ALBANIAN JOURNAL OF MATHEMATICS
Volume 17, Number 2, Pages 81–92
ISSN: 1930-1235; (**2023**)

FIELDS OF DEFINITION FOR ADMISSIBLE GROUPS

DANNY NEFTIN

Deptartment of Mathematics,
Technion-Israel Institute of Technology,
Haifa 32000, Israel

UZI VISHNE

Department of Mathematics,
Bar Ilan University,
Ramat Gan 52900, Israel

ABSTRACT. A finite group G is called admissible over a field M if it is realizable as the Galois group of an extension of M which is contained in a division algebra with center M. We consider the extent to which admissibility over M implies admissibility over a subfield $K \subset M$, comparing variations where the division algebra, the extension field, or the Galois extension, are asserted to be defined over K. We completely determine the logical implications between the variants.

MSC 2020: Primary 11R04, 11B39, Secondary 11R09, 12F05
KEYWORDS: Admissible group; adequate field; admissibility over a subfield; tame admissibility.

1. INTRODUCTION

A group G is **admissible** over a number field M if it appears as the Galois group of a field extension of M which is contained in a finite dimensional division algebra with center M, that is, an M-central division algebra [19, Proposition 2.2].

E-mail addresses: `dneftin@technion.ac.il, vishne@math.biu.ac.il`.

The first author is grateful for the support of Israel Science Foundation (grants no. 577/15 and 353/21) and the hospitality of the Institute for Advanced Study. The second author was partially supported by the U.S.-Israel Binational Science Foundation (grant no. 2010/149) and the Israel Science Foundation (grant no. 1994/20).

This notion was introduced in the 60's in connection with (explicit) crossed product constructions of division algebras: Indeed, G is M-admissible if and only if there exists an M-central division algebra D which is a G-crossed product, that is, D has a maximal subfield L which is Galois over M with group G, see [19].

One of the longstanding open problems of inverse Galois nature is to ascertain which groups G are admissible over a given field M, cf. [2, §11.A]. This question has been extensively studied over number fields [9, 11, 22], and other fields [7, 15].

Notably, in these works, admissibility over M is related to admissibility over subfields K of M. Namely, for appropriate fields K and M, it is shown that if G is M-admissible, then there exists a G-crossed product division algebra D_0 over K, whose restriction to M is a (G-crossed product) division algebra D. In such a case, we say that the crossed product D is defined over K.

It therefore makes sense to ask, for a given extension M/K and an M-admissible group G, to which extent the M-admissibility of G can be realized over K. The existence of a G-crossed product over M which is defined over K is the strongest descent condition to require. Failing this strong condition, it is still possible that some part of the structure exists over K. For example, it is possible that G is both K- and M-admissible; that the division algebra D is defined over K (namely, $D = D_0 \otimes_K M$ for a suitable division algebra over K); that L is defined and is Galois over K (namely, $L = L_0 \otimes_K M$ where L_0/K is a G-extension); or that L is merely defined over K and becomes Galois after the extension.

This paper studies eight variations of M-admissibility of a group G with respect to a fixed number field extension M/K. Furthermore, these variants are considered when admissibility is assumed to be tame, that is, when the tamely ramified part of each of the completions of the extension L/M splits D, see Section 3.1. These variants are defined in Section 2.1, and their tame versions are analogously defined in Section 3.2.

We first show that these eight tame variants are all equivalent for solvable groups G, and that they all hold if G is a cyclic group, see Corollary 3.6 and Proposition 3.7, respectively. However, when admissibility is not assumed to be tame, we show that only the trivial implications between the variants hold, see Theorem 2.2. In Section 4 we provide counterexamples to every implication which is not proved in Section 2.2, with G being a p-group and M a number field. The difference from tame admissibility is an essential ingredient in the construction of counterexamples.

A ninth condition, where the maximal subfield L is required merely to be Galois over K, comes from the study of noncrossed products over Henselian fields: If E is a tame division algebra over a Henselian field F such that K is the residue field $\overline{F}$ and M is the center of $D := \overline{E}$, then E is a crossed product for some group if and only if D contains a maximal subfield $L \supseteq M$ that is Galois over K, by a generalization of Brussel's criterion, see [8]. Moreover, the latter criterion shows that E is a crossed product for a group that is built from the Galois group of L/K, indicating that the condition is also applicable to the question of rigidity of division algebras, that is, determining the existence of a division algebra over F which is a crossed product with respect to G and no other group. The relation of the ninth condition to the implication diagram for the eight variations is determined in Section 5.

Finally, we remark that other noncommutative variants of the inverse Galois problem were recently considered in [1, 4, 5], where one considers automorphisms of the division algebras themselves. Also note that generic G-crossed products over K give another approach to comparing the nine conditions for G as they admit every G-crossed product over K and over M as a specialization, see [6].

2. Conditions on the field of definition and the main theorem

Let K be a field and G a finite group. We say that a field L is **K-adequate** if it is a maximal subfield in some division algebra whose center is K. For a finite dimensional K-central simple algebra A, denote by $\text{ind}_K(A)$ the index of A, that is, $\sqrt{\dim_K D}$ where D is a division algebra[1] such that A is a matrix algebra over D. We repeatedly use the following well-known characterization of maximal subfields of K-central simple algebras A: an extension field $L \supseteq K$ embeds as a maximal subfield of A if and only if it splits A and its degree $[L : K]$ is the index $\text{ind}_K(A)$ of A. We say that L is a **G-extension** of K if L/K is a Galois extension with Galois group $\text{Gal}(L/K) \cong G$.

2.1. **The eight variations.** We present eight variations on admissibility over M with respect to a subfield $K \subseteq M$.

Let M/K be a finite field extension. One way to study the condition

(1) G is M-admissible

is by refining it to require that the crossed-product division algebra or its maximal subfield are defined over K (we say that a field or an algebra over M is **defined over** K if it is obtained by scalar extension from K to M).

Condition (1) requires the existence of an M-adequate G-extension L/M. Two ways in which L can be related to K provide the following variants:

(2) there exists an M-adequate G-extension L/M for which L is defined over K; *or*

(3) there exists an M-adequate G-extension L/M so that $L = L_0 \otimes M$ for some field L_0 for which $\text{Gal}(L_0/K) \cong G$.

For the algebra D to be defined over K, we may require that:

(4) there exists a K-division algebra D_0 and a G-extension L/M for which L is a maximal subfield of $D = D_0 \otimes M$; *or*

(5) there exists a K-division algebra D_0 and a maximal subfield L_0 which is a G-extension of K so that $L_0 \cap M = K$ and $L = L_0 M$ is a maximal subfield of the division algebra $D = D_0 \otimes M$.

If $L = L_0 \otimes_K M$, the interaction between L_0 and L may involve the division algebras:

(6) there exists a K-adequate G-extension L_0/K for which $L_0 M$ is an M-adequate G-extension; *or*

(7) there exists a K-adequate extension L_0/K for which $L_0 M$ is an M-adequate G-extension.

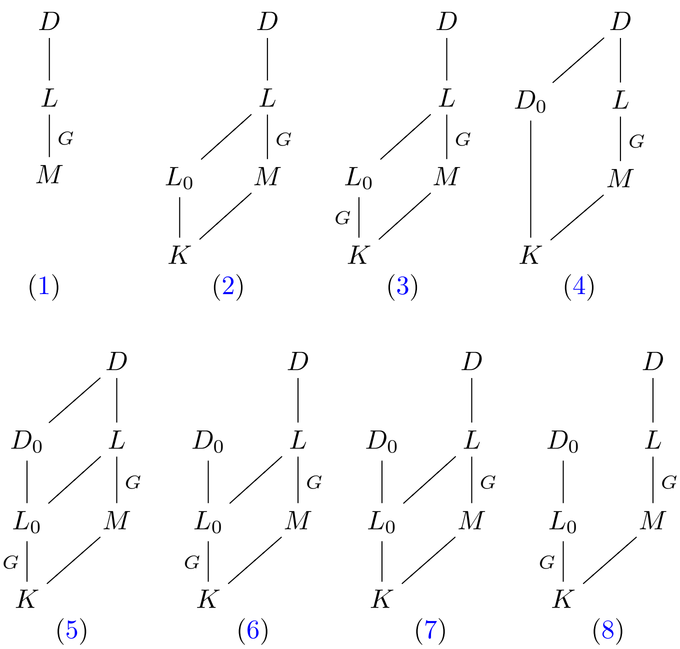
Finally, we have the double condition

(8) G is both K-admissible and M-admissible.

We provide a diagrammatic description of each condition, for easy reference. Inclusion is denoted by a vertical line, and diagonal lines show the extension of scalars from K to M. A vertical line decorated by G represents a G-extension.

[1] Such a division algebra must exist by Wedderburn's theorem.

Note that the fact that the extension L_0/K is Galois implies that L/M is Galois as well, with the same Galois group (this influences cases (3), (5) and (6)).

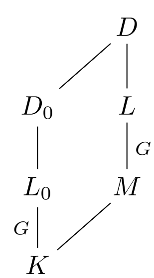


We say that a triple (K, M, G) satisfies Condition (m) if there are L_0, L, D_0 and D as required in this condition. In such case we also say (L_0, L, D_0, D) realizes Condition (m), omitting L_0 or D_0 if they are not used.

Remark 2.1. Let M/K be a finite extension of fields and G a finite group. One might also consider the condition

($5'$) there exists a G-crossed product K-division algebra D_0, for which $D = D_0 \otimes M$ is also a G-crossed product division algebra.

In the spirit of previous diagrams, this condition is described by



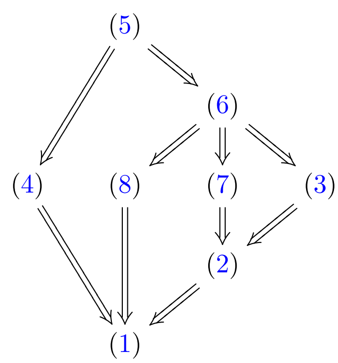
This is similar to (5), but in case ($5'$) we do not assume explicitly a relation between the maximal subfields of D_0 and those of D. However, ($5'$) is equivalent to Condition (5). Indeed, suppose that (L_0, L, D_0, D) realizes ($5'$). Then D is of index $|G|$ and D is also split by $L' = ML_0$. Therefore $[L' : M] = |G|$, $L_0 \cap M = K$ and hence we can take L' to be the required maximal G-subfield of D. Thus, (L_0, L', D_0, D) realizes (5). The converse implication is obvious, taking $L = L_0 \otimes_K M \subset D_0 \otimes_K M = D$.

2.2. **The logical implications.** The following theorem describes the relation between the eight variants:

Theorem 2.2. *Of the eight conditions in Subsection 2.1, (m) implies (n) for all finite extensions M/K and finite groups G, if and only if the diagram of (n) can be obtained from the diagram of (m) by removal of lines and decorations.*

More explicitly, the implications in Diagram 2.1 always hold, and every other implication fails for some extension of number fields and some finite p-group:

(2.1)



Proof of positive part of Theorem 2.2.

(5) $\implies$ (4)+(6): Fix K, M, and G. Clearly, if (L_0, L, D_0, D) realizes Condition (5), then (L_0, L, D_0, D) also realizes (6), and (L, D_0, D) realizes (4).

(6) $\implies$ (3) + (8) + (7): If (L_0, L, D_0, D) realizes (6), then L_0/K is a G-extension and hence $L = L_0M/M$ is also a G-extension (since $L_0 \cap M = K$). Thus, (L_0, L, D_0, D) realizes (7). It is clear that L_0 is a field of definition of L (and $\mathrm{Gal}(L_0/K) = G$) and therefore (L_0, L, D) realizes (3). As L_0 is a K-adequate G-extension and L is an M-adequate G-extension, (L_0, L, D_0, D) realizes (8).

(3) $\implies$ (2): If (L_0, L, D) realizes Condition (3) then $\mathrm{Gal}(L_0/K) \cong G$, $\mathrm{Gal}(L/M) \cong G$ (since $L_0 \cap M = K$) and hence (L_0, L, D_0, D) realizes Condition (2).

(7) $\implies$ (2): If (L_0, L, D_0, D) realizes Condition (7), clearly L_0 is a field of definition of L. Thus, hence (L_0, L, D) realizes Condition (2).

Finally, when (K, M, G) satisfies either of the Conditions (2), (4), (8) we have that G is M-admissible, and hence each of (2), (4), (8) implies (1). □

In Section 4 we provide counterexamples to all the implications which were not proved here, thus showing that the diagram in Theorem 2.2 depicts the precise logical interaction between the eight conditions.

3. Tame admissibility and cyclic groups

3.1. **Background.** Let K be a number field. For a prime v of K, we denote by K_v the completion of K with respect to v. If L/K is a finite Galois extension, L_v denotes the completion of L with respect to some prime of L dividing v. Further identify $\mathrm{Gal}(L_v/K_v)$ with a subgroup of $\mathrm{Gal}(L/K)$ up to conjugacy. For t prime to n, let $\sigma_{t,n}$ be the automorphism of $\mathbb{Q}(\mu_n)/\mathbb{Q}$ defined by $\sigma_{t,n}(\zeta) = \zeta^t$ for $\zeta \in \mu_n$.

The basic criterion for admissibility over number fields is due to Schacher [19]:

Theorem 3.1. *Let K be a number field and G a finite group. Then G is K-admissible if and only if there exists a Galois G-extension L/K such that, for every* *rational prime p dividing $|G|$, there is a pair of primes v_1, v_2 of K such that each of the subgroups* $\mathrm{Gal}(L_{v_i}/K_{v_i})$ *contains a p-Sylow subgroup of G.*

We say that a finite extension L/K is **tamely K-adequate** if L is a maximal subfield of a K-central division algebra D that is split by L *tamely*, that is, the maximal tamely ramified subextension of L_v/K_v splits $D \otimes_K K_v$, for every place v of K. Likewise, a finite group G is **tamely K-admissible** if there exists a tamely K-adequate G-extension L/K.

It follows from [12] (see also [13, Corollary 2.1.7]) that tamely K-admissible groups G have metacyclic p-Sylow subgroups that satisfy the following condition for every prime divisor p of $|G|$:

Definition 3.2. We say that a metacyclic p-group G satisfies **Liedahl's condition** (first defined in [12]) with respect to K, if it has a presentation

$$G = \langle x, y \mid x^m = y^i,\ y^n = 1,\ x^{-1}yx = y^t \rangle \tag{3.1}$$

such that $\sigma_{t,n}$ fixes $K \cap \mathbb{Q}(\mu_n)$.

As a direct consequence of [10, Lemma 2.1] and Chebutarev's density theorem, we note that a metacyclic p-group satisfies Liedahl's condition over K if and only if it is realizable over infinitely many completions of K.

There are no known examples of groups whose Sylow subgroup satisfy Liedahl's condition but are not K-admissible. In particular, the following is shown in [12, Theorem 30] for G a p-group, and in [14, Theorem 1.3] for G solvable.

Theorem 3.3. *Let K be a number field and G a solvable group whose Sylow subgroups satisfy Liedahl's condition over K. Then G is tamely K-admissible.*

As a direct corollary of the theorem and [12, Theorem 28], one has:

Corollary 3.4. *Let G be a solvable group such that the rational prime divisors of $|G|$ do not decompose in K. Then G is K-admissible if and only if its Sylow subgroups are metacyclic and satisfy Liedhal's condition.*

Remark 3.5. In fact the proof of [14, Theorem 1.3] shows that there exists a G-extension $L_0/\mathbb{Q}$ and a $\mathbb{Q}$-central division algebra D_0 such that D_0 is split by L_0 tamely; L_0 is a maximal subfield of D_0; and $D := D_0 \otimes_{\mathbb{Q}} K$ is a division algebra.

3.2. **Fields of definition for tame admissibility.** Conditions (1)-(8) of Section 2 can also be considered with respect to tame K-admissibility. Let G be a solvable group and K, M number fields. For $m = 1, \dots, 8$, let (m^*) denote the condition (m), where every adequate extension is assumed to be tamely adequate, and an admissible group is assumed tamely admissible. More precisely for $m = 4, 5$ we consider

- (4^*) there exists a K-division algebra D_0 and a G-extension L/M for which $D = D_0 \otimes_K M$ is split by L tamely, and L is a maximal subfield of D,

and

- (5^*) there exists a K-division algebra D_0 and a maximal subfield L_0 which is a G-extension of K which splits D_0 tamely and satisfies $L_0 \cap M = K$, so that $L = L_0 M$ is a maximal subfield of $D = D_0 \otimes M$ (splitting it tamely).

As a consequence of Theorem 3.3 and Remark 3.5 we have:

Corollary 3.6. *Let G be a solvable group and M/K a finite extension of number fields. Then the conditions* (1^*)–(8^*) *are all equivalent.*

Proof. With the added conditions the implications given in (2.1) clearly holds. We show that the implication $(1^*) \Rightarrow (5^*)$ also holds and hence the conditions are all equivalent.

Assume G is tamely M-admissible. By Theorem 3.3 and Remark 3.5, there exists $\mathbb{Q}$-central division algebra D_0 and a G-extension $N_0/\mathbb{Q}$ such that N_0 is a maximal subfield of D_0 which splits D_0 tamely and such that $D = D_0 \otimes_{\mathbb{Q}} M$ is a division algebra. It follows that $L_0 := N_0 \otimes_{\mathbb{Q}} K$ and $L := N_0 \otimes_{\mathbb{Q}} M$ are fields, and hence are G-extensions of K and M which are maximal subfields of $D_0 \otimes K$ and D, respectively. Since N_0 splits D_0 tamely, L splits D tamely, so that (5^*) holds. □

3.3. **Cyclic extensions.** We now show the conditions hold for cyclic groups. The proof is based on the Albert–Brauer-Hasse-Noether (ABHN) theorem. To a K-central division algebra D over a number field K, the ABHN theorem associates invariants $\mathrm{inv}_v(D) \in \mathbb{Q}/\mathbb{Z}$ for every finite place v of K such that all but finitely many invariants are zero. If $D \otimes_K K_v$ is split at the infinite places v, the sum of all invariants at finite primes is zero. Conversely, given a sequence $\alpha_v \in \mathbb{Q}/\mathbb{Z}$, where v runs over primes of K and all but finitely many α_v's are zero, there exists a unique division algebra D with $\mathrm{inv}_v(D) = \alpha_v$ for every prime v such that D is split at the infinite primes. Moreover, for a finite extension M/K, one has $\mathrm{inv}_w(D \otimes_{K_v} M_w) = [M_w : K_v] \cdot \mathrm{inv}_v(D)$, for every prime w of M lying over v. In particular, for D that splits at the infinite primes, $\mathrm{ind}_K(D \otimes_K K_v)$ is the order of $\mathrm{inv}_v(D) \in \mathbb{Q}/\mathbb{Z}$, and $\mathrm{ind}_K(D)$ is the least common multiple of orders of $\mathrm{inv}_v(D)$, where v runs over all finite primes of K.

Proposition 3.7. *Let G be a cyclic group. Then Conditions (1)–(8) are satisfied for every extension of number fields M/K.*

Proof. It suffices to show that (5^*) is satisfied. By Chebutarev's density theorem (applied to the Galois closure of M/K) there are infinitely many primes v of K that split completely in M. Let v_1, v_2 be two such primes that do not divide $2|G|$. By the weak version (prescribing degrees and not local extensions) of the Grunwald-Wang Theorem (see [23, Corollary 2] or [3, Chapter 10]), there exists a G-extension L_0/K for which $[(L_0)_{v_i} : K_{v_i}] = |G|$. By ABHN, there exists a K-central division algebra D_0 with invariants $\pm 1/|G|$ at v_1 and v_2 which is split at any other prime. By our choice of L_0, it has full local degrees at v_1, v_2 and hence splits D_0. Moreover, $[L_0 : K] = |G| = \mathrm{ind}(D_0)$, so that L_0 is K-adequate. As v_1 and v_2 split completely in M, the compositum $L := L_0 M$ has local degrees $[L_{v_i} : M_{v_i}] = |G|$ for $i = 1, 2$. Moreover, $\mathrm{ind}(D_0 \otimes M_{w_i}) = |G|$ so that $D = D_0 \otimes M$ is of index $|G|$ and hence is a division algebra. Moreover, since D has nontrivial invariants only over the primes dividing v_1 and v_2, and since the latter are coprime to $|G|$, the field L splits D tamely. Thus L is tamely M-adequate and (K, M, G) satisfies (5^*). □

We mention in this context the 'linear disjointness' (LD) of number fields, as defined and established in [17, Prop. 2.7]: for every finite extension M/K in characteristic 0, every central simple algebra over K contains a maximal separable subfield P that is linearly disjoint from M over K. This notion can be bypassed by appealing to the Chebutarev density, as above.

4. Examples

In this section we give counterexamples to all the implications not claimed in Theorem 2.2. In all the examples, K is a number field and G is a p-group. This shows that Diagram 2.1 describes all the correct implications even for p-groups. We repeatedly use the ABHN theorem, see §3.3.

Let us first show that neither one of the Conditions (4) or (8) imply any other condition except (1). For this, by the implication Diagram 2.1, it suffices to show that (4) $\not\Rightarrow$ (8), (8) $\not\Rightarrow$ (4), (4) $\not\Rightarrow$ (2) and that (8) $\not\Rightarrow$ (2). We will show that (8) $\not\Rightarrow$ (4) by demonstrating that (6) $\not\Rightarrow$ (4). In fact an example for (6) $\not\Rightarrow$ (4) will show that no other condition, except (5), implies Condition (4). To complete the proof we should also prove (7) $\not\Rightarrow$ (8), (7) $\not\Rightarrow$ (3), (3) $\not\Rightarrow$ (8) and (3) $\not\Rightarrow$ (7).

The first example relies on:

Remark 4.1. If F_1 and F_2 are field extensions of F such that $L = F_1 \otimes_F F_2$ is a field, and F_1/F and L/F_1 are Galois, then L is Galois over F.

Example 4.2 ((4) $\not\Rightarrow$ (2), (8) $\not\Rightarrow$ (2)). Let $p \equiv 1 \pmod 4$, $G = (\mathbb{Z}/p\mathbb{Z})^3$ and $K = \mathbb{Q}(\sqrt{-1}, \sqrt{p})$. Note that p splits in K. Denote the prime divisors of p in K by v_1, v_2.

Let $\overline{K_{v_i}(p)}^{\mathrm{ab}}$ be the maximal abelian pro-p extension of K_{v_i}. By local class field theory the Galois group $\mathrm{Gal}(\overline{K_{v_i}(p)}^{\mathrm{ab}}/K_{v_i})$ is isomorphic to the pro-p completion of the multiplicative group $K_{v_i}^\times$ which is $\mathbb{Z}_p^n$ where $n = [K_{v_i} : \mathbb{Q}_p] + 1 = 3$, see [21, Chp. 14, §6].

Since $K_{v_1} = K_{v_2} = \mathbb{Q}_p(\sqrt{p})$ this shows that G is realizable over K_{v_1}, K_{v_2}. By the Grunwald-Wang Theorem there exists a $(\mathbb{Z}/p^2\mathbb{Z})^3$-extension $\hat{M}/K$ such that $\hat{M}_{v_i}$ is the maximal abelian extension of exponent p^2 of K_{v_i}, namely the unique $(\mathbb{Z}/p^2\mathbb{Z})^3$-extension of K_{v_i}. Let $M = \hat{M}^G$, so that $\mathrm{Gal}(M/K) \cong G$.

Since $\hat{M}/M$ and M/K both have full local degrees at v_1, v_2, both are adequate G-extensions as maximal subfields of division algebras with invariants $\pm 1/|G|$ at v_1 and v_2 and 0 elsewhere. By choosing $L = \hat{M}$ and $L_0 = M$, we deduce that (K, M, G) satisfies Condition (8). To show that (K, M, G) satisfies (4) it suffices to notice that v_1, v_2 have unique prime divisors w_1, w_2 in M. Thus every division algebra D whose invariants are zero outside $\{w_1, w_2\}$ is defined over K by a K-central division algebra D_0 whose invariants are zero outside $\{v_1, v_2\}$, see the description of invariants in finite extensions in §3.3. Take D with

$$\mathrm{inv}_{w_1}(D) = \frac{1}{p^3}, \quad \mathrm{inv}_{w_2}(D) = -\frac{1}{p^3}$$

and $\mathrm{inv}_w(D) = 0$ for every other place w of M. Thus D is a G-crossed product division algebra defined over K, and is split by $\hat{M}$, so that (K, M, G) satisfies (4).

Let us show (2) is not satisfied. Suppose on the contrary that there exists a triple (L_0, L, D) realizing (2). By Remark 4.1, L/K is Galois and

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L/L_0) \ltimes \mathrm{Gal}(L/M) \cong G \ltimes_\phi G$$

via some homomorphism $\phi : G \to \mathrm{Aut}(G) = \mathrm{GL}_3(\mathbb{F}_p)$. As G is a p-group, ϕ is a homomorphism into some p-Sylow subgroup P of $\mathrm{GL}_3(\mathbb{F}_p)$. These are all conjugate, so we can choose a basis $\{v_1, v_2, v_3\}$ of $\mathbb{F}_p^3$ for which P is the Heisenberg group (in other words the unipotent radical of the standard Borel subgroup), generated by the transformations:

$$\phi_x(a,b,c) = (a+b,b,c),\ \phi_y(a,b,c) = (a,b+c,c),\ \phi_u(a,b,c) = (a+c,b,c)$$

which correspond to the matrices

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, u = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Denoting $[x,y] = x^{-1}y^{-1}xy$, P has the presentation

$$P = \langle x, y, u \mid x^p = y^p = u^p = [x,u] = [y,u] = 1, [x,y] = u\rangle.$$

Every subgroup of the form $\mathbb{F}_p^2 \ltimes G$ is a maximal subgroup of $G \ltimes G$ and thus the Frattini subgroup Φ of $G \ltimes_\phi G$ is contained in $1 \ltimes G$. The subgroup $H := \langle v_1, v_2\rangle \leq G$ is invariant under the action of P and hence under the action of G via ϕ. So, $G \ltimes_\phi H \leq G \ltimes_\phi G$ is a maximal subgroup and $\Phi \leq 1 \ltimes H$. This shows that $\dim_{\mathbb{F}_p} G/\Phi \geq 4$ and thus $G \ltimes_\phi G$ is not generated by less than 4 elements. Therefore $G \ltimes G$ is not realizable over $\mathbb{Q}_p(\sqrt{p})$, see [20, Chp. II,§5, Thm. 3].

On the other hand both L/M and M/K have full rank at w_i and v_i and hence $\mathrm{Gal}(L_{w_i}/K_{v_i}) = G \ltimes G$ which is a contradiction as $G \ltimes G$ is not realizable over K_{v_i}. Thus, (K, M, G) does not satisfy Condition (2). □

Example 4.3 ((7) $\not\Rightarrow$ (8), (7) $\not\Rightarrow$ (3)). Let $p \equiv 1 \pmod 4$, $K = \mathbb{Q}(\sqrt{-1})$ and v_1, v_2 the two prime divisors of p in K. Let $G = \mathbb{F}_p^p$ and $P = \mathbb{F}_p \wr (\mathbb{Z}/p\mathbb{Z})$ so that $P = G \rtimes \langle x\rangle$ where $x^p = 1$.

The maximal p-extension $\overline{\mathbb{Q}_p(p)}$ has Galois group $\overline{G_{\mathbb{Q}_p}(p)} := \mathrm{Gal}(\overline{\mathbb{Q}_p(p)}/\mathbb{Q}_p)$ which is a free pro-p group on two generators [20, Chp. II,§5, Thm. 3]. As P is generated by two elements it is realizable over $\mathbb{Q}_p$. Since P is a wreath product of abelian groups it has a generic extension over K and hence by [18], there exists a P-extension L/K for which $\mathrm{Gal}(L_{v_i}/K_{v_i}) = P$ for $i = 1,2$. Let us choose $M = L^G$ to be the G-fixed subfield of L and $L_0 := L^{\langle x\rangle}$. Note that since v_i has a unique prime divisor in L_0 for $i = 1,2$, we write $(L_0)_{v_i}$ to denote the completion at that prime divisor.

Then L/M is an M-adequate extension which is defined over K since $L_0 = L^{\langle x\rangle}$ is a subfield for which:

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L/L_0) \ltimes \mathrm{Gal}(L/M).$$

Moreover, since $[(L_0)_{v_i} : K_{v_i}] = p^p$ for $i = 1,2$, L_0 is a maximal subfield of a K-central division algebra D_0 with invariants $\pm 1/p^p$ at v_1 and v_2 that is split elsewhere. Thus L_0 is K-adequate and (K, M, G) satisfies Condition (7).

Now since G is an abelian group of rank $p > 2$, G is not realizable over $K_{v_1}, K_{v_2} \cong \mathbb{Q}_p$ and hence not K-admissible. It follows that (K, M, G) does not satisfy Condition (8). In order for (K, M, G) to satisfy Condition (3) there should be a G-extension L_0/K for which L_0M is M-adequate. In particular, $\mathrm{Gal}((L_0M)_{v_1}/M_{v_1}) \cong G$ and hence $\mathrm{Gal}((L_0)_{v_1}/K_{v_1}) \cong G$ which contradicts the fact that G is not realizable over $K_{v_1} \cong \mathbb{Q}_p$. Thus (K, M, G) does not satisfy Condition (3) either. □

Example 4.4 ((3) $\not\Rightarrow$ (8), (3) $\not\Rightarrow$ (7)). Let $p \equiv 1 \pmod 4$ and v be its unique prime divisor in $K = \mathbb{Q}(\sqrt{p})$. Let $M = \mathbb{Q}(\sqrt{p}, i)$ and $G = (\mathbb{Z}/p\mathbb{Z})^3$.

By the Grunwald-Wang Theorem, there exists a Galois G-extension L_0/K for which $\mathrm{Gal}((L_0)_v/K_v) = G$. Thus $L = L_0M$ is a Galois G-extension of M such that $\mathrm{Gal}(L_{v_i}/M_{v_i}) = G$ for each of the two prime divisors v_1, v_2 of v in M. It follows that L is M-adequate and (K, M, G) satisfies Condition (3). But as p has a unique prime divisor in K and G is not metacyclic, G is not K-admissible and hence (K, M, G) does not satisfy Condition (8).

Let us also show that (K, M, G) does not satisfy Condition (7). Assume, on the contrary, that (L_0, L, D_0, D) realizes (7). Then, as there exists a division algebra of exponent p^3 split by L_0 and whose sum of invariants is zero, there exist two primes w_1, w_2 of K for which $[(L_0)_{w_i} : K_{w_i}] = p^3$. Without loss of generality we assume $w_1 \neq v$ (otherwise we interchange w_1 and w_2). Then $\mathrm{Gal}(L_{w_1}/M_{w_1}) \cong G$ since $(L_0)_{w_1} \cap M_{w_1} = K_{w_1}$. This is a contradiction since tamely ramified extensions (such as L_{w_1}/M_{w_1}) have metacyclic Galois groups. Thus (K, M, G) does not satisfy Condition (7). □

Remark 4.5. Let us also show that (K, M, G) of the previous example does not satisfy (4), so that this example also shows that (3) does not imply (4). Assume on the contrary that there exists a tuple (L, D_0, D) that realizes (4). Since D contains L as a maximal subfield, $\mathrm{Gal}(L_{v_i}/M_{v_i}) = G$ and $\mathrm{inv}_{v_i}(D) = \frac{m_i}{p^3}$ where $(m_i, p) = 1$, for $i = 1, 2$. Note that G is realizable over M_v only for divisors v of p, so that $\mathrm{inv}_u(D) = \frac{m_u}{p^2}$ for suitable $m_u \in \mathbb{Z}$ for every $u \neq v_1, v_2$. Now, since D is in the image of the restriction, we have $m_1 = m_2$. The sum of M-invariants of D is an integer and hence $p \mid m_1 + m_2 = 2m_1$ which contradicts $(m_i, p) = 1$.

Example 4.6 ((4) $\not\Rightarrow$ (8)). Choose an odd prime p, and a prime $q \equiv 1 \pmod p$. Let $K = \mathbb{Q}(\sqrt{p})$, so that q splits (completely) in K. We define v to be the unique prime of K lying over p, and choose w to be a prime divisor of q in K. Let M be a $\mathbb{Z}/p\mathbb{Z}$-extension of K in which v splits and w is inert. Set $G := (\mathbb{Z}/p\mathbb{Z})^3$.

Consider the K-division algebra D_0 whose invariants are:

$$\mathrm{inv}_v(D_0) = \frac{1}{p^3}, \quad \mathrm{inv}_w(D_0) = -\frac{1}{p^3}$$

and $\mathrm{inv}_u(D_0) = 0$ for every other place u of K. Now $D = D_0 \otimes_K M$ has M-invariants $\mathrm{inv}_{v_i}(D) = \frac{1}{p^3}$ for the prime divisors $v_1, v_2, \ldots, v_p$ of v in M, $\mathrm{inv}_{w'}(D) = -\frac{1}{p^2}$ for the prime divisor w' of w and $\mathrm{inv}_u(D) = 0$ for every other place u of M. Note that G is realizable over $M_{v_i} \cong K_v$ and $(\mathbb{Z}/p\mathbb{Z})^2$ is realizable over $M_{w'}$ since $q \equiv 1 \pmod p$. By the Grunwald-Wang Theorem, there exists a Galois G-extension L/M for which:

$$\mathrm{Gal}(L_{v_i}/M_{v_i}) = G \ \text{ for } \ i = 1, \ldots, p, \ \text{ and } \ \mathrm{Gal}(L_{w'}/M_{w'}) = (\mathbb{Z}/p\mathbb{Z})^2.$$

As the degree $[L : M]$ is equal to the index of D over M, and M splits D, it is a maximal subfield of D. Thus (K, M, G) satisfies Condition (4). Since p has a unique prime divisor in K and G is not metacyclic, we deduce that G is not K-admissible by Corollary 3.4, and hence (K, M, G) does not satisfy Condition (8). □

Example 4.7 ((6) $\not\Rightarrow$ (4)). Let $p \geq 13$ be a prime such that $p \equiv 1 \pmod 4$. Let $K = \mathbb{Q}(\mu_p)$ and $M = \mathbb{Q}(\mu_{4p^2}) = \mathbb{Q}(i, \mu_{p^2})$. Let G be the following metacyclic group of order p^3:

$$G = \left\langle x, y \mid x^p = y^{p^2} = 1,\ x^{-1}yx = y^{p+1} \right\rangle. \tag{4.1}$$

Note that p splits in $\mathbb{Q}(i)$ and has exactly two prime divisors v_1, v_2 in M. Let u be the unique prime divisor of p in K.

Let us first show that (K, M, G) does not satisfy Condition (4). As M does not satisfy Liedahl's condition, G is not realizable over M_v for every $v \neq v_1, v_2$. Assume on the contrary there exists an M-adequate G-extension L/M and an M-division algebra D which is defined over K and has a maximal subfield L. Then necessarily: $\mathrm{inv}_{v_1}(D) = \mathrm{inv}_{v_2}(D) = \frac{a}{p^3}$ for some $(a, p) = 1$. But as the sum of invariants of D is 0 and G is not realizable over any other v, we have $p \mid 2a$ contradicting that a and p are coprime.

We next prove that (K, M, G) satisfies Condition (6). Let $\sigma_{p+1} \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^2})/\mathbb{Q})$ be the automorphism that sends $\sigma_{p+1}(\zeta) = \zeta^{p+1}$ where ζ is a primitive root of unity of order p^2. Thus σ_{p+1} fixes μ_p and hence $\sigma_{p+1} \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^2})/K)$. As G satisfies Liedahl's condition over K, G is realizable over infinitely many primes of K as in §3.1, so choose one such prime w which is not a divisor of p. Since $[K_u : \mathbb{Q}_p] = p-1 \geq 12$, there exists a free pro-p extension of K_u of rank $(p-1)/2 \geq 6$, so that G is realizable over K_u by a G-extension L_0^p/K_u for which $M_u \cap L_0^p = K_u$.

By Theorems 6.4(b) and 2.5 of [16] (see also [13, Proposition 1.2.13]), there exists a G-extension L_0/K for which $\mathrm{Gal}((L_0)_w/K_w) = G$ and $(L_0)_u = L_0^p$. Hence L_0 is K-adequate. Let $L = L_0 M$. As $M_u \cap L_0^p = K_u$, we have $\mathrm{Gal}(L_{v_i}/M_{v_i}) = G$ for $i = 1, 2$. Thus L/M is an M-adequate G-extension and (K, M, G) satisfies Condition (6). This concludes the proof of Example 4.7. □

5. Galois extensions of the subfield

Having established the connections between Conditions (1)–(8), we consider in this section a final condition where the maximal subfield of the division algebra is Galois over K:

(9) there exists an M-adequate G-extension L/M for which L is Galois over K;

Proposition 5.1. *The implication (9)⇒(1) holds. On the other hand* (9) *does not imply* (m) *for* $m = 2, \ldots, 8$*, and* (m) *does not imply* (9) *for* $m = 1, \ldots, 8$.

Before providing a proof we make some remarks. Proposition 3.7 shows that when G is cyclic, Conditions (1)–(8) are satisfied for every extension of number fields M/K. This is not the case for (9):

Example 5.2. If M/K is not normal, (9) does not necessarily hold for a cyclic group G: Let $n \geq 2$ and M/K be an extension of degree n whose Galois closure M' has Galois group $\mathrm{Gal}(M'/K) = S_n$. Then every field $L \supseteq M$, which is Galois over K, must contain M' and hence there is no (adequate) C_n-extension L/M for which L/K is Galois. □

Remark 5.3. Remark 4.1 shows that if M/K is Galois then (2) implies (9). In particular (9) holds for G cyclic if M/K is Galois.

Proof of Proposition 5.1. Clearly when (K, M, G) satisfies (9), G is M-admissible and hence (1) holds. Example 5.2 shows that (5) does not imply (9), and hence no other condition among (1)–(8) implies (9). The examples presented in Section 4 show that (9) does not imply any of the Conditions (2), (8), (4). Indeed:

- (9) $\not\Rightarrow$ (2) follows from Example 4.2 where (K, M, G) does not satisfy (2), but $L = \hat{M}$ was constructed to be Galois over K and hence (9) holds.
- (9) $\not\Rightarrow$ (8) follows from Example 4.3 where (8) does not hold, but (7) does. Since by Remark 5.3, (7) ⇒ (2) ⇒ (9) as M/K is Galois, (K, M, G) also satisfies (9).

- (9) $\not\Rightarrow$ (4): Consider Example 4.7. By Remark 5.3, as M/K is Galois, (6) $\Rightarrow$ (9). Thus, (K, M, G) in this example also satisfies (9).

This completes the placement of (9) in Diagram 2.1 of Theorem 2.2. □

References

[1] G. Alon, F. Legrand, E. Paran, Galois groups over rational function fields over skew fields. C. R. Math. Acad. Sci. Paris 358 (2020), 785–790.

[2] A. Auel, E. Brussel, S. Garibaldi, U. Vishne, Open problems on central simple algebras. Transform. Groups 16 (2011), 219–264.

[3] E. Artin, J. Tate, Class field theory. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1990.

[4] A. Behajina, Théorie inverse de Galois sur les corps des fractions rationnelles tordus. J. Pure App. Algebra 225 (2021), 106549.

[5] A. Behajina, B. Deschamps, F. Legrand, Problèmes de plongement finis sur les corps non commutatifs. To appear in Israel Journal of Mathematics.

[6] O. David, The center of the generic G-crossed product. J. Algebra 463 (2016), 103–133.

[7] D. Habater, J. Hartmann, D. Krashen, Patching subfields of division algebras. Trans. AMS. 363 (2011), 3335–3349.

[8] T. Hanke, D. Neftin, A. Wadsworth, Galois subfields of tame division algebras. Israel J. Math. 211 (2016), 367–389.

[9] J. König, D. Neftin, The admissibility of M_{11} over number fields. J. Pure and Applied Algebra 222 (2018), 2456–2464.

[10] J. König, D. Neftin, The local dimension of a finite group over a number field. Trans. Amer. Math. Soc. 375 (2022), 4783–4808.

[11] J. König, F. Legrand, D. Neftin, On the local behaviour of specializations of function field extensions. IMRN (2019), 2951–2980.

[12] S. Liedahl, Presentations of metacylic p-groups with applications to K-admissibility questions. J. Algebra 169 (1994), 965–983.

[13] D. Neftin, Admissibility of finite groups over number fields. Ph.D. Thesis, Technion 2011.

[14] D. Neftin, Tamely ramified subfields of division algebras. J. Algebra 378 (2013), 184–195.

[15] D. Neftin, E. Paran, Patching and admissibility over two-dimenisonal complete local domains. Algebra and Number Theory 4 (2010), 743–762.

[16] J. Neukirch, Uber das Einbettungsproblem der algebraischen Zahlentheorie. Invent. Math. 21 (1973), 59–116.

[17] A.S. Rapinchuk and I.R. Rapinchuk, On division algebras having the samemaximal subfields. Manuscripta Math. 132 (2010), 273–293.

[18] D. Saltman, Generic Galois extensions. Proc. Nat. Acad. Sci. U.S.A. 77 (1980), 1250–1251.

[19] M. Schacher, Subfields of division rings I. J. Algebra 9 (1968), 451–477.

[20] J.-P. Serre, Galois Cohomology. Springer, 1964 (English trans. 1996).

[21] J.-P. Serre, Local fields. Graduate Texts in Mathematics 67. Springer-Verlag, New York-Berlin, 1979.

[22] J. Sonn, $\mathbb{Q}$-admissibility of solvable groups. J. Algebra 84 (1983), 411–419.

[23] S. Wang, On Grunwald's theorem. Ann. Math. (2) 51 (1950), 471–484.