(G_d^c)$ respecting the direct decompositions into Lie modules.*

This lemma follows from [Schmid 2017, Proposition 3]. If α sends basis vectors to basis vectors or zero, and L_δ^1, L_d^1 are computed with regard to these bases (see above), then α_z maps L_δ^1 onto L_d^1. The following lemma is Proposition 4 in [Schmid 2017].

Lemma 3.3. *Let $H = G_d^c$ with $d \geq 2$, $c \geq 2$, and let $G = H/Z(H)$ ($\cong G_d^{c-1}$). There is a natural (transgression) isomorphism* $\mathrm{Hom}(Z(H), \mathbb{F}_2) \xrightarrow{\sim} H^2(G, \mathbb{F}_2)$*. Choose a basis $\{\rho_\tau\}$ of $H^2(G, \mathbb{F}_2)$, and let H_τ for each τ be an extension of G by $Z_2 \cong \mathbb{F}_2$ with cohomology class ρ_τ. Then the fibre product of the H_τ amalgamating G is isomorphic to H.*

4. The Scholz obstructions

Let $d \geq 2$, $c \geq 2$, and let $G = G_d^{c-1}$. Let N be an integer with $N \geq c$, and suppose we have a strong Scholz field K with respect to N realizing G as Galois group over $\mathbb{Q}$. Let $\{\rho_\tau\}$ be a basis of $H^2(G, \mathbb{F}_2)$. For any τ let H_τ be a (central) extension of G by $Z_2 \cong \mathbb{F}_2$ with cohomology class ρ_τ, and let E_τ be a solution of the corresponding nonsplit embedding problem with $\mathrm{Ram}(E_\tau) = \mathrm{Ram}(K)$ (see Proposition 2.1). The compositum $E = \prod_\tau E_\tau$ is a normal number field containing K with $\mathrm{Ram}(E) = \mathrm{Ram}(K)$, and $H = \mathrm{Gal}(E\,|\,\mathbb{Q})$ is the fibre product of the H_τ amalgamating G. Hence $H \cong G_d^c$ by Lemma 3.3.

For proof-technical reasons we assume in what follows merely that the E_τ are chosen such that if there is $q \in \mathrm{Ram}(E) \setminus \mathrm{Ram}(K)$, then $q \in 1 + 2^N\mathbb{Z}$ and q splits completely in $\mathfrak{S}(K)$. We also will choose the basis $\{\rho_\tau\}$ of $H^2(G, Z_2)$ suitably, without altering the field E (see below). Let $t = \dim H^2(G, Z_2) = \dim Z(H)$ (Lemma 3.3).

By Proposition 3.1 we have $Z(H) = \lambda_c(H) \subseteq \Phi(H)$ and $H/Z(H) \cong G$. Hence by assumption $\mathfrak{S}(E) = \mathfrak{S}(K) = P_1 \cdots P_d$, where the $\mathrm{Ram}(P_i)$ are pairwise disjoint and of the same cardinality. Let b_i be the discriminant of P_i. By (S1) 2 is unramified in $P_i = \mathbb{Q}(\sqrt{b_i})$ and hence

$$b_i = \prod_{q \in \mathrm{Ram}(P_i)} q \in 1 + 2^N\mathbb{Z}.$$

Given a prime q we simply write $I_q \subseteq D_q$ for the inertia and decomposition groups in H of some fixed prime $\mathfrak{Q}$ of E above q (determined up to H-conjugacy). The images of these groups in $H/\Phi(H) = \mathrm{Gal}(\mathfrak{S}(E)\,|\,\mathbb{Q})$ and their intersections with $Z(H) = \mathrm{Gal}(E\,|\,K)$ are independent of the choice of $\mathfrak{Q}$. Recall that I_q is cyclic (by tame ramification).

Lemma 4.1. *Let $I_q = \langle x_i \rangle$ be the inertia group in H of some $q \in \mathrm{Ram}(P_i)$ $(1 \leq i \leq d)$. Then $\bar{x}_i = x_i\Phi(H)$ and $z_i = x_i^{2^{c-1}}$ are independent of the choice of the prime q in $\mathrm{Ram}(P_i)$, and $\{x_i\}_{i=1}^d$ is a minimal system* *of generators for H. For any $q \in \mathrm{Ram}(P_i)$ we have $I_q \cap Z(H) = \langle z_i \rangle$, and the primes of K above q are unramified in $E^{\langle z_i \rangle}$.*

This is immediate from the structure of $\mathfrak{S}(E) = E^{\Phi(H)}$ and from Proposition 3.1. We also get that $L_d^1 = \langle z_1, \dots, z_d \rangle$ is an $\mathbb{F}_2$-subspace of $Z(H)$ of dimension $d = \ell_d^1$ complementary to $Z'(H) = H' \cap Z(H)$ in $Z(H)$. Hence letting $E^\perp = \bigcap_{i=1}^d E^{\langle z_i \rangle}$ be the fixed field of this L_d^1 we have $E = E^\perp \cdot E^{Z'(H)}$ and $E^\perp \cap E^{Z'(H)} = K$. Let also

$$E(i) = \bigcap_{j \neq i} E^{\langle z_j \rangle} \cap E^{Z'(H)}$$

for each $i = 1, \dots, d$. Now choose a basis $\{\chi_\tau\}$ of $\mathrm{Hom}(Z(H), \mathbb{F}_2)$ such that $E_\tau = E^{\mathrm{Ker}(\chi_\tau)}$ either is contained in $E^\perp$ or is equal to $E(i)$ for some i, and let $\{\rho_\tau\}$ correspond to $\{\chi_\tau\}$ under the transgression isomorphism $\mathrm{Hom}(Z(H), \mathbb{F}_2) \xrightarrow{\sim} H^2(G, \mathbb{F}_2)$ (Lemma 3.3).

For each τ write $E_\tau = K(\sqrt{\mu_\tau})$ for some $\mu_\tau \in K^*$ (determined mod $(K^*)^2$). Then every group extension of G by Z_2 with cohomology class ρ_τ is realized as $K(\sqrt{m\mu_\tau})$ for some (square-free) integer $m \neq 0$, because it is obtained by Baer addition of H_τ with the split extension of G by Z_2 realized as $K(\sqrt{m}) = \mathbb{Q}(\sqrt{m}) \cdot K$ (with $\mathbb{Q}(\sqrt{m}) \nsubseteq K$; alternately, multiply $\psi_\tau : G_\mathbb{Q} \twoheadrightarrow H_\tau$ with $\chi_m : G_\mathbb{Q} \twoheadrightarrow Z_2$ having $\overline{\mathbb{Q}}^{\mathrm{Ker}(\chi_m)} = \mathbb{Q}(\sqrt{m})$).

Let $q \in \mathrm{Ram}(P_i)$ for some i, and let $I_q \subseteq D_q$ be as above. For any prime $\mathfrak{q}$ of K above q, determined up to G-conjugacy, the Frobenius

$$\bar{\phi}_q = \left(\frac{E^{\langle z_i \rangle} \,|\, K}{\mathfrak{q}} \right)$$

(Artin symbol) is an element of $\mathrm{Gal}(E^{\langle z_i \rangle} \,|\, K)$ and independent of the choice of $\mathfrak{q}$ above q. Since q is busy in the Scholz field K, both I_q and D_q have the same image (of order 2^{c-1}) in $H/Z(H) \cong G$. Hence $D_q = I_q(D_q \cap Z(H))$ and

$$D_q \cap Z(H) = \langle z_i \rangle \times \langle \sigma_q \rangle$$

for some element σ_q (of order 2 or 1) mapping onto $\bar{\phi}_q$, which in turn maps onto the generator of D_q/I_q. If $\sigma_q \neq 0$ (additive notation), we may replace σ_q by $z_i + \sigma_q$. In spite of this ambiguity we call σ_q “the” *Scholz obstruction* for E associated to q. This will be no problem since we only shall consider the restrictions of σ_q to fields $E_\tau \subseteq E^{\langle z_i \rangle}$.

Proposition 4.2. *Let $\sigma_i = \sum_{q \in \mathrm{Ram}(P_i)} \sigma_q$, and assume that $\sigma_i = 0$ (or that $\sigma_i \in \langle z_i \rangle$) for all $i = 1, \dots, d$. Then there exist infinitely many pairwise disjoint t-sets $\{p_1, \dots, p_t\}$ of rational primes such that $\widehat{E} = \prod_{\tau=1}^t K(\sqrt{p_\tau e \mu_\tau})$ is a strong Scholz field with respect to N admitting G_d^c as Galois group over $\mathbb{Q}$ and having $\mathrm{Ram}(\widehat{E}) = \mathrm{Ram}(K) \cup \{p_1, \dots, p_t\}$.*

Proof. We argue by induction. Suppose that either $K_0 = K$ or that $K_0 = \prod_{\tau'} K(\sqrt{p_{\tau'} e \mu_{\tau'}})$ is a strong Scholz field with respect to N (with corresponding $\mathrm{Ram}(K_0)$) for certain τ' and primes $p_{\tau'}$, but that there is still some τ different from all these τ'. We prove that there are infinitely many primes $p_\tau \in 1 + 2^N\mathbb{Z}$

which split completely in K_0 such that $\hat{E}_0 = K_0(\sqrt{p_\tau e \mu_\tau})$ is a strong Scholz field with respect to N with $\mathrm{Ram}(\hat{E}_0) = \mathrm{Ram}(K_0) \cup \{p_\tau\}$.

Let $G_0 = \mathrm{Gal}(K_0|\mathbb{Q})$. By Lemma 3.3 this represents a central Frattini extension of G and is an epimorphic image over G of $H \cong G_d^c$. In particular $\mathfrak{S}(K_0) = \mathfrak{S}(K) = \mathfrak{S}(E)$. By construction the image ρ_0 of ρ_τ under the inflation map $\inf : H^2(G, \mathbb{F}_2) \to H^2(G_0, \mathbb{F}_2)$ is nontrivial. Let $E_0 = K_0 E_\tau = K_0(\sqrt{\mu_\tau})$ and $H_0 = \mathrm{Gal}(E_0|\mathbb{Q})$. For $x \in G_0$ choose an inverse image $\tilde{x} \in H_0$, and observe that $E_0 = K_0(\sqrt{\mu_\tau}^{\tilde{x}})$ and $(\sqrt{\mu_\tau}^{\tilde{x}})^2 = (\sqrt{\mu_\tau}^2)^{\tilde{x}} = \mu_\tau^x$. Hence

$$\mu_\tau^x = \beta_x^2 \mu_\tau$$

for some $\beta_x \in K_0^*$. Let $\mathfrak{q}_0 | q$ be primes of $K_0|\mathbb{Q}$. For the $\mathfrak{q}_0$-adic valuation we have $v_{\mathfrak{q}_0}(\mu_\tau) = v_{\mathfrak{q}_0{}^x}(\mu_\tau^x) = 2 \cdot v_{\mathfrak{q}_0{}^x}(\beta_x) + v_{\mathfrak{q}_0{}^x}(\mu_\tau)$. This shows that the fractional ideal (μ_τ) of K_0 generated by μ_τ splits into a square of a fractional ideal $\mathfrak{b}$ and a G_0-invariant square-free (integral) ideal of K_0, the latter being decomposed into products of G_0-conjugates of primes of K_0 ramified over $\mathbb{Q}$ and those which are not. Hence may write uniquely

$$(\mu_\tau) = \mathfrak{b}^2 \cdot \mathfrak{D} \cdot (e),$$

where $\mathfrak{D}$ is a G_0-invariant ideal of K_0 composed of pairwise distinct prime ideals of K_0 ramified over the rationals, and where e is a square-free positive integer relatively prime to the discriminant of K_0.

Let again $\mathfrak{q}_0 | q$ be primes of $K_0|\mathbb{Q}$. By [Hecke 1981, Theorem 120], $\mathfrak{q}_0$ is ramified in $E_0 = K_0(\sqrt{\mu_\tau})$ if and only if $v_{\mathfrak{q}_0}(\mu_\tau)$ is odd, except possibly when $\mathfrak{q}_0$ is dyadic (lying above 2). But 2 is not ramified in the Scholz field K_0 by (S1), and $\mathrm{Ram}(E_\tau) \subseteq 1 + 2^N \mathbb{Z}$ by assumption. So this exception does not happen. Hence $\mathfrak{q}_0$ is ramified in E_0 if and only if either $\mathfrak{q}_0$ appears in $\mathfrak{D}$ or q is a divisor of e. Each rational prime dividing e is unramified in K_0 but ramified in $E_0 = K_0 E_\tau$ and hence in E_τ. The prime divisors of e (if any) therefore are in $\mathrm{Ram}(E) \setminus \mathrm{Ram}(K)$, thus belong to $1 + 2^N \mathbb{Z}$ and split completely in $\mathfrak{S}(K)$ (by our convention).

Let R be the subset of $\mathrm{Ram}(K)$ consisting of those rational primes q for which the primes $\mathfrak{q}$ of K above q do not ramify in E_τ. We claim that $R = R(\rho_\tau)$ is an invariant of the cohomology class ρ_τ. By Hecke $v_\mathfrak{q}(\mu)$ is even, and knowing that $q \neq 2$ one just has to show that $v_\mathfrak{q}(m\mu) = v_\mathfrak{q}(m) + v_\mathfrak{q}(\mu)$ also is even for any integer $m \neq 0$. But this is clear since $v_\mathfrak{q}(m) = e(\mathfrak{q}|q) \cdot v_q(m)$ and the ramification index $e(\mathfrak{q}|q) = |I_\mathfrak{q}|$ is a proper power of 2. Similarly, the set R_0 of rational primes ramified in K_0 but not in $E_0 = K_0 E_\tau$ is an invariant of $\rho_0 = \inf(\rho_\tau)$.

Now let $q \in \mathrm{Ram}(\mathfrak{S}(K_0)) = \mathrm{Ram}(\mathfrak{S}(K))$, say $q \in \mathrm{Ram}(P_i)$. We assert that $q \in R$ if and only if $q \in R_0$. Let $\mathfrak{q}_0 | \mathfrak{q}$ be primes of $K_0|K$ above q. We have $q \in R$ if and only if $\mathfrak{q}$ is unramified in E_τ ($E_\tau \subseteq E^{\langle z_i \rangle}$), and then (obviously) $\mathfrak{q}_0$ is unramified in $E_0 = K_0 E_\tau$ and hence $q \in R_0$. Conversely, suppose that $\mathfrak{q}_0$ is unramified in E_0 ($q \in R_0$). Assume that $q \notin R$; that is, $\mathfrak{q} = \mathfrak{q}_0 \cap K$ is ramified in E_τ. Then $E_\tau = E(i)$ by construction. Moreover then $\mathfrak{q}$ is unramified in $E_{\tau'} = K(\sqrt{\mu_{\tau'}})$ for all $\tau' \neq \tau$ since then $E_{\tau'} \subseteq E^{\langle z_i \rangle}$. As this is a property of the cohomology class ρ, we know $\mathfrak{q}$ is unramified in the fields $K(\sqrt{p_{\tau'} e \mu_{\tau'}})$ generating K_0. Consequently $\mathfrak{q}$ is unramified in K_0, whence splits completely in the Scholz field K_0. It follows that $\mathfrak{q}_0$ must be ramified in E_0. This is the desired contradiction. (The "converse" statement is not true in general; a corresponding argument is missing in [Shafarevich 1954, p. 121].)

Let $\mathfrak{q}_0 | q$ be primes of $K_0 | \mathbb{Q}$ with $q \in R_0$. Then the Frobenius

$$\phi_q = \left(\frac{E_0 | K_0}{\mathfrak{q}_0} \right)$$

is defined, which is a central element in $H_0 = \mathrm{Gal}(E_0 | \mathbb{Q})$ and so depends only on q. Independent of the choice of the square root $\sqrt{\mu_\tau}$ we have

$$(\sqrt{\mu_\tau})^{\phi_q} = \left(\frac{\mu_\tau}{\mathfrak{q}_0} \right) \sqrt{\mu_\tau},$$

where

$$\left(\frac{\mu_\tau}{\mathfrak{q}_0} \right) = \pm 1$$

is the Legendre symbol (quadratic residue symbol). Since

$$\left(\frac{\mu_\tau}{\mathfrak{q}_0} \right) = \left(\frac{\mu_\tau^x}{\mathfrak{q}_0{}^x} \right) = \left(\frac{\beta_x^2 \mu_\tau}{\mathfrak{q}_0{}^x} \right) = \left(\frac{\mu_\tau}{\mathfrak{q}_0{}^x} \right)$$

for each $x \in G_0$, and since q is the absolute norm of $\mathfrak{q}_0$ by (S2), it is appropriate to write this symbol as $\left[\frac{\mu_\tau}{q} \right]$ (like in [Shafarevich 1954]). As usual the Legendre symbol is extended multiplicatively to products of nondyadic primes in the denominator (Jacobi symbol), yielding also certain extensions of the Shafarevich symbol. For an integer $m \neq 0$ the symbol $\left[\frac{m\mu_\tau}{q} \right]$ is defined since R_0 is an invariant of ρ_0, and if m is not divisible by q then

$$\left[\frac{m\mu_\tau}{q} \right] = \left(\frac{m}{q} \right) \left[\frac{\mu_\tau}{q} \right].$$

In this case $\mathfrak{q}_0 | q$ are unramified in $K_0(\sqrt{m}) | \mathbb{Q}(\sqrt{m})$ and

$$\left(\frac{K_0(\sqrt{m}) | K_0}{\mathfrak{q}_0} \right) \quad \text{restricts to} \quad \left(\frac{\mathbb{Q}(\sqrt{m}) | \mathbb{Q}}{(q)} \right)$$

since q is busy in K_0 by (S2). Thus $\left(\frac{m}{q} \right) = \left(\frac{m}{\mathfrak{q}_0} \right)$, and the result follows since evidently

$$\left(\frac{m}{\mathfrak{q}_0} \right) \left(\frac{\mu_\tau}{\mathfrak{q}_0} \right) = \left(\frac{m\mu_\tau}{\mathfrak{q}_0} \right).$$

Let again $q \in \mathrm{Ram}(P_i)$ for some i, and let $q \in R_0$. Using that q is busy in the Scholz field K_0, the restrictions to E_τ of σ_q and of the Frobenius ϕ_q introduced above agree. Therefore

$$(\sqrt{\mu_\tau})^{\sigma_q} = (\sqrt{\mu_\tau})^{\phi_q} = \left[\frac{\mu_\tau}{q} \right] \sqrt{\mu_\tau}.$$

We know that $q \in R \cap \mathrm{Ram}(P_i)$, and this implies that all primes in $\mathrm{Ram}(P_i)$ belong to R and hence to R_0 (see Lemma 4.1). Therefore

$$\left[\frac{\mu_\tau}{b_i} \right] = \prod_{q \in \mathrm{Ram}(P_i)} \left[\frac{\mu_\tau}{q} \right]$$

is defined, and

$$(\sqrt{\mu_\tau})^{\sigma_i} = \left[\frac{\mu_\tau}{b_i}\right]\sqrt{\mu_\tau}.$$

Thus

$$\left[\frac{\mu_\tau}{b_i}\right] = 1$$

by the hypothesis of the proposition.

Recall that e is coprime to the discriminant of K_0 and so not divisible by any prime in R_0. By the Chinese remainder theorem there is an *odd* integer m such that

$$\left(\frac{m}{q}\right) = \left[\frac{e\mu_\tau}{q}\right] = \left(\frac{e}{q}\right)\left[\frac{\mu_\tau}{q}\right]$$

for each $q \in R_0$. Then m is prime to every $q \in R_0$ and

$$\left[\frac{me\mu_\tau}{q}\right] = \left(\frac{m}{q}\right)\left[\frac{e\mu_\tau}{q}\right] = 1.$$

Since $R_0 \subseteq \mathrm{Ram}(K_0) \subseteq 1 + 2^N\mathbb{Z}$ (with $N \geq c \geq 2$), replacing m by $-m$ if necessary, we may assume that $m > 0$. We assert that

$$\left(\frac{b_i}{m}\right) = 1$$

whenever $\mathrm{Ram}(P_i) \subseteq R_0$. By quadratic reciprocity

$$\left(\frac{b_i}{m}\right) = \left(\frac{m}{b_i}\right),$$

because b_i and m are relatively prime positive odd integers and $b_i \in 1 + 2^N\mathbb{Z}$. We have

$$\left(\frac{e}{b_i}\right) = \left(\frac{b_i}{e}\right) = 1$$

since the primes dividing e are in $1 + 2^N\mathbb{Z}$ and split completely in $P_i = \mathbb{Q}(\sqrt{b_i})$. Consequently

$$1 = \prod_{q \in \mathrm{Ram}(P_i)} \left[\frac{me\mu_\tau}{q}\right] = \left[\frac{me\mu_\tau}{b_i}\right] = \left(\frac{m}{b_i}\right)\left(\frac{e}{b_i}\right)\left[\frac{\mu_\tau}{b_i}\right] = \left(\frac{m}{b_i}\right),$$

as required.

Let $T = \prod_{q \in R_0} \mathbb{Q}(\sqrt{q})$. Using that $\mathfrak{S}(T) = T$, $\mathrm{Ram}(\mathbb{Q}(\zeta_{2^N})) = \{2\}$ and $2 \notin R_0 = \mathrm{Ram}(T)$ we get

$$T \cap K_0(\zeta_{2^N}) = \prod_i{}' \mathbb{Q}(\sqrt{b_i}),$$

where the product is taken over those indices i where $\mathrm{Ram}(P_i) \subseteq R_0$. (This is always true when $E_\tau \subseteq E^\perp$, and if $E_\tau = E(i)$ for some i then $\mathrm{Ram}(P_j) \subseteq R_0$ for all $j \neq i$ and $\mathrm{Ram}(P_i) \cap R_0 = \varnothing$.) By construction the Artin automorphism

$$\phi = \left(\frac{T \mid \mathbb{Q}}{(m)}\right)$$

is defined and is trivial on $\prod'_i \mathbb{Q}(\sqrt{b_i})$. Hence ϕ can be extended to an automorphism $\hat{\phi}$ of $T \cdot K_0(\zeta_{2^N})$ which is trivial on $K_0(\zeta_{2^N})$. By Chebotarev's density theorem there are infinitely many rational primes p_τ which are unramified in $T \cdot K_0(\zeta_{2^N})$ and for which some prime above p_τ has $\hat{\phi}$ as Frobenius automorphism. Then p_τ splits completely in $K_0(\zeta_{2^N})$; that is, p_τ splits completely in K_0 and belongs to $1 + 2^N\mathbb{Z}$. Moreover

$$\phi = \left(\frac{T \mid \mathbb{Q}}{(p_\tau)}\right).$$

Thus

$$\left(\frac{q}{p_\tau}\right) = \left(\frac{q}{m}\right)$$

for all $q \in R_0$, in view of the action of ϕ on $\mathbb{Q}(\sqrt{q})$ (and consistency of the Artin symbol). But

$$\left(\frac{q}{p_\tau}\right) = \left(\frac{p_\tau}{q}\right) \quad \text{and} \quad \left(\frac{q}{m}\right) = \left(\frac{m}{q}\right)$$

by quadratic reciprocity. Consequently

$$\left[\frac{p_\tau e \mu_\tau}{q}\right] = \left(\frac{p_\tau}{q}\right)\left[\frac{e\mu_\tau}{q}\right] = \left(\frac{m}{q}\right)\left[\frac{e\mu_\tau}{q}\right] = \left[\frac{me\mu_\tau}{q}\right] = 1.$$

Let $\widehat{E}_0 = K_0(\sqrt{p_\tau e \mu_\tau})$. By the above, every prime in R_0 is busy in $\widehat{E}_0$. From

$$(p_\tau e \mu_\tau) = (e\mathfrak{b})^2 \cdot \mathfrak{D} \cdot (p_\tau)$$

we infer that $\mathrm{Ram}(\widehat{E}_0) = \mathrm{Ram}(K_0) \cup \{p_\tau\}$ (Hecke; 2 does not ramify in $\widehat{E}_0$ as it does not ramify in $E_0 = K_0 E_\tau$ or in $\mathbb{Q}(\sqrt{p_\tau e})$). Consequently $\widehat{E}_0$ is a (strong) Scholz field with respect to N. The proposition follows by induction and by appealing to Lemma 3.3. □

5. The shrinking process

We are going to construct Scholz fields fulfilling the assumptions made in Proposition 4.2. As above we consider disposition 2-groups G_d^c. Arguing by induction on the 2-class c (varying d) this will prove the theorem. For $c = 1$ (or $d = 1$) Lemmas 2.2 and 2.3 apply, in which case we may define the polynomial $f_c = X$. So let $N \geq c \geq 2$ be integers. We assume that for every $d \geq 2$ there are infinitely many strong Scholz fields K_d^{c-1} with respect to N with pairwise coprime discriminants admitting G_d^{c-1} as Galois group over the rationals, all these fields having the property that $|\mathrm{Ram}(K_d^{c-1})| \leq f_{c-1}(d)$ for some (unique) polynomial $f_{c-1} \in \mathbb{Z}[X]$ with $\deg f_{c-1} = (c+2)!/24$.

Fixing $d \geq 2$ we let $\delta = r \cdot d$ where

$$r = 2d^2 \sum_{\kappa=1}^{c} \kappa \cdot \ell_d^\kappa$$

(see Proposition 3.1 for notation). We know that $r = r(d)$ is an integral polynomial in d of degree $c+2$. By our inductive hypothesis there is a strong Scholz field $K_\delta = K_\delta^{c-1}$ with respect to N admitting G_δ^{c-1}

as Galois group over the rationals. Indeed there are infinitely many such fields with pairwise coprime discriminants. By Proposition 2.1 and Lemma 3.3 we can embed K_δ into a normal number field E_δ with group G_δ^c having $\mathrm{Ram}(E_\delta)=\mathrm{Ram}(K_\delta)$. In particular $K_\delta=E_\delta^{Z(G_\delta^c)}$ and

$$\mathfrak{S}(E_\delta)=\mathfrak{S}(K_\delta)=\prod_{j=1}^{r}\prod_{i=1}^{d}P_{ij},$$

where the $\mathrm{Ram}(P_{ij})$ have the same cardinality and are pairwise disjoint. Adapted to this decomposition there is a minimal system $\{x_{ij}\}_{i,j}$ of generators of G_δ^c such that the image $\bar{x}_{ij}$ in $W=G_\delta^c/\Phi(G_\delta^c)$ of x_{ij} generates the image in W of the inertia group I_q in G_δ^c for any $q\in\mathrm{Ram}(P_{ij})$, and $z_{ij}=x_{ij}^{2^{c-1}}$ has order 2 and generates $I_q\cap Z(G_\delta^c)$ (see Lemma 4.1).

For every $q\in\mathrm{Ram}(\mathfrak{S}(E_\delta))$ we choose a Scholz obstruction σ_q for E_δ (determined by q up to adding z_{ij} if $\sigma_q\neq 0$ and $q\in\mathrm{Ram}(P_{ij})$). Define

$$\sigma_{ij}=\sum_{q\in\mathrm{Ram}(P_{ij})}\sigma_q$$

for each pair i,j. Let L_δ^1 be the subspace of $Z(G_\delta^c)$ generated by all the z_{ij}, and let $\psi_\delta^1:W\xrightarrow{\sim}L_\delta^1$ be the linear map given by $\bar{x}_{ij}\mapsto z_{ij}$ for all i,j. By Proposition 3.1 we have the decomposition $Z(G_\delta^c)=\bigoplus_{\kappa=1}^{c}L_\delta^\kappa$ into $\mathbb{F}_2$-vector spaces. We also introduce a "target" disposition 2-group G_d^c of rank d and class c with generators $x_1,\dots,x_d$, yielding the basis $\bar{x}_i=x_i\Phi(G_d^c)$ of $V=G_d^c/\Phi(G_d^c)$, and let L_d^1 be the subspace of $Z(G_d^c)$ generated by the $z_i=x_i^{2^{c-1}}$ $(1\le i\le d)$. Then we have again the vector space decomposition $Z(G_d^c)=\bigoplus_{\kappa=1}^{c}L_d^\kappa$. Let $\psi_d^1:V\xrightarrow{\sim}L_d^1$ be the linear isomorphism given by $\bar{x}_i\mapsto z_i$ for each i, and define the epimorphisms $\psi_\delta^\kappa:W^{\otimes\kappa}\twoheadrightarrow L_\delta^\kappa$ and $\psi_d^\kappa:V^{\otimes\kappa}\twoheadrightarrow L_d^\kappa$ for $2\le\kappa\le c$ as in Proposition 3.1.

Now let $\alpha=(a_j)$ be any nontrivial r-tuple in $\mathbb{F}_2^{(r)}$. We shall also write $\alpha:W\twoheadrightarrow V$ for the (surjective) linear map given by $\alpha(\bar{x}_{ij})=a_j\bar{x}_i$ for all pairs i,j (additive notation). By Lemma 3.2 every lift of α to G_δ^c gives rise to the same epimorphism $\alpha_z:Z(G_\delta^c)\twoheadrightarrow Z(G_d^c)$, and α_z respects the corresponding vector space decompositions. From Proposition 3.1 it follows that $\alpha_z\circ\psi_\delta^\kappa=\psi_d^\kappa\circ\alpha^{\otimes\kappa}$ for each $\kappa=1,\dots,c$ (where $\alpha^{\otimes\kappa}:W^{\otimes\kappa}\twoheadrightarrow V^{\otimes\kappa}$ is the κ-th tensor power of α). In particular $\alpha_z(z_{ij})=a_jz_i$ for all i,j (additive notation).

Though irrelevant for our purposes, but following [Shafarevich 1954], we consider the "canonical" epimorphism $\pi(\alpha):G_\delta^c\twoheadrightarrow G_d^c$ given by mapping x_{ij} onto x_i for all i if $a_j=1$ and to 1 if $a_j=0$. This is a distinguished lift of α to G_δ^c. (Writing $G_\delta^c=F_\delta/\lambda_{c+1}(F_\delta)$ and letting $\{t_{ij}\}$ be a basis of the free group, there is an automorphism of G_δ^c sending x_{ij} to $t_{ij}\lambda_{c+1}(F_\delta)$ for all i,j. Then $\pi(\alpha)$ is given via the assignments $t_{ij}\mapsto x_i$ if $a_j=1$ and $t_{ij}\mapsto 1$ otherwise.) Let

$$E(\alpha)=E_\delta^{\mathrm{Ker}(\pi(\alpha))}\quad\text{and}\quad K(\alpha)=E(\alpha)\cap K_\delta.$$

Obviously $K(\alpha)$ is a Scholz field with respect to N; condition (S2) might fail for the field $E(\alpha)$.

It is convenient to identify $\mathrm{Gal}(E(\alpha)\,|\,\mathbb{Q})$ with G^c_d through the isomorphism induced by $\pi(\alpha)$. Then every element of G^c_δ is sent by $\pi(\alpha)$ to its restriction on $E(\alpha)$. In particular $K(\alpha) = E(\alpha)^{Z(G^c_d)}$ since $K_\delta = E_\delta^{Z(G^c_\delta)}$ and $\pi(\alpha)$ (resp. α_z) maps $Z(G^c_\delta)$ onto $Z(G^c_d)$. It follows that $\mathrm{Gal}(K(\alpha)\,|\,\mathbb{Q}) \cong G^{c-1}_d$ and that $\mathfrak{S}(K(\alpha)) = \mathfrak{S}(E(\alpha))$.

If there is a prime $q \in \mathrm{Ram}(E(\alpha)) \setminus \mathrm{Ram}(K(\alpha))$, then $q \in \mathrm{Ram}(K_\delta) \subseteq 1 + 2^N\mathbb{Z}$ and q is busy in the Scholz field K_δ. It follows that q splits completely in $K(\alpha)$ (being busy and unramified). In particular q splits completely in $\mathfrak{S}(K(\alpha))$.

We have $\mathfrak{S}(E(\alpha)) = E(\alpha) \cap \mathfrak{S}(E_\delta)$ since $\pi(\alpha)(\Phi(G^c_\delta)) = \Phi(G^c_d)$. For each $i = 1, \ldots, d$ we let

$$P_i(\alpha) = E(\alpha) \cap \prod_{j=1}^{r} P_{ij}.$$

If I_q is the inertia group in G^c_δ for some $q \in \mathrm{Ram}(P_{ij})$, then $\pi(\alpha)(I_q)$ maps onto $\langle \bar{x}_i \rangle$ if $a_j = 1$ (which exists) and $\pi(a)(I_q) \subseteq \Phi(G^c_d)$ otherwise. So $P_i(\alpha)$ is the (cyclic) subfield of $\mathfrak{S}(E(\alpha))$ fixed (centralized) by all $\bar{x}_{i'}$ for $i' \neq i$ (but not by $\bar{x}_i$), and $\mathrm{Ram}(P_i(\alpha)) = \biguplus'_j \mathrm{Ram}(P_{ij})$, where j varies over the indices in $\{1, \ldots, r\}$ for which $a_j = 1$. Hence we have

$$\mathfrak{S}(K(\alpha)) = \mathfrak{S}(E(\alpha)) = P_1(\alpha) \cdots P_d(\alpha),$$

and we infer that $K(\alpha)$ is *strongly* Scholz.

Let $q \in \mathrm{Ram}(P_i(\alpha))$ for some i. Then $q \in \mathrm{Ram}(P_{ij})$ for a unique j, and $\alpha_z(z_{ij}) = a_j z_i = z_i$. Every prime $\mathfrak{q}$ of K_δ above q is unramified in $E_\delta^{\langle z_{ij} \rangle}$, and $\mathfrak{q}_\alpha = \mathfrak{q} \cap K(\alpha)$ is unramified in $E(\alpha)^{\langle z_i \rangle} = E(\alpha) \cap E_\delta^{\langle z_{ij} \rangle}$. The restriction of

$$\left(\frac{E_\delta^{\langle z_{ij} \rangle} \,|\, K_\delta}{\mathfrak{q}} \right)$$

to $E(\alpha)^{\langle z_i \rangle}$ agrees with

$$\left(\frac{E(\alpha)^{\langle z_i \rangle} \,|\, K(\alpha)}{\mathfrak{q}_a} \right)$$

as q is busy in K_δ. Hence $\alpha_z(\sigma_q)$ may be identified with "the" Scholz obstruction for $E(\alpha)$ associated to q. We have

$$\sum_{q \in \mathrm{Ram}(P_i(\alpha))} \alpha_z(\sigma_q) = \sum_j{}' \alpha_z(\sigma_{ij}),$$

where the sum is taken over all j for which $a_j = 1$.

Consider $Z(G^c_\delta) \otimes L^1_\delta = \bigoplus_{\kappa=1}^{c} (L^\kappa_\delta \otimes L^1_\delta)$. Let α^κ_z denote the restriction to L^κ_δ of α_z. The map $\alpha_z \otimes \alpha^1_z : Z(G^c_\delta) \otimes L^1_\delta \to Z(G^c_d) \otimes L^1_d$ respects the corresponding decompositions, and the diagram

$$\begin{array}{ccc}
V^{\otimes\kappa} \otimes V & \xleftarrow{\;\alpha^{\otimes\kappa} \otimes \alpha\;} & W^{\otimes\kappa} \otimes W \\
\Big\downarrow{\scriptstyle \psi^\kappa_d \otimes \psi^1_d} & & \Big\downarrow{\scriptstyle \psi^\kappa_\delta \otimes \psi^1_\delta} \\
L^\kappa_d \otimes L^1_d & \xleftarrow[\;\alpha^\kappa_z \otimes \alpha^1_z\;]{} & L^\kappa_\delta \otimes L^1_\delta
\end{array}$$

commutes for each κ. All maps in this square are surjections. On the obvious bases of $W^{\otimes\kappa+1}$ and $V^{\otimes\kappa+1}$ we have

$$\alpha^{\otimes\kappa+1}(\bar{x}_{i_1,j_1}\otimes\cdots\otimes\bar{x}_{i_{\kappa+1},j_{\kappa+1}})=(\bar{x}_{i_1}\otimes\cdots\otimes\bar{x}_{i_{\kappa+1}})a_{j_1}\cdots a_{j_{\kappa+1}}.$$

Let $z\in Z(G_\delta^c)\otimes L_\delta^1$ with κ-component $z^\kappa\in L_\delta^\kappa\otimes L_\delta^1$, and let $\widehat{z^\kappa}\in W^{\otimes\kappa}\otimes W$ be an inverse image of z^κ with regard to $\psi_\delta^\kappa\otimes\psi_\delta^1$. Given a nontrivial linear form $\chi\in\operatorname{Hom}(L_d^\kappa\otimes L_d^1,\mathbb{F}_2)$, the element $\chi\circ(\psi_d^\kappa\otimes\psi_d^1)\circ\alpha^{\otimes\kappa+1}(\widehat{z^\kappa})$ may be interpreted as evaluation at (a_j) of some homogeneous polynomial of degree $\kappa+1$ in r variables over $\mathbb{F}_2$ determined by $\widehat{z^\kappa}$ and χ. But $(\psi_d^\kappa\otimes\psi_d^1)\circ\alpha^{\otimes\kappa+1}(\widehat{z^\kappa})=(\alpha_z^\kappa\otimes\alpha_z^1)(z^\kappa)$ and so this evaluation only relies on z^κ (and on χ). Hence we may state that $\chi\circ(\alpha_z^\kappa\otimes\alpha_z^1)(z^\kappa)=0$ if (a_j) is a (nontrivial) zero of a certain homogeneous polynomial of degree $\kappa+1$ in r variables over $\mathbb{F}_2$. Varying χ over a basis for $\operatorname{Hom}(L_d^\kappa\otimes L_d^1,\mathbb{F}_2)$ we obtain that $(\alpha_z^\kappa\otimes\alpha_z^1)(z^\kappa)=0$ if (a_j) is a common zero of $\ell_d^\kappa\cdot d$ such polynomials, and we get $(\alpha_z\otimes\alpha_z^1)(z)=0$ if (a_j) is a common zero of $d\sum_{\kappa=1}^c\ell_d^\kappa$ such homogeneous polynomials in r variables over $\mathbb{F}_2$ of respective degrees $\kappa+1=2,\dots,c+1$.

Now consider for each $i=1,\dots,d$ the element $z(i)=\sum_{j=1}^r\sigma_{ij}\otimes z_{ij}$ of $Z(G_\delta^c)\otimes L_\delta^1$. Since by definition $r>d^2\sum_{\kappa=1}^c(\kappa+1)\cdot\ell_d^\kappa$, the Chevalley–Warning theorem guarantees that we may choose $\alpha=(a_j)$ nontrivial in $\mathbb{F}_2^{(r)}$ such that $(\alpha_z\otimes\alpha_z^1)(z(i))=0$ for all i. We have

$$(\alpha_z\otimes\alpha_z^1)(z(i))=\sum_{j=1}^r\alpha_z(\sigma_{ij})\otimes\alpha_z(z_{ij})=\sum_{j=1}^r\alpha_z(\sigma_{ij})\otimes a_jz_i=\Bigg(\sum_{q\in\operatorname{Ram}(P_i(\alpha))}\alpha_z(\sigma_q)\Bigg)\otimes z_i.$$

Hence $\sum_{q\in\operatorname{Ram}(P_i(\alpha))}\alpha_z(\sigma_q)=0$ for all $i=1,\dots,d$, so that Proposition 4.2 applies. Consequently there is a strong Scholz field E with respect to N containing $K(\alpha)=E(\alpha)\cap K_\delta$ and admitting G_d^c as Galois group over the rationals. We also get

$$\operatorname{Ram}(E)=\operatorname{Ram}(K(\alpha))\cup\{p_1,\dots,p_t\},$$

where $t=\dim Z(G_d^c)=\sum_{\kappa=1}^c\ell_d^\kappa$. Here the t-set $\{p_1,\dots,p_t\}$ of rational primes may be chosen in infinitely many pairwise disjoint ways.

By induction $|\operatorname{Ram}(E_\delta)|=|\operatorname{Ram}(K_\delta)|\le f_{c-1}(\delta)$. Define f_c such that $f_c(d)=f_{c-1}(\delta)+\sum_{\kappa=1}^c\kappa\cdot\ell_d^\kappa$. Then $|\operatorname{Ram}(E)|\le f_c(d)$. Since $\delta=rd$ is an integral polynomial in d of degree $c+3$, this f_c is an integral polynomial of degree $(c+3)\deg f_{c-1}=(c+3)!/24$. This completes the proof of the theorem.

Acknowledgements

I owe special thanks to J.-P. Serre for some revealing discussions on the inverse problem of Galois theory for nilpotent (and for solvable) groups. I am also indebted to the referee for some valuable comments.

References

[Fröhlich 1983] A. Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemp. Math. **24**, Amer. Math. Soc., Providence, RI, 1983. MR Zbl

[Geyer and Jarden 1998] W.-D. Geyer and M. Jarden, "Bounded realization of l-groups over global fields: the method of Scholz and Reichardt", *Nagoya Math. J.* **150** (1998), 13–62. MR Zbl

[Hecke 1981] E. Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Math. **77**, Springer, 1981. MR Zbl

[Kisilevsky et al. 2010] H. Kisilevsky, D. Neftin, and J. Sonn, "On the minimal ramification problem for semiabelian groups", *Algebra Number Theory* **4**:8 (2010), 1077–1090. MR Zbl

[Meshulam and Sonn 1999] R. Meshulam and J. Sonn, "A quantitative version of a lemma of Shafarevich–Ishkhanov", *Comm. Algebra* **27**:3 (1999), 1255–1259. MR Zbl

[Neukirch et al. 2000] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der Math. Wissenschaften **323**, Springer, 2000. MR Zbl

[Plans 2004] B. Plans, "On the minimal number of ramified primes in some solvable extensions of $\mathbb{Q}$", *Pacific J. Math.* **215**:2 (2004), 381–391. MR Zbl

[Rabayev 2013] D. Rabayev, *Upper bound on the minimal number of ramified primes for solvable groups over the rationals*, Ph.D. thesis, Technion-Israel Institute of Technology, 2013.

[Reichardt 1937] H. Reichardt, "Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung", *J. Reine Angew. Math.* **177** (1937), 1–5. MR Zbl

[Schmid 2014] P. Schmid, "On 2-extensions of the rationals with restricted ramification", *Acta Arith.* **163**:2 (2014), 111–125. MR Zbl

[Schmid 2017] P. Schmid, "Disposition p-groups", *Arch. Math.* (*Basel*) **108**:2 (2017), 113–121. MR Zbl

[Scholz 1937] A. Scholz, "Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung, I", *Math. Z.* **42**:1 (1937), 161–188. MR Zbl

[Serre 1992] J.-P. Serre, *Topics in Galois theory*, Research Notes in Math. **1**, Jones and Bartlett, Boston, 1992. MR Zbl

[Shafarevich 1954] I. R. Shafarevich, "On the construction of fields with a given Galois group of order l^{α}", *Izv. Akad. Nauk SSSR Ser. Mat.* **18**:3 (1954), 261–296. In Russian; translated in *Amer. Math. Soc. Trans.* (2) 4 (1956), 107–142. Zbl

[Shafarevich 1989] I. R. Shafarevich, "Factors of a descending central series", *Mat. Zametki* **45**:3 (1989), 114–117. In Russian; translated in *Math. Notes* **45**:3 (1989), 262–264. MR Zbl

[Weil 1967] A. Weil, *Basic number theory*, Grundlehren der Math. Wissenschaften **144**, Springer, 1967. MR Zbl

Communicated by Pham Huu Tiep
Received 2017-07-26 Revised 2018-07-21 Accepted 2018-08-26

peter.schmid@uni-tuebingen.de *Mathematisches Institut, Universität Tübingen, Tübingen, Germany*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2018 is US $340/year for the electronic version, and $535/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 12 No. 10 2018