Münster J. of Math. **12** (2019), 139–161
DOI 10.17879/85169760740
urn:nbn:de:hbz:6-85169761153

**Münster Journal of Mathematics**

# Composita of symmetric extensions of $\mathbb{Q}$

Wulf-Dieter Geyer, Moshe Jarden, and Aharon Razon

(Communicated by Linus Kramer)

**Abstract.** Let $K$ be a Hilbertian presented field with elimination theory of characteristic $\neq 2$, let $K_{\mathrm{symm}}$ be the compositum of all symmetric extensions of $K$, and let $K_{\mathrm{symm,ins}}$ be the maximal purely inseparable extension of $K_{\mathrm{symm}}$. Then, $\mathrm{Th}(K_{\mathrm{symm,ins}})$ is a primitive recursive theory. Moreover, the set of finite groups that can be realized as Galois groups over $K$ in $K_{\mathrm{symm}}$ as well as the set of finite groups that occur as Galois groups over $K_{\mathrm{symm}}$ are primitive recursive subsets of the set of all finite groups. Finally, if $K$ is countable, then $\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q})$.

## Introduction

Let $\mathbb{Q}_{\mathrm{cycl}}$ be the field obtained from $\mathbb{Q}$ by adjoining all roots of unity. By the Kronecker–Weber theorem, $\mathbb{Q}_{\mathrm{cycl}}$ coincides with the compositum $\mathbb{Q}_{\mathrm{ab}}$ of all finite abelian extensions of $\mathbb{Q}$. In particular, the set $\mathrm{Im}(\mathrm{Gal}(\mathbb{Q}_{\mathrm{cycl}}/\mathbb{Q}))$ of all finite quotients of $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cycl}}/\mathbb{Q})$ consists of all finite abelian groups. By a conjecture of Shafarevich, the absolute Galois group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cycl}})$ of $\mathbb{Q}_{\mathrm{cycl}}$ is isomorphic to the free profinite group $\hat{F}_\omega$ on $\aleph_0$ generators. Under this conjecture, $\mathrm{Im}(\mathrm{Gal}(\mathbb{Q}_{\mathrm{cycl}}))$ is the set of all finite groups. Thus, if the Shafarevich conjecture holds, then both $\mathrm{Im}(\mathrm{Gal}(\mathbb{Q}_{\mathrm{cycl}}/\mathbb{Q}))$ and $\mathrm{Im}(\mathrm{Gal}(\mathbb{Q}_{\mathrm{cycl}}))$ are explicit sets of finite groups. In technical terms, both sets are primitive recursive subsets of the set FiniteGroups of all finite groups, up to isomorphism.

Replacing $\mathbb{Q}$ by the rational function field $\mathbb{F}_p(t)$ for a prime number $p$, we find that $\mathbb{F}_p(t)_{\mathrm{cycl}} = \tilde{\mathbb{F}}_p(t)$, where $\tilde{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$. In this case,

$$\mathrm{Im}(\mathrm{Gal}(\mathbb{F}_p(t)_{\mathrm{cycl}}/\mathbb{F}_p(t))) = \mathrm{Im}(\mathrm{Gal}(\mathbb{F}_p))$$

is the set of all finite cyclic groups. Moreover, the analog of the Shafarevich conjecture holds, that is, $\mathrm{Gal}(\tilde{\mathbb{F}}_p(t)) \cong \hat{F}_\omega$. See [12, Cor. 4.2], [15, Thm. 1], [11, Cor. 4.7], and [13, p. 186, Cor. 9.4.9]. In particular, we have $\mathrm{Im}(\mathrm{Gal}(\tilde{\mathbb{F}}_p(t))) =$ FiniteGroups.

Going back to $\mathbb{Q}$, Example 9.4, due to Fried and Völklein, presents Galois extensions $N$ of $\mathbb{Q}$, with $\mathrm{Gal}(N/\mathbb{Q}) \cong \prod_{n=2}^{\infty} S_n$ and $\mathrm{Gal}(N) \cong \hat{F}_\omega$, and with a simple procedure to find the finite quotients of these groups.

All of these fields are contained in the distinguished Galois extension $\mathbb{Q}_{\mathrm{symm}}$ of $\mathbb{Q}$. Here, $\mathbb{Q}_{\mathrm{symm}}$ is the compositum of all symmetric extensions of $\mathbb{Q}$, where a Galois extension $L/K$ of fields is *symmetric* if $\mathrm{Gal}(L/K) \cong S_n$ for some positive integer $n$.

One goal of this work is to prove that $\mathbb{Q}_{\mathrm{symm}}$ itself has those properties.

**Theorem A.** *Both* $\mathrm{Im}(\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q}))$ *and* $\mathrm{Im}(\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}))$ *are primitive recursive subsets of* FiniteGroups*.*

On the other hand, the list of explicitly known Galois extensions of $\mathbb{Q}$ with a decidable elementary theory is quite restrictive. It contains the fields $\mathbb{Q}_{\mathrm{tot},S}$, where $S$ is a finite set of primes and $\mathbb{Q}_{\mathrm{tot},S}$ is the maximal Galois extension of $\mathbb{Q}$ in which each $p \in S$ totally splits [6, Thm. 1.1]. Moreover, if $S$ and $S'$ are finite sets of prime numbers such that $S \cap S' \neq \varnothing$, then also $\mathbb{Q}_{\mathrm{tot},S}\mathbb{Q}_{\mathrm{tot},S'}$ is decidable [5, theorem below Proposition 5].

In addition, every finite extension of the above mentioned fields is decidable [4, Sec. 3, Cor.].

Taking $S = \varnothing$, we observe that the above list contains the field $\tilde{\mathbb{Q}}$ of all algebraic numbers. If $S$ consists of the infinite prime of $\mathbb{Q}$, then $\mathbb{Q}_{\mathrm{tot},S}$ is the field of all totally real algebraic numbers. In both cases, the elementary theory, $\mathrm{Th}(\mathbb{Q}_{\mathrm{tot},S})$, of $\mathbb{Q}_{\mathrm{tot},S}$ is even primitive recursive (see [9, p. 168, Thm. 9.3.1 (c)] and [7, Thm. 10.1]).

In this work we prove that every Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{symm}}$ is a compositum of symmetric extensions of $\mathbb{Q}$ (Lemma 7.1). This gives an explicit procedure to examine whether a polynomial $f \in \mathbb{Q}[X]$ has a root in $\mathbb{Q}_{\mathrm{symm}}$ (Lemma 8.1). Using that $\mathbb{Q}_{\mathrm{symm}}$ is PAC with $\hat{F}_\omega$ as an absolute Galois group, we conclude the following result from [14, Lemma 3.3].

**Theorem B.** $\mathrm{Th}(\mathbb{Q}_{\mathrm{symm}})$ *is primitive recursive.*

It turns out that the method we use to prove Theorems A and B actually gives a much more general result (Theorem 8.5):

**Theorem C.** *Let $K$ be a finitely generated presented extension of $\mathbb{Q}$ in the sense of* [9, Chap. 19]*. In particular, $K$ is Hilbertian and the following statements hold:*

(a) *Both families* $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}}))$ *and* $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}}/K))$ *are primitive recursive in* FiniteGroups*. Indeed,* $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}})) = \mathrm{FiniteGroups}$*.*

(b) $\mathrm{Th}(K_{\mathrm{symm}})$ *is primitive recursive.*

We note that Part (a) of Theorem C also holds for each infinite finitely generated extension of each of the fields $\mathbb{F}_p$ with $p \neq 2$. Moreover, Part (b) of Theorem C holds for every infinite finitely generated extension of $\mathbb{F}_p$, albeit with the maximal purely inseparable extension $K_{\mathrm{symm,ins}}$ of $K_{\mathrm{symm}}$ replacing $K_{\mathrm{symm}}$.

More surprising is the fact that for both $\mathrm{Gal}(K_{\mathrm{symm}}/K)$ and $\mathrm{Gal}(K_{\mathrm{symm}})$ there exists a "formation" $\mathcal{C}$ of finite groups such that the respective group is the free pro-$\mathcal{C}$-group of rank $\aleph_0$.

To be more explicit, we say that a finite group $G$ is *symmetrically presentable* if there are a finite set $I$ and an embedding $\iota\colon G \to \prod_{i\in I} S_{n_i}$ such that $\mathrm{pr}_i(\iota(G)) = S_{n_i}$ for each $i \in I$. It turns out that the family $\mathcal{SP}$ of all symmetrically presentable groups is a *formation* in the sense of [9, Section 17.3]. Hence, there exists a unique (up to isomorphism) *free pro-$\mathcal{C}$-group* $\hat{F}_\omega(\mathcal{SP})$ of rank $\aleph_0$ [9, Prop. 17.4.2]. We also mention that the free pro-FiniteGroups-group of rank $\aleph_0$ is usually denoted by $\hat{F}_\omega$.

**Theorem D** (Theorem 7.5 and Theorem 8.5)**.** *The following statements hold for each countable Hilbertian field $K$ of* $\mathrm{char}(K) \neq 2$*:*

(a) $\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \hat{F}_\omega(\mathcal{SP})$.
(b) $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$.
(c) $\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q})$.

Note that Part (b) of the theorem is a consequence of well-known results of Field Arithmetic (see the proof of Theorem 8.5).

Finally, we realize that $K_{\mathrm{symm}}$ is the largest field in a descending sequence of Galois extensions of $K$ that satisfy the consequences of Theorem C. Indeed, for each positive integer $m$, we let $K_{\mathrm{symm}}^{(m)}$ be the compositum of all $S_n$-extensions of $K$ with $n \geq m$. Then, Theorem C and the remark that follows Theorem C hold for $K_{\mathrm{symm}}^{(m)}$ replacing $K_{\mathrm{symm}}$. Moreover, $K_{\mathrm{symm}}^{(m+1)} \subseteq K_{\mathrm{symm}}^{(m)}$ for each $m$ (Example 9.1). In addition, Example 9.1 and Remark 9.2 contain an analog of Theorem D.

## 1. Symmetric groups

As usual, for each positive integer $n$ we denote the group of all permutations of the set $\{1,\dots,n\}$ by $S_n$. One refers to $S_n$ also as the *symmetric group of degree $n$*. We call a group $G$ *symmetric* if $G$ is isomorphic to $S_n$ for some positive integer $n$. For $m \leq n$, we consider $S_m$ as the subgroup of $S_n$ that fixes each $m+1 \leq i \leq n$. In particular, $S_2$ is the subgroup $\{(1),(1\,2)\}$ of $S_n$. As usual, we denote the multiplicative cyclic group of order $n$ by $C_n$.

We start by listing some well known facts about symmetric groups. To this end, we use the standard notation $A_n$ for the *alternating group of degree $n$* and recall that $A_n$ consists of all even permutations of the set $\{1,\dots,n\}$. We also mention the *Klein four-group*

$$V_4 = \bigl\{(1),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\bigr\}.$$

**Fact 1.1.** *Let $n$ be a positive integer.*

(a) *For $n \neq 4$, the only normal subgroups of $S_n$ are $\mathbf{1}$, $A_n$, and $S_n$ with respective quotients $S_n$, $S_2$, and $S_1$.*
(b) *The only normal subgroups of $S_4$ are $\mathbf{1}$, $V_4$, $A_4$, and $S_4$ with respective quotients $S_4$, $S_3$, $S_2$, and $S_1$. Moreover, $V_4 \leq A_4$ and $V_4 \cong C_2 \times C_2$.*
(c) *For $n = 3$, we have $A_3 \cong C_3$. If $n \geq 5$, then $A_n$ is nonabelian. In both cases, $A_n$ is a simple group.*

Fact 1.1 (a), (b) imply the following observation.

**Lemma 1.2.** *Every quotient group of a symmetric group is a symmetric group.*

Recall that a nontrivial normal subgroup $N$ of a group $S$ is said to be *minimal* if $S$ has no normal subgroup $N_0$ with $\mathbf{1} < N_0 < N$. In this case, if $\pi\colon S \to S'$ is an epimorphism and $\pi(N) \neq \mathbf{1}$, then $\pi(N)$ is a minimal normal subgroup of $S'$.

**Notation 1.3.** For every integer $n \geq 2$, we introduce the group

$$A_{(n)} = \begin{cases} S_2 & \text{if } n = 2, \\ V_4 & \text{if } n = 4, \\ A_n & \text{otherwise,} \end{cases}$$

and note, by Fact 1.1 (a), (b), that $A_{(n)}$ is the unique minimal normal subgroup of $S_n$. Moreover, $A_{(n)}$ is abelian if $n \in \{2, 3, 4\}$.

Also, if $n \geq 5$, then $A_{(n)} = A_n$ is a nonabelian simple group (Fact 1.1 (c)). In particular, the center of $A_{(n)}$ is in this case trivial. Note that $A_{(n)} \cong A_{(n')}$, with $n, n' \geq 2$, implies that $n = n'$.

Finally, note, for $n \geq 2$, that

$$S_n/A_{(n)} \cong \begin{cases} \mathbf{1} & \text{if } n = 2, \\ S_3 & \text{if } n = 4, \\ S_2 & \text{otherwise.} \end{cases}$$

**Notation 1.4.** A direct product of symmetric groups has the form

$$S = S_{n_1} \times \cdots \times S_{n_r} = \prod_{i \in I} S_{n_i}$$

with an index set $I = \{1, 2, \ldots, r\}$ and a family $(n_i)_{i \in I}$ of positive integers. For each subset $J$ of $I$, we identify $S_J = \prod_{j \in J} S_{n_j}$ with the subgroup $\prod_{j \in J} S_{n_j} \times \prod_{i \in I \smallsetminus J} \mathbf{1}$ of $S$.

We set $\mathrm{pr}_i\colon S \to S_{n_i}$ to be the projection of $S$ on the $i$th coordinate. Thus, for $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_r)$, we have $\mathrm{pr}_i(\boldsymbol{\sigma}) = \sigma_i$. The kernel of $\mathrm{pr}_i$ is $S^{(i)} = \prod_{j \neq i} S_{n_j}$.

We also consider the normal subgroup

$$A = \prod_{i \in I} A_{(n_i)}$$

of $S$ with the quotient

$$\bar{S} = S/A \cong \prod_{n_i \neq 2,4} S_2 \times \prod_{n_i = 4} S_3.$$

**Remark 1.5** (Signs of permutations)**.** Recall that $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ is the homomorphism of $S_n$ that maps the even permutations onto 1 and the odd permutations onto $-1$. In particular, $\mathrm{Ker}(\mathrm{sgn}) = A_n$.

Since $A_3 \cong C_3$ (Fact 1.1 (c)), $\mathrm{Aut}(A_3) \cong C_2$ consists of raising the elements of $A_3$ to the powers 1 or $-1$. Thus, for each $a \in A_3$ and $\sigma \in S_3$, we have $a^\sigma = a^{\mathrm{sgn}(\sigma)}$. Considering $\sigma$ as an automorphism of $S_3$ that acts by conjugation, we find that each automorphism of $A_3$ can be lifted to an inner automorphism of $S_3$. This yields a short exact sequence

$$\mathbf{1} \to A_3 \to S_3 \xrightarrow{\text{sgn}} \mathrm{Aut}(A_3) \to \mathbf{1}.$$

Since $\mathrm{sgn}(1\,2) = -1$, we also have that sgn maps $S_2$ bijectively onto $\mathrm{Aut}(A_3)$.

For $n = 4$ and for $\sigma \in S_4$, we define $\mathrm{Sgn}(\sigma)$ to be the automorphism of $V_4$ defined by conjugation with $\sigma$. Since $V_4$ is abelian, $V_4 \leq \mathrm{Ker}(\mathrm{Sgn})$. Embedding $S_3$ into $S_4$ as the subgroup of all permutations of $\{1, 2, 3, 4\}$ that fix 4, we find that Sgn is injective on $S_3$. Since $V_4 \cong \mathbb{F}_2^2$, we have $|\mathrm{Aut}(V_4)| = 6 = |S_3|$. Hence, Sgn maps $S_3$ bijectively onto $\mathrm{Aut}(V_4)$. Finally, since $(S_4 : V_4) = 6$ (Fact 1.1 (b)), we find that $V_4 = \mathrm{Ker}(\mathrm{Sgn})$. This leads to the following short exact sequence:

$$\mathbf{1} \to V_4 \to S_4 \xrightarrow{\text{Sgn}} \mathrm{Aut}(V_4) \to \mathbf{1}.$$

## 2. Semi-direct products

We fix our notation for two basic notions of group theory, "the automorphism group" and "semi-direct product" of groups.

**Notation 2.1** (Automorphisms)**.** For each $a$ in a group $A$ and $\alpha \in \mathrm{Aut}(A)$ we write $a^\alpha$ for the image of $a$ under $\alpha$. Thus, $(ab)^\alpha = a^\alpha b^\alpha$ for $a, b \in A$ and $a^{\alpha\beta} = (a^\alpha)^\beta$.

**Remark 2.2** (Semi-direct Products)**.** (a) If a group $G$ contains a normal subgroup $N$ and a subgroup $H$ such that $H \cap N = \mathbf{1}$ and $HN = G$, then $G$ is an (inner) *semi-direct product* of $H$ and $N$, and we write $G = H \ltimes N$. In this case, we say that $H$ is a *complement* of $N$ in $G$. In the special case where also $H$ is normal in $G$, we have that $G = H \times N$ is the direct product of $H$ and $N$.

(b) Let $A, B, C$ be subgroups of a group $G$ such that $A$ normalizes $B$ and $C$, and $B$ normalizes $C$. In addition, assume that $B \cap C = \mathbf{1}$ and $A \cap BC = \mathbf{1}$. Then, under the above identifications, $ABC = A \ltimes (B \ltimes C)$. Moreover, $A \cap B = \mathbf{1}$ and $AB \cap C = \mathbf{1}$. Hence, $ABC = AB \ltimes C = (A \ltimes B) \ltimes C$. Similarly, if $A \cap B = \mathbf{1}$ and $AB \cap C = \mathbf{1}$, then $ABC = AB \ltimes C = (A \ltimes B) \ltimes C$. In both cases,

$$A \ltimes (B \ltimes C) = (A \ltimes B) \ltimes C.$$

A special case of this rule is $A \ltimes (B \times C) = (A \ltimes B) \ltimes C$, where $B$ acts trivially on $C$.

(c) Let $N \leq G \leq S$ and $T \leq S$ be groups such that $N \lhd S$, $T \cap N = \mathbf{1}$, and $TN = S$, so that $S = T \ltimes N$. Then, $H = T \cap G$ satisfies $H \cap N = \mathbf{1}$ and $HN = G$. Hence, $G = H \ltimes N$.

Similarly, let $H \leq Q \leq G$ and $A \leq G$ be groups with $G = H \ltimes A$. Then, $A' = A \cap Q$ satisfies $Q = H \ltimes A'$.

(d) Let $\phi \colon G \to \bar{G}$ be an epimorphism of groups and let $N$ be a normal subgroup of $G$ on which $\phi$ is injective. Set $\bar{N} = \phi(N)$ and suppose that $\bar{G} = \bar{M} \ltimes \bar{N}$ is a semi-direct decomposition of $\bar{G}$. Then, $G = M \ltimes N$, with $M = \phi^{-1}(\bar{M})$.

Indeed, each $n \in M \cap N$ satisfies $\phi(n) \in \bar{M} \cap \bar{N}$, hence $\phi(n) = 1$, so $n = 1$. Thus, $M \cap N = \mathbf{1}$.

Further, for each $g \in G$, there exist $\bar{m} \in \bar{M}$ and $n \in N$ such that $\phi(g) = \bar{m}\phi(n)$. Thus, $\phi(gn^{-1}) = \bar{m} \in \bar{M}$, so $gn^{-1} \in M$, by the definition of $M$. Therefore, $g = (gn^{-1})n \in MN$.

Combining the latter two paragraphs, we conclude that $G = M \ltimes N$, as claimed.

**Remark 2.3** (Examples of automorphism groups and semi-direct products)**.**

(a) As mentioned in Remark 1.5, the group $A_3$ is isomorphic to the cyclic group $C_3$ of order 3, so $\mathrm{Aut}(A_3) = C_2$ is generated by the automorphism $\sigma \mapsto \sigma^{-1}$.

(b) Also, $\mathrm{Aut}(V_4) = S_3$, where $S_3$ is acting on $V_4$ by conjugation in $S_4$. Moreover, since $S_3 \cap V_4 = \mathbf{1}$ and $S_3V_4 = S_4$, we have $S_4 = S_3 \ltimes V_4$.

(c) By Notation 1.3, we have

$$\begin{aligned}
&S_2 = \mathbf{1} \times S_2 = S_1 \times A_{(2)},\\
&S_3 = S_2 \ltimes A_3 = S_2 \ltimes A_{(3)},\\
&S_4 = S_3 \ltimes V_4 = S_3 \ltimes A_{(4)} \quad \text{and} \quad S_4 = S_2 \ltimes A_4,\\
&S_n = S_2 \ltimes A_n = S_2 \ltimes A_{(n)} \quad \text{if } n \geq 5.
\end{aligned}$$

It follows from Fact 1.1 (a), (b) that, for every $n \geq 2$, every normal subgroup $N$ of $S_n$ has a complement $M$ in $S_n$ and $M \cong S_n/N$ is again a symmetric group.

## 3. Symmetrically presentable groups

Garrett Birkhoff refers to an algebra $B$ as a "sub-direct product of algebras $B_1, \dots, B_r$" if there is an embedding $\iota\colon B \to \prod_{i=1}^r B_i$ such that $\mathrm{pr}_i(\iota(B)) = B_i$ for $i = 1, \dots, r$ [2, p. 175]. We introduce a similar notion for finite groups and finitely many symmetric groups.

**Set-up 3.1.** Let $I = \{1, \dots, r\}$ and set $S = \prod_{i\in I} S_{n_i}$ with positive integers $n_i$ for $i \in I$. For each $i \in I$, let $\mathrm{pr}_i\colon S \to S_{n_i}$ be the projection on the $i$th component. Then, $S^{(i)} = \mathrm{Ker}(\mathrm{pr}_i) = \prod_{j\neq i} S_{n_j}$ and $S = S^{(i)} \times S_{n_i}$. We let $\mathrm{pr}^{(i)}\colon S \to S^{(i)}$ be the projection of $S$ on the first factor.

We say that a group $G$ is *symmetrically presentable* if there exists a direct product $S$ of finitely many symmetric groups as in the preceding paragraph and an embedding

$$\iota\colon G \to S \tag{3.1}$$

such that $\mathrm{pr}_i(\iota(G)) = S_{n_i}$ for each $i \in I$. In this case we say that $\iota$ is a *symmetric presentation* of $G$. Thus, in the language of Birkhoff, $G$ is a sub-direct product of symmetric groups and $\iota$ is a presentation of $G$ as a sub-direct product of symmetric groups.

We identify $G$ with its image in $S$ under $\iota$ and assume that $\iota$ is the inclusion map. In particular, we have $\mathrm{pr}_i(G) = S_{n_i}$ for each $i \in I$. Then, we consider a subgroup $N$ of $G$ which is normal in $S$ and let

$$(3.2)\qquad \begin{cases} & G^{(i)} = \mathrm{pr}^{(i)}(G), \\ G^{[i]} = S^{(i)} \cap G = \mathrm{Ker}(\mathrm{pr}_i|_G), & G_i = S_{n_i} \cap G = \mathrm{Ker}(\mathrm{pr}^{(i)}|_G), \\ N^{[i]} = S^{(i)} \cap N = \mathrm{Ker}(\mathrm{pr}_i|_N), & N_i = S_{n_i} \cap N = \mathrm{Ker}(\mathrm{pr}^{(i)}|_N), \\ N_{(i)} = \mathrm{pr}_i(N), & N^{(i)} = \mathrm{pr}^{(i)}(N). \end{cases}$$

This leads to the following commutative diagrams whose rows are short exact sequences and where the vertical edges are inclusions:

(3.3)
$$\begin{tikzcd}
\mathbf{1} \arrow[r] & S^{(i)} \arrow[r] & S \arrow[r, "\mathrm{pr}_i"] & S_{n_i} \arrow[r] & \mathbf{1} \\
\mathbf{1} \arrow[r] & G^{[i]} \arrow[r] \arrow[u, dash] & G \arrow[r] \arrow[u, dash] & S_{n_i} \arrow[r] \arrow[u, equal] & \mathbf{1} \\
\mathbf{1} \arrow[r] & N^{[i]} \arrow[r] \arrow[u, dash] & N \arrow[r, "\pi_i"] \arrow[u, dash] & N_{(i)} \arrow[r] \arrow[u, dash] & \mathbf{1}
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbf{1} \arrow[r] & S_{n_i} \arrow[r] & S \arrow[r, "\mathrm{pr}^{(i)}"] & S^{(i)} \arrow[r] & \mathbf{1} \\
\mathbf{1} \arrow[r] & G_i \arrow[r] \arrow[u, dash] & G \arrow[r] \arrow[u, dash] & G^{(i)} \arrow[r] \arrow[u, dash] & \mathbf{1} \\
\mathbf{1} \arrow[r] & N_i \arrow[r] \arrow[u, dash] & N \arrow[r] \arrow[u, dash] & N^{(i)} \arrow[r] \arrow[u, dash] & \mathbf{1}.
\end{tikzcd}$$

Here, $\pi_i = \mathrm{pr}_i|_N$, so $N_{(i)} = \pi_i(N)$ for each $i \in I$. One observes that for each $i \in I$, the embedding of $G^{(i)}$ in $S^{(i)}$ is a symmetric presentation of $G^{(i)}$.

**Lemma 3.2.** *In the notation of Set-up 3.1, $N_i \triangleleft G$, $N_{(i)} \triangleleft S_{n_i}$, $N^{[i]} \triangleleft G$, and $N^{(i)} \triangleleft G^{(i)}$. Moreover, if $N$ is a minimal normal subgroup of $G$ and $N_{(i)} \neq \mathbf{1}$, then $N^{[i]} = \mathbf{1}$ and $\pi_i \colon N \to N_{(i)}$ is an isomorphism.*

*Proof.* Since $N \triangleleft G$ and $G_i = \mathrm{Ker}(\mathrm{pr}^{(i)}|_G) \triangleleft G$, we have $N_i = G_i \cap N \triangleleft G$. In addition, since $N \triangleleft G$, $\mathrm{pr}_i(N) = N_{(i)}$, and $\mathrm{pr}_i(G) = S_{n_i}$, we have $N_{(i)} \triangleleft S_{n_i}$.

Now, $G^{[i]} = \mathrm{Ker}(\mathrm{pr}_i|_G) \triangleleft G$. By assumption, $N \triangleleft G$, so $N^{[i]} = G^{[i]} \cap N \triangleleft G$. Finally, since $\mathrm{pr}^{(i)}(G) = G^{(i)}$ and $\mathrm{pr}^{(i)}(N) = N^{(i)}$, we have $N^{(i)} \triangleleft G^{(i)}$.

It follows that if $N$ is a minimal normal subgroup of $G$ and $N_{(i)} \neq \mathbf{1}$, then $\mathbf{1} \leq N^{[i]} < N$, so $N^{[i]} = \mathbf{1}$, hence $\pi_i \colon N \to N_{(i)}$ is an isomorphism. □

**Definition 3.3.** The symmetric presentation (3.1) of $G$ is said to be *minimal* if the lexicographically ordered pair $(r, |S|)$ is minimal for all possible symmetric presentations of $G$. In particular, if $G = \mathbf{1}$, then $r = 0$ and $I = \varnothing$.

If (3.1) is a minimal symmetric presentation of $G$ and $s \in S$, then the conjugate presentation $\iota^s \colon G \to S$, defined by $\iota^s(g) = s^{-1}\iota(g)s$, is again a minimal symmetric presentation of $G$.

**Lemma 3.4.** *Let $\iota \colon G \to S$ be a minimal symmetric presentation of a finite nontrivial group $G$, as in* (3.1)*. Then, $|I| \geq 1$, and for each $i \in I$, we have $n_i \geq 2$ and the group $G_i$ is nontrivial and normal in $S_{n_i}$.*

*Proof.* Since $G$ is nontrivial, $S$ is nontrivial, hence $|I| \geq 1$. If $n_i = 1$ for some $i \in I$, then we can delete $i$ from $I$ and obtain a smaller symmetric presentation for $G$ than $\iota$. This contradicts the minimality of $\iota$. Hence, $n_i \geq 2$ for each $i \in I$.

Since $G_i$ is the kernel of the epimorphism $\mathrm{pr}^{(i)}|_G\colon G \to G^{(i)}$, we have $G_i \lhd G$. Since $\mathrm{pr}_i(G) = S_{n_i}$ (by (3.3)) and $\mathrm{pr}_i$ maps $G_i$ as a subgroup of $S_{n_i}$ onto itself, we have $G_i \lhd S_{n_i}$.

Finally, if $G_i = \mathbf{1}$, then $\mathrm{pr}^{(i)}|_G\colon G \to S^{(i)}$ is a symmetric presentation of $G$ which is smaller than $\iota\colon G \to S$, contradicting the minimality assumption on $\iota$. It follows that $G_i \neq \mathbf{1}$. □

**Lemma 3.5.** *Suppose that the symmetric presentation $\iota\colon G \to S$ in* (3.1) *is minimal and assume that $\iota$ is the inclusion map. Let $A = \prod_{i\in I} A_{(n_i)}$ be the normal subgroup of $S$ introduced in Notation 1.4.*

*Then, $\prod_{j\in J} A_{(j)} \lhd G$ for every subset $J$ of $I$, in particular, $A \lhd G$.*

*Proof.* We consider an $i \in I$. By Lemma 3.4, the nontrivial normal subgroup $G_i$ of $G$ is also normal in $S_{n_i}$. Hence, $G_i$ contains the unique minimal normal subgroup $A_{(n_i)}$ of $S_{n_i}$ (Notation 1.3), so we also have $A_{(n_i)} \lhd G$. Therefore, $\prod_{j\in J} A_{(n_j)} \lhd G$ for every subset $J$ of $I$. □

**Remark 3.6.** Here is an effective procedure to decide whether a given finite group $G$ has a symmetric presentation.

We make a list $N_1, \dots, N_r$ of all normal subgroups of $G$ such that $G/N_i \cong S_{n_i}$ for some positive integer $n_i$, with $n_i! \leq |G|$, $i = 1, \dots, r$. Then, $G$ has a symmetric presentation if and only if $\bigcap_{i=1}^r N_i = \mathbf{1}$. If the latter condition holds, then the quotient maps $G \to G/N_i$ yield a symmetric presentation of $G$,

$$G \to \prod_{i=1}^r G/N_i \cong \prod_{i=1}^r S_{n_i}.$$

## 4. Quotients of symmetrically presentable groups

We prove that every quotient of a symmetrically presentable group is symmetrically presentable. Throughout, we use Notation 1.3 and the notation introduced in Set-up 3.1, in particular, the notation of diagrams (3.3) in the latter set-up.

**Lemma 4.1.** *Let $G$ be a finite nontrivial group and $\iota\colon G \to S$ a minimal symmetric presentation that we assume to be the inclusion map. Let $N$ be a minimal normal subgroup of $G$ and let $J = \{i \in I \mid N_{(i)} \neq \mathbf{1}\}$. Then, the following statements hold:*

(a) *If $|J| = 1$, say $J = \{j\}$, then $N = A_{(n_j)}$.*

(b) *If $|J| > 1$, then there exist an integer $2 \leq m \leq 4$ and elements $\gamma_j \in \mathrm{Aut}(A_{(m)})$ for $j \in J$ such that $n_j = m$ for all $j \in J$ and*

$$N = \Big\{ (a^{\gamma_j})_{j\in J} \in \prod_{j\in J} S_{n_j} \mid a \in A_{(m)} \Big\}.$$

*In particular, $N \cong A_{(m)}$ is abelian.*

*Proof.* If $j \in J$, then $N_{(j)} \neq \mathbf{1}$, so $N^{[j]} < N$. By Lemma 3.2, $N^{[j]} \lhd G$. It follows from the minimality of $N$ that $N^{[j]} = \mathbf{1}$. Thus,

$$\pi_j \colon N \to N_{(j)} \text{ is an isomorphism for each } j \in J. \tag{4.1}$$

Since $\mathrm{pr}_j(G) = S_{n_j}$ and $N_{(j)} = \mathrm{pr}_j(N) \neq \mathbf{1}$, we have that $N_{(j)}$ is a minimal normal subgroup of $S_{n_j}$ for each $j \in J$. Hence,

$$N_{(j)} = A_{(n_j)} \quad \text{for each } j \in J. \tag{4.2}$$

Since $\mathrm{pr}_i(N) = N_{(i)} = \mathbf{1}$ for each $i \in I \smallsetminus J$, we have $N \leq S_J = \prod_{j \in J} S_{n_j}$. Therefore, (a) is a consequence of (4.1) and (4.2).

In order to prove (b), we assume that

$$|J| > 1. \tag{4.3}$$

For each $j \in J$ the map $\gamma_j = \pi_1^{-1} \circ \pi_j$ (acting from the right) is an isomorphism from $A_{(n_1)}$ onto $A_{(n_j)}$. Hence, setting $m = n_1$, we find that $n_j = m$, so $\gamma_j \in \mathrm{Aut}(A_{(m)})$.

For $\mathbf{a} \in N$, we set $a = \mathbf{a}^{\pi_1}$ and get $\mathrm{pr}_j(\mathbf{a}) = \mathbf{a}^{\pi_j} = (\mathbf{a}^{\pi_1})^{\gamma_j} = a^{\gamma_j}$ for each $j \in J$. Here, $\mathbf{a}^{\pi_j}$ denotes the image of $\mathbf{a}$ under $\pi_j$. Therefore, we have $N = \{(a^{\gamma_j})_{j \in J} \in \prod_{j \in J} S_{n_j} \mid a \in A_{(m)}\}$, hence

$$|N| = |A_{(m)}|. \tag{4.4}$$

We claim that $m \leq 4$. Otherwise $m \geq 5$, so by Fact 1.1 (c), $A_{(m)} = A_m$ is a nonabelian simple group. By Lemma 3.5, $A_m^{|J|} = \prod_{j \in J} A_{(n_j)} \lhd G$. Since $N \leq A_m^{|J|}$ and $N \lhd G$, we have that $N \lhd A_m^{|J|}$. By (4.2) and [9, p. 374, Lemma 18.3.9], $N \cong A_m^{|J|}$. Hence, by (4.4), $|J| = 1$. This contradiction to (4.3) proves that indeed $m \leq 4$, as claimed.

By Notation 1.3, $A_{(m)}$ is abelian. This concludes the proof of (b). □

**Lemma 4.2.** *Let $r \geq 2$ be an integer, consider $m \in \{2, 3, 4\}$, and let $G$ be a subgroup of $S = S_m^r$ such that the inclusion map $\iota \colon G \to S$ is a minimal symmetric presentation of $G$. Suppose that*

$$N = \{(a, \dots, a) \in S \mid a \in A_{(m)}\} \tag{4.5}$$

*is a normal subgroup of $G$. Then, $N$ has a complement $M$ in $G$ and $M \cong G/N$ is symmetrically presentable.*

*Proof.* If $m = 2$, then $S = S_2^r$ is a vector space of dimension $r$ over $\mathbb{F}_2$, $G$ is a subspace of $S$, and $N$ is a subspace of $G$. Hence, $N$ has a complement $M$ in $G$. Moreover, $M$ is a subspace of $S$. As such, $M \cong \prod_{i=1}^{r'} S_2$ for some $r' \leq r$. Hence, $M$ is symmetrically presentable and we are reduced to the case where $m = 3$ or $m = 4$.

We set sg = sgn in the first case and sg = Sgn in the second case. In both cases, Remark 1.5 yields a short exact sequence

$$\mathbf{1} \to A_{(m)} \to S_m \xrightarrow{\mathrm{sg}} \mathrm{Aut}(A_{(m)}) \to \mathbf{1} \tag{4.6}$$

such that

$$\mathrm{sg}(S_{m-1}) = \mathrm{Aut}(A_{(m)}). \tag{4.7}$$

*Claim A. The normalizer of $N$ in $S$ is*

$$\tilde{G} = \big\{(\sigma_1, \ldots, \sigma_r) \in S_m^r \mid \mathrm{sg}(\sigma_1) = \cdots = \mathrm{sg}(\sigma_r)\big\}.$$

Indeed, consider $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_r) \in S_m^r$. For each $j \in \{1, \ldots, r\}$, we set $\tau_j = \mathrm{sg}(\sigma_j)$ and let $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_r)$. Then, for each $\mathbf{a} = (a, \ldots, a) \in N$, we have $\mathbf{a}^{\boldsymbol{\sigma}} = \mathbf{a}^{\boldsymbol{\tau}}$. Thus, $\mathbf{a}^{\sigma} \in N$ if and only if $a^{\tau_j} = a^{\tau_1}$ for $j = 1, \ldots, r$. Since $\tau_1, \ldots, \tau_r$ are automorphisms of $A_{(m)}$, this is true for all $\mathbf{a} \in N$ if and only if $\tau_j = \tau_1$ for $j = 1, \ldots, r$. Thus, $\mathrm{sg}(\sigma_1) = \cdots = \mathrm{sg}(\sigma_r)$, so $\boldsymbol{\sigma} \in \tilde{G}$. Therefore, $\tilde{G}$ is the normalizer of $N$ in $S$, as claimed.

*Claim B. $\tilde{G} = G$.*

Indeed, since $N$ is normal in $G$, we have by Claim A that $G \leq \tilde{G}$. By Lemma 3.5, $A = A_{(m)}^r \leq G$. Moreover, (4.6) yields a short exact sequence

$$\mathbf{1} \to A \to \tilde{G} \xrightarrow{\mathrm{sg}_1} \mathrm{Aut}(A_{(m)}) \to \mathbf{1}, \tag{4.8}$$

where $\mathrm{sg}_1(\boldsymbol{\sigma}) = \mathrm{sg}(\sigma_1)$. Hence, $(\tilde{G} : A) = |\mathrm{Aut}(A_{(m)})| = (S_m : A_{(m)})$. On the other hand, $\mathrm{pr}_1(G) = S_m$ and $\mathrm{pr}_1(A) = A_{(m)}$, so $(G : A) \geq (S_m : A_{(m)}) = (\tilde{G} : A)$. It follows from $A \leq G \leq \tilde{G}$ that $\tilde{G} = G$, as claimed.

*Claim C. The group $M = \{(\sigma_1, \ldots, \sigma_r) \in G \mid \sigma_1 \in S_{m-1}\}$ is a complement of $N$ in $G$.*

Indeed, by Remark 2.3 (c), $S_{m-1}$ is a complement of $A_{(m)}$ in $S_m$. If $\mathbf{a} = (a_1, \ldots, a_r) \in M \cap N$, then $a_1 \in S_{m-1}$ and $a_j = a_1 \in A_{(m)}$, so $a_j = 1$ for $j = 1, \ldots, r$. Thus, $M \cap N = \mathbf{1}$.

On the other hand, consider $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_r) \in G$. By Claim B, $\mathrm{sg}(\sigma_j) = \mathrm{sg}(\sigma_1)$ for $j = 1, \ldots, r$. By Remark 2.3 (c), $S_2 A_{(3)} = S_2 A_3 = S_3$ and $S_3 A_{(4)} = S_3 V_4 = S_4$. Hence, $\sigma_1 = \tau a$, with $\tau \in S_{m-1}$ and $a \in A_{(m)}$. By (4.6), $\mathrm{sg}(a) = 1$, so $\mathrm{sg}(\sigma_j a^{-1}) = \mathrm{sg}(\sigma_1) = \mathrm{sg}(\tau)$ for $j = 1, \ldots, r$. Hence, by Claim B, $\boldsymbol{\tau} = (\tau, \sigma_2 a^{-1}, \ldots, \sigma_r a^{-1}) \in \tilde{G} = G$. Moreover, by (4.5), $\mathbf{a} = (a, a, \ldots, a) \in N$ and $\boldsymbol{\sigma} = \boldsymbol{\tau}\mathbf{a} \in MN$. Thus, $G = M \ltimes N$, so $M$ is a complement of $N$ in $G$.

*Claim D. $M$ is symmetrically presentable.*

By definition, $M \leq S_{m-1} \times S_m^{r-1}$. If $\sigma_1 \in S_{m-1}$, then there exist $\sigma_2, \ldots, \sigma_r \in S_m$ such that $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_r) \in G$, because by assumption, $\mathrm{pr}_1(G) = S_m$. Hence, $\boldsymbol{\sigma} \in M$, so $\mathrm{pr}_1(M) = S_{m-1}$.

If $2 \leq i \leq r$ and $\sigma_i \in S_m$, we may assume that $i = 2$. By (4.6) and (4.7), there exists $\sigma_1 \in S_{m-1}$ such that $\mathrm{sg}(\sigma_1) = \mathrm{sg}(\sigma_2)$. Hence, with $\sigma_j = \sigma_1$ for $j = 3, \ldots, r$, we have by Claim B that $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_r) \in G$ and $\mathrm{pr}_2(\boldsymbol{\sigma}) = \sigma_2$. Therefore, $\boldsymbol{\sigma} \in M$, so $\mathrm{pr}_2(M) = S_m$. It follows that $M$ is symmetrically presentable, as claimed. □

**Lemma 4.3.** *Let $N$ be a minimal normal subgroup of a symmetrically presentable group $G$. Then, $N$ has a complement $M$ in $G$ and $G/N \cong M$ is symmetrically presentable.*

*Proof.* We assume without loss that $G \neq \mathbf{1}$ and that $\iota\colon G \to S$ is a minimal symmetric presentation of $G$. We also assume that $\iota$ is the inclusion map. Then, in the notation of Set-up 3.1, let $J = \{i \in I \mid N_{(i)} \neq \mathbf{1}\}$.

*Case A. $J = I$ and $|I| = 1$.*

Then, $G = S = S_{n_i}$, where $i$ is the unique element of $I$ and $N = A_{(n_i)}$. Hence, by Remark 2.3 (c), $N$ has a complement $M$ in $G$ which is a symmetric group. In particular, $G/N$ is symmetrically presentable.

*Case B. $J = I$ and $|I| > 1$.*

In view of Lemma 4.1 (b), there exist an integer $2 \leq m \leq 4$ and elements $\gamma_i \in \mathrm{Aut}(A_{(m)})$, for $i \in I$, such that $n_i = m$ for all $i \in I$ and

$$N = \bigl\{(a^{\gamma_i})_{i \in I} \in S \mid a \in A_{(m)}\bigr\}.$$

Then, in the notation of the second paragraph of the proof of Lemma 4.2 and by (4.6), there exists, for each $i \in I$, an element $\delta_i \in S_m$ such that $\mathrm{sg}(\delta_i) = \gamma_i$. Hence, $\boldsymbol{\delta} = (\delta_i)_{i \in I} \in S$, $N' = N^{\boldsymbol{\delta}^{-1}} = \bigl\{(a)_{i \in I} \mid a \in A_{(m)}\bigr\}$ is a minimal normal subgroup of $G' = G^{\boldsymbol{\delta}^{-1}}$. By Lemma 4.2, $N'$ has a complement $M'$ in $G'$ and $M'$ is symmetrically presentable. It follows that $M = (M')^{\delta}$ is a complement of $N$ in $G$ and $M$ is symmetrically presentable.

*Case C. $J$ is a proper subset of $I$.*

Let $J' = I \smallsetminus J$, $S_J = \prod_{j \in J} S_{n_j}$, and $S_{J'} = \prod_{j' \in J'} S_{n_{j'}}$. Then, $S = S_J \times S_{J'}$, and we set $\mathrm{pr}_J\colon S \to S_J$ and $\mathrm{pr}_{J'}\colon S \to S_{J'}$ to be the projection on the factors. Note that $\mathrm{Ker}(\mathrm{pr}_J) = S_{J'}$ and $\mathrm{Ker}(\mathrm{pr}_{J'}) = S_J$.

Now let $G_J = \mathrm{pr}_J(G)$. By Set-up 3.1, in particular, by the left diagram of (3.3) in that set-up, $\mathrm{pr}_{j'}(N) = \mathbf{1}$ for each $j' \in J'$, so $N \leq S_J$. Since $\mathrm{pr}_J$ is the identity map on $S_J$, we have $\mathrm{pr}_J(n) = n$ for each $n \in N$, so $N = \mathrm{pr}_J(N)$ is a minimal normal subgroup of $G_J$.

By induction on $|I|$, there is a symmetric presentation $\kappa\colon G_J/N \to \prod_{k \in K} S_{n_k}$, where $K$ is a finite set disjoint from $I$. Using $\kappa$, we define a map $\lambda\colon G/N \to \prod_{k \in K} S_{n_k} \times \prod_{j' \in J'} S_{n_{j'}}$ by $\lambda(gN) = (\kappa(\mathrm{pr}_J(g)N), \mathrm{pr}_{J'}(g))$ for each $g \in G$. We prove that $\lambda$ is a symmetric presentation.

Indeed, if $g_1N = g_2N$ for $g_1, g_2 \in G$, then $\mathrm{pr}_J(g_2^{-1}g_1) = g_2^{-1}g_1 \in N$, so $\mathrm{pr}_J(g_1)N = \mathrm{pr}_J(g_2)N$, hence $\lambda$ is well defined, therefore $\lambda$ is a homomorphism.

If $g \in G$ and $\lambda(gN) = 1$, then $\kappa(\mathrm{pr}_J(g)N) = 1$ and $\mathrm{pr}_{J'}(g) = 1$. The latter equality implies that $g \in S_J$, so $\mathrm{pr}_J(g) = g$. Since $\kappa$ is injective, $gN = \mathrm{pr}_J(g)N = 1$. Therefore, $\lambda$ is injective.

Since $\kappa$ is a symmetric presentation, there exists, for all $k \in K$ and $s \in S_{n_k}$, an element $g \in G$ such that $\mathrm{pr}_k(\lambda(gN)) = \mathrm{pr}_k(\kappa(\mathrm{pr}_J(g)N)) = s$. Also, if $j' \in J'$ and $s' \in S_{n_{j'}}$, then there exists $g \in G$ with $\mathrm{pr}_{j'}(g) = s'$. Hence, $\mathrm{pr}_{j'}(\lambda(gN)) = \mathrm{pr}_{j'}(\mathrm{pr}_{J'}(g)) = s'$. We conclude that $\lambda$ is a symmetric presentation of $G/N$.

Finally, since $|J| < |I|$, an induction hypothesis implies that $N$ has a complement $M_J$ in $G_J$. Hence, by Remark 2.2 (d), $M = \mathrm{pr}_J^{-1}(M_J) \cap G$ is a complement of $N$ in $G$. □

**Proposition 4.4.** *Let $N$ be a normal subgroup of a symmetrically presentable group $G$. Then, $N$ has a complement $M$ in $G$ and $G/N \cong M$ is symmetrically presentable.*

*Proof.* The case where $N$ is a minimal normal subgroup of $G$ is taken care of by Lemma 4.3. Hence, we assume without loss that $N \neq \mathbf{1}$ and $N$ is not a minimal normal subgroup of $G$. Then, $N$ has a proper subgroup $N_0$ which is a minimal normal subgroup of $G$. By Lemma 4.3, $G/N_0$ is symmetrically presentable. Since $N/N_0$ is a normal subgroup of $G/N_0$ and the order of $G/N_0$ is smaller than that of $G$, an induction hypothesis on the order of the group implies that $(G/N_0)/(N/N_0)$ is symmetrically presentable. Since $G/N \cong (G/N_0)/(N/N_0)$, the group $G/N$ is symmetrically presentable.

Again, by Lemma 4.3, $N_0$ has a complement $M_1$ in $G$. Then, $N_1 = M_1 \cap N$ is a normal subgroup of $M_1$ that complements $N_0$ in $N$, i.e. $N = N_1 \ltimes N_0$ (Remark 2.2 (c)). By the preceding paragraph, $M_1 \cong G/N_0$ is symmetrically presentable and $M_1 < G$. An induction on the order of the group yields a complement $M$ of $N_1$ in $M_1$. Then, by Remark 2.2 (b), $G = M_1 \ltimes N_0 = (M \ltimes N_1) \ltimes N_0 = M \ltimes (N_1 \ltimes N_0) = M \ltimes N$, as claimed. □

## 5. Embedding problems over a field

We quote two special results about the solvability of finite embedding problems over Hilbertian fields. Then, we introduce the notions of cartesian squares and fiber products of finite groups, and prove that the family of symmetrically presentable groups is closed under fiber products.

**Definition 5.1** (Regularly solvable embedding problems, [9, Def. 16.4.1])**.** Consider a *finite embedding problem* $\alpha\colon G \to \mathrm{Gal}(L/K)$ over a field $K$, where $L/K$ is a Galois extension, $G$ is a finite group, and $\alpha$ is an epimorphism. A *proper solution* of the embedding problem is an isomorphism $\beta\colon \mathrm{Gal}(N/K) \to G$ that satisfies $\alpha \circ \beta = \mathrm{res}_{N/L}$, where $N$ is a Galois extension of $K$ that contains $L$. We refer to $N$ as a *proper solution field* of the embedding problem.

Next we consider algebraically independent elements $t_1, \dots, t_r$ over $K$ and set $\mathbf{t} = (t_1, \dots, t_r)$. Then, res: $\mathrm{Gal}(L(\mathbf{t})/K(\mathbf{t})) \to \mathrm{Gal}(L/K)$ is an isomorphism. Hence, $\alpha\colon G \to \mathrm{Gal}(L/K)$ gives rise to an embedding problem $\alpha_{\mathbf{t}}\colon G \to \mathrm{Gal}(L(\mathbf{t})/K(\mathbf{t}))$ over $K(\mathbf{t})$ with $\alpha = \mathrm{res}_{L(\mathbf{t})/L} \circ \alpha_{\mathbf{t}}$. We refer to a proper solution of $\alpha_{\mathbf{t}}$ as a *proper solution* of $\alpha$ over $K(\mathbf{t})$. We refer to a proper solution field $F$ of $\alpha_{\mathbf{t}}$ as a *proper regular solution* of $\alpha$ if $F/L$ is regular. We say that $\alpha$ is *properly and regularly solvable* if there are $t_1, \dots, t_r$ as above such that $\alpha_{\mathbf{t}}$ has a proper solution field $F$ which is regular over $L$. In this case we also say that $L/K$ can be *properly and regularly embedded* into a $G$-extension.

**Definition 5.2.** A *finite embedding problem* for a profinite group $\Gamma$ is a pair

$$(\rho\colon \Gamma \to \bar{G},\ \alpha\colon G \to \bar{G}), \tag{5.1}$$

where $G$ is a finite group and both $\rho$ and $\alpha$ are epimorphisms. A *proper solution* of (5.1) is an epimorphism $\gamma\colon \Gamma \to G$ such that $\alpha \circ \gamma = \rho$.

Given a field $K$, we fix a separable algebraic closure $K_{\mathrm{sep}}$ of $K$ and let $\mathrm{Gal}(K) = \mathrm{Gal}(K_{\mathrm{sep}}/K)$ be the absolute Galois group of $K$. Then, we quote two lemmas from [9, Section 16.4].

**Lemma 5.3** ([9, p. 303, Lemma 16.4.2]). *Let $K$ be a Hilbertian field, $\alpha\colon G \to \mathrm{Gal}(L/K)$ a finite embedding problem, and $M$ a finite separable extension of $L$. If $\alpha$ is properly and regularly solvable, then $\alpha$ has a proper solution field $N$ which is linearly disjoint from $M$ over $L$.*

**Lemma 5.4** ([9, p. 304, Prop. 16.4.4]). *Let $G \ltimes A$ be a semi-direct product of finite groups, where $G = \mathrm{Gal}(L/K)$ for a Galois extension $L/K$ and $A$ is abelian. Let $\pi\colon G \ltimes A \to G$ be the projection map. Then, $\pi$ is properly and regularly solvable.*

We also quote a result of David Brink.

**Proposition 5.5** ([3, Thm. 9]). *Let $n \geq 3$ be an integer and $K$ a field of characteristic different from 2. Then, any quadratic extension $L/K$ can be properly and regularly embedded into an $S_n$-extension.*

Next, we recall that a commutative diagram

$$\begin{tikzcd} D \arrow[r, "\delta"] \arrow[d, "\beta"'] & C \arrow[d, "\gamma"] \\ B \arrow[r, "\alpha"] & A \end{tikzcd} \tag{5.2}$$

of profinite groups and homomorphisms is said to be *cartesian* if for each profinite group $G$ and all homomorphisms $\phi\colon G \to B$ and $\psi\colon G \to C$ satisfying $\alpha\circ\phi = \gamma\circ\psi$, there exists a unique homomorphism $\pi\colon G \to D$ such that $\beta\circ\pi = \phi$ and $\delta \circ \pi = \psi$.

Note that the map $\varepsilon$ of $D$ onto the *fiber product*

$$B \times_A C = \big\{(b, c) \in B \times C \mid \alpha(b) = \gamma(c)\big\}, \tag{5.3}$$

defined by $\varepsilon(d) = (\beta(d), \delta(d))$ for each $d \in D$, is an isomorphism that satisfies $\mathrm{pr}_B \circ \varepsilon = \beta$ and $\mathrm{pr}_C \circ \varepsilon = \delta$ [9, p. 499, Prop. 22.2.1].

We say that the fiber product (5.3) has *surjective homomorphisms* if both $\alpha$ and $\gamma$ are surjective.

**Lemma 5.6** ([9, p. 500, Lemma 22.2.4]). *Let* (5.2) *be a commutative diagram of epimorphisms of profinite groups. Then,* (5.2) *is cartesian if and only if* $\mathrm{Ker}(\alpha \circ \beta) = \mathrm{Ker}(\delta) \times \mathrm{Ker}(\beta)$.

Here is the field theoretic counterpart of Lemma 5.6:

**Lemma 5.7** ([9, p. 501, Example 22.2.7 (a)]). *Let $M$ and $M'$ be Galois extensions of a field $K$. Set $L = M \cap M'$ and $N = MM'$. Then, the square*

$$\begin{tikzcd} \mathrm{Gal}(N/K) \arrow[r] \arrow[d] & \mathrm{Gal}(M'/K) \arrow[d] \\ \mathrm{Gal}(M/K) \arrow[r] & \mathrm{Gal}(L/K), \end{tikzcd}$$

*in which all of the arrows are restriction maps is cartesian.*

Proposition 4.4 ensures that the family of symmetrically presentable groups is preserved under taking quotients. Here is another preservation rule for that family.

**Lemma 5.8.** *The family of symmetrically presentable groups is closed under fiber products with surjective homomorphisms.*

*Proof.* We consider the cartesian diagram (5.2) with the additional assumption that all homomorphisms are surjective. Suppose that $I$ and $J$ are disjoint finite sets, $\{n_i \mid i \in I\}$ and $\{n_j \mid j \in J\}$ are sets of positive integers, $B$ is a subgroup of $\prod_{i\in I} S_{n_i}$ with $\mathrm{pr}_i(B) = S_{n_i}$ for each $i \in I$, and $C$ is a subgroup of $\prod_{j\in J} S_{n_j}$, with $\mathrm{pr}_j(C) = S_{n_j}$ for each $j \in J$. Let $\lambda\colon D \to \prod_{i\in I} S_{n_i} \times \prod_{j\in J} S_{n_j}$ be the map defined by $\lambda(d) = (\mathrm{pr}_i(\beta(d)), \mathrm{pr}_j(\delta(d)))_{(i,j)\in I\times J}$ for each $d \in D$.

We assume without loss that $D = B \times_A C$, $\beta$ is the projection of $D$ on $B$, and $\delta$ is the projection of $D$ on $C$. If $\lambda(d) = 1$, then $\mathrm{pr}_i(\beta(d)) = 1$ for each $i \in I$, so $\beta(d) = 1$. Similarly, $\delta(d) = 1$. Hence, $(\beta(d), \delta(d))$ is the unit of $D$. Therefore, $d = 1$, so $\lambda$ is injective.

Also, if $s \in S_{n_i}$, with $i \in I$, then there exists $b \in B$ with $s = \mathrm{pr}_i(b)$. Let $c$ be an element of $C$ such that $\gamma(c) = \alpha(b)$. Then, $(b, c) \in D$ and $\mathrm{pr}_i(\lambda(b, c)) = \mathrm{pr}_i(b) = s$. Thus, $\mathrm{pr}_i(D) = S_{n_i}$ for each $i \in I$. Similarly, $\mathrm{pr}_j(D) = S_{n_j}$ for each $j \in J$. It follows that $\lambda$ is a symmetric presentation of $D$. □

## 6. Embedding problems for the absolute Galois group of a Hilbertian field

We prove in this section that every finite embedding problem

$$(\rho\colon \mathrm{Gal}(K) \to \bar{G},\ \alpha\colon G \to \bar{G}) \tag{6.1}$$

over a Hilbertian field $K$ of $\mathrm{char}(K) \neq 2$ in which $G$ is a symmetrically presentable group has a proper solution.

**Lemma 6.1.** *Let $K$ be a Hilbertian field of* $\mathrm{char}(K) \neq 2$. *Then, every finite embedding problem* (6.1) *in which $G$ is a symmetrically presentable group and $N = \mathrm{Ker}(\alpha)$ is a minimal normal subgroup of $G$ has a proper solution.*

*Proof.* As in Set-up 3.1, let $\iota\colon G \to S$ be a minimal symmetric presentation for $G$, with $S = \prod_{i\in I} S_{n_i}$, where $\iota$ is the inclusion map. By Lemma 4.3, $N$ has a complement in $G$. Hence, if $N$ is abelian, then, by Lemma 5.4 and Lemma 5.3, embedding problem (6.1) has a proper solution.

We may therefore assume that $N$ is nonabelian. Then, case (a) of Lemma 4.1 holds. Thus, there exists a unique $j \in I$ such that $N = A_{(n_j)}$. We assume without loss that $j = 1$ and set $n = n_1$. Since $N$ is nonabelian, Notation 1.3 implies that $n \geq 5$ and $N = A_n$. The rest of the proof consists of three parts.

*Part A. Commutative square.*

The assumptions made so far yield direct decompositions of groups

$$S = S_n \times S',\ \text{with } S' = \prod_{i\neq 1} S_{n_i}, \quad A = A_n \times A',\ \text{with } A' = \prod_{i\neq 1} A_{(n_i)}, \tag{6.2}$$

such that the projection $\phi = \mathrm{pr}_1|_G \colon G \to S_n$ is surjective. Note that $\phi$ maps the subgroup $A_n = N$ of $G$ identically onto the subgroup $A_n$ of $S_n$. Hence, for each $a \in A_n$ we have $\mathrm{sgn}(\phi(a)) = \mathrm{sgn}(a) = 1$. Therefore, there exists a homomorphism $\psi \colon \bar{G} \to \{\pm 1\}$ that makes the following diagram commutative:

(6.3)
$$\begin{tikzcd}
G \arrow[r, "\alpha"] \arrow[d, "\phi"'] & \bar{G} \arrow[d, "\psi"] \\
S_n \arrow[r, "\mathrm{sgn}"] & \{\pm 1\}.
\end{tikzcd}$$

*Claim B. The square* (6.3) *is cartesian.*

Since sgn, $\phi$, and $\alpha$ are surjective, so is $\psi$. Let $\beta = \psi \circ \alpha = \mathrm{sgn} \circ \phi$. Since $\mathrm{Ker}(\phi) \le \mathrm{Ker}(\mathrm{pr}_1) = S'$ and $\mathrm{Ker}(\alpha) = N = A_n \le S_n$, we have $\mathrm{Ker}(\phi) \cap \mathrm{Ker}(\alpha) = \mathbf{1}$. Thus, by Lemma 5.6, it suffices to prove that $\mathrm{Ker}(\beta) = \mathrm{Ker}(\phi)\mathrm{Ker}(\alpha)$.

Indeed, each $g \in \mathrm{Ker}(\beta)$ can be written as

(6.4)
$$g = as, \quad \text{with } a \in S_n \text{ and } s \in S'.$$

Hence, $\phi(g) = \mathrm{pr}_1(g) = a$, so $\mathrm{sgn}(a) = \mathrm{sgn}(\phi(g)) = \beta(g) = 1$. Therefore, $a \in A_n = \mathrm{Ker}(\alpha) \le G$, so, by (6.4), $s = a^{-1}g \in G$. Therefore,

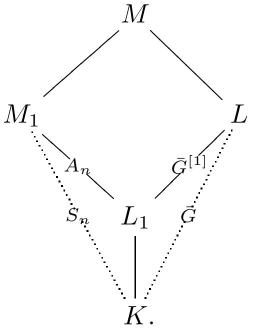
$$\phi(s) = \phi(a)^{-1}\phi(g) = a^{-1}\phi(g) = 1,$$

so $s \in \mathrm{Ker}(\phi)$, which proves our claim.

*Part C. Solving embedding problem* (6.1)*.*

Let $L$ be a Galois extension of $K$ with Galois group $\bar{G}$. Let $L_1$ be the fixed field of $\mathrm{Ker}(\psi \circ \rho)$. Then, $\mathrm{Gal}(L_1/K) \cong S_2$. By Proposition 5.5 and Lemma 5.3, $K$ has a Galois extension $M_1$ with Galois group $S_n$ such that $M_1$ contains $L_1$ and is linearly disjoint from $L$ over $L_1$. In particular, $\mathrm{Gal}(M_1/L_1) \cong A_n$. Moreover, since $\mathrm{sgn} \colon S_n \to \{\pm 1\}$ is the only epimorphism from $S_n$ to $\{\pm 1\}$, the restriction map $\mathrm{res}_{M_1/L_1}$ coincides with $\mathrm{sgn} \colon S_n \to \{\pm 1\}$. Finally, we set $M = M_1 L$ and have the following diagram of Galois extensions:

(6.5)



Since $M_1$ and $L$ are linearly disjoint over $L_1$, the corresponding commutative diagram of groups

$$\begin{tikzcd}
\mathrm{Gal}(M/K) \arrow[r] \arrow[d] & \mathrm{Gal}(L/K) \arrow[d] \\
\mathrm{Gal}(M_1/K) \arrow[r] & \mathrm{Gal}(L_1/K),
\end{tikzcd} \tag{6.6}$$

where all maps are restrictions, is cartesian (Lemma 5.7). Hence, diagram (6.3) is the Galois theoretic counterpart of diagram (6.6), so $M$ is a proper solution field of our embedding problem. □

**Proposition 6.2.** *Let $K$ be a Hilbertian field with* $\mathrm{char}(K) \neq 2$. *Then, every finite embedding problem*

$$(\rho\colon \mathrm{Gal}(K) \to \bar{G},\ \alpha\colon G \to \bar{G}), \tag{6.7}$$

*in which $G$ is a symmetrically presentable group, has a proper solution.*

*Proof.* Let $N = \mathrm{Ker}(\alpha)$. If $N = \mathbf{1}$, then $\alpha$ is an isomorphism, so $\alpha^{-1} \circ \rho$ is a proper solution of (6.7). If $N$ is a minimal normal subgroup of $G$, then Lemma 6.1 yields a proper solution of (6.7). Therefore, we may assume that $N$ is neither $\mathbf{1}$ nor minimal normal.

Then, $G$ has a nontrivial normal subgroup $N_0$ which is properly contained in $N$. Let $\pi\colon G \to G/N_0$ be the quotient map. Then, the epimorphism $\bar{\alpha}\colon G/N_0 \to \bar{G}$, defined by $\bar{\alpha}(gN_0) = \alpha(g)$, satisfies $\bar{\alpha} \circ \pi = \alpha$. Also, $N/N_0 = \mathrm{Ker}(\bar{\alpha})$ has a smaller order than $N = \mathrm{Ker}(\alpha)$. By Proposition 4.4, $G/N_0$ is also symmetrically presentable. Hence, by an induction hypothesis on the order of the kernel of the embedding problem, there exists an epimorphism $\bar{\rho}\colon \mathrm{Gal}(K) \to G/N_0$ such that $\bar{\alpha} \circ \bar{\rho} = \rho$. Next note that the order of $N_0 = \mathrm{Ker}(\pi)$ is also smaller than the order of $N$. Hence, another use of the induction hypothesis yields an epimorphism $\gamma\colon \mathrm{Gal}(K) \to G$ such that $\pi \circ \gamma = \bar{\rho}$:

$$\begin{tikzcd}
 & & & \mathrm{Gal}(K) \arrow[dl, "\gamma"'] \arrow[ddl, "\bar{\rho}"] \arrow[d, "\rho"] & \\
\mathbf{1} \arrow[r] & N \arrow[r] \arrow[d] & G \arrow[r, "\alpha"] \arrow[d, "\pi"] & \bar{G} \arrow[r] \arrow[d, equal] & \mathbf{1} \\
\mathbf{1} \arrow[r] & N/N_0 \arrow[r] & G/N_0 \arrow[r, "\bar{\alpha}"] & \bar{G} \arrow[r] & \mathbf{1}.
\end{tikzcd}$$

Then, $\alpha \circ \gamma = \bar{\alpha} \circ \pi \circ \gamma = \bar{\alpha} \circ \bar{\rho} = \rho$, so $\gamma$ is a proper solution of the embedding problem (6.7). □

## 7. The maximal symmetric extension of a field

We say that a Galois extension $L/K$ is *symmetric* if $\mathrm{Gal}(L/K) \cong S_n$ for some positive integer $n$. We denote the compositum of all symmetric extensions of a field $K$ by $K_{\mathrm{symm}}$ and prove that if $\mathrm{char}(K) \neq 2$, then $\mathrm{Gal}(K_{\mathrm{symm}}/K)$ is isomorphic to the free pro-$\mathcal{SP}$-group of rank $\aleph_0$, where $\mathcal{SP}$ is the formation of all symmetrically presentable groups.

**Lemma 7.1.** *The following conditions on a finite Galois extension $L/K$ are equivalent:*

(a) *$L$ is a compositum of finitely many symmetric extensions of $K$.*
(b) *$\mathrm{Gal}(L/K)$ is symmetrically presentable.*
(c) *$L$ is a finite Galois extension of $K$ in $K_{\mathrm{symm}}$.*

*Proof.* (a) ⇒ (b). Suppose that $L$ is a compositum of symmetric extensions $L_1, \dots, L_r$ of $K$. Then, the map $\sigma \mapsto (\mathrm{res}_{L/L_1}(\sigma), \dots, \mathrm{res}_{L/L_r}(\sigma))$ is an embedding of $\mathrm{Gal}(L/K)$ into $\prod_{i=1}^r \mathrm{Gal}(L_i/K)$. Moreover, the restriction map $\mathrm{res}_{L/L_i} \colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_i/K)$ is surjective for $i = 1, \dots, r$. Therefore, $\mathrm{Gal}(L/K)$ is symmetrically presentable.

(b) ⇒ (a). Suppose that $G = \mathrm{Gal}(L/K)$ has a symmetric presentation $\iota \colon G \to \prod_{i=1}^r S_{n_i}$. Without loss we assume that $\iota$ is the inclusion map. For each $1 \leq i \leq r$, let $L_i$ be the fixed field in $L$ of the kernel of the epimorphism $\mathrm{pr}_i|_G \colon G \to S_{n_i}$. Then, $\mathrm{Gal}(L_i/K) \cong S_{n_i}$ and $\mathrm{Gal}(L/L_i) \leq \prod_{j \neq i} S_{n_j}$. Hence, $\bigcap_{i=1}^r \mathrm{Gal}(L/L_i) \leq \bigcap_{i=1}^r \prod_{j\neq i} S_{n_j} = \mathbf{1}$. Therefore, $L = L_1 \cdots L_r$. We conclude that $L$ is a compositum of symmetric extensions.

(a) ⇒ (c). If $L$ is a compositum of symmetric extensions $L_1, \dots, L_r$, then $L \subseteq K_{\mathrm{symm}}$.

(c) ⇒ (a). Suppose that $L$ is a finite Galois extension of $K$ in $K_{\mathrm{symm}}$. Then, there exist symmetric extensions $N_1, \dots, N_r$ of $K$ such that $N = N_1 \cdots N_r$ contains $L$. By "(a) ⇒ (b)", $\mathrm{Gal}(N/L)$ is symmetrically presentable. Hence, $\mathrm{Gal}(L/K)$ is a quotient of a symmetrically presentable group, so, by Proposition 4.4, $\mathrm{Gal}(L/K)$ is symmetrically presentable. By "(b) ⇒ (a)", $L$ is a compositum of finitely many symmetric extensions of $K$, as claimed. □

**Corollary 7.2.** *Let $K$ be a Hilbertian field with* $\mathrm{char}(K) \neq 2$ *and let $G$ be a symmetrically presented group. Then, every finite embedding problem $(\bar{\rho} \colon \mathrm{Gal}(K_{\mathrm{symm}}/K) \to \bar{G},\ \alpha \colon G \to \bar{G})$ is properly solvable. In particular, $G$ itself is a quotient of* $\mathrm{Gal}(K_{\mathrm{symm}}/K)$.

*Proof.* Let $\rho = \bar{\rho} \circ \mathrm{res}_{K_{\mathrm{sep}}/K_{\mathrm{symm}}}$. By Proposition 6.2, there exists an epimorphism $\gamma \colon \mathrm{Gal}(K) \to G$ such that $\alpha \circ \gamma = \rho$. Let $N$ be the fixed field of $\mathrm{Ker}(\rho)$. Then, $\mathrm{Gal}(N/K) \cong G$, so, by Lemma 7.1, $N \subseteq K_{\mathrm{symm}}$. Hence, there exists an epimorphism $\bar{\gamma} \colon \mathrm{Gal}(K_{\mathrm{symm}}/K) \to G$ that solves the given embedding problem.

Finally, considering the embedding problem

$$(\mathrm{Gal}(K_{\mathrm{symm}}/K) \to \mathbf{1},\ G \to \mathbf{1}),$$

we have, by the preceding paragraph, that $G$ is a quotient of $\mathrm{Gal}(K_{\mathrm{symm}}/K)$, as claimed. □

**Remark 7.3** (The formation of all symmetrically presentable groups)**.** We denote the family of all symmetrically presentable groups (up to isomorphisms) by $\mathcal{SP}$. By Proposition 4.4, $\mathcal{SP}$ is closed under taking quotients. By Lemma 5.8, $\mathcal{SP}$ is closed under taking fiber products with surjective homomorphisms. Hence, in the terminology of [9, p. 344], $\mathcal{SP}$ is a *formation of finite groups.* It is the smallest formation of finite groups that contains all symmetric groups.

Each inverse limit of $\mathcal{SP}$-groups in which the connecting homomorphisms are epimorphisms is a *pro-$\mathcal{SP}$-group* [9, p. 344]. In particular, for each set $X$, there exists a free pro-$\mathcal{SP}$-group $\hat{F}_X(\mathcal{SP})$ *on* $X$. Thus, there exists a map $\iota\colon X \to \hat{F}_X(\mathcal{SP})$ that converges to 1 such that $\iota(X)$ generates $\hat{F}_X(\mathcal{SP})$, and for each map $\phi$ of $X$ into a pro-$\mathcal{SP}$-group $G$ that converges to 1 and satisfies $G = \langle\phi(X)\rangle$, there exists a unique epimorphism $\hat{\phi}\colon \hat{F}_X(\mathcal{SP}) \to G$ with $\hat{\phi}\circ\iota = \phi$.

Since $S_2^n \in \mathcal{SP}$ for each positive integer $n$, it follows from [9, p. 346, Prop. 17.4.2 and p. 348, Lemma 7.4.6 (a)] that there exists a free pro-$\mathcal{SP}$-group $\hat{F}_\omega(\mathcal{SP})$ of rank $\aleph_0$.

**Remark 7.4** (The embedding property)**.** We denote the set of all finite quotients (up to isomorphisms) of a profinite group $G$ by $\mathrm{Im}(G)$. We say that $G$ has the *embedding property* if every finite embedding problem ($\phi\colon G \to A$, $\alpha\colon B \to A$), with $B \in \mathrm{Im}(G)$, has a proper solution [9, p. 564, Def. 24.1.2].

**Theorem 7.5.** *Let $K$ be a countable Hilbertian field with* $\mathrm{char}(K) \neq 2$. *Then,*

$$\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \hat{F}_\omega(\mathcal{SP}).$$

*Hence,* $\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q})$ *and* $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}}/K)) = \mathcal{SP}$.

*Proof.* By Remark 7.3, $\mathcal{SP}$ is a formation of finite groups. By Lemma 7.1, each finite quotient of $\mathrm{Gal}(K_{\mathrm{symm}}/K)$ belongs to $\mathcal{SP}$. Conversely, by Corollary 7.2, each $G \in \mathcal{SP}$ is a quotient of $\mathrm{Gal}(K_{\mathrm{symm}}/K)$. Hence, $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}}/K)) = \mathcal{SP}$. Therefore, by Corollary 7.2, $\mathrm{Gal}(K_{\mathrm{symm}}/K)$ has the embedding property. Since $K$ is countable, $\mathrm{rank}(\mathrm{Gal}(K_{\mathrm{symm}}/K)) \leq \aleph_0$.

It follows from a generalization of a theorem of Iwasawa, see [9, p. 581, Thm. 24.8.1], that

$$\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \hat{F}_\omega(\mathcal{SP}).$$

In particular, since $\mathbb{Q}$ is countable and Hilbertian, $\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q}) \cong \hat{F}_\omega(\mathcal{SP})$. Therefore, $\mathrm{Gal}(\mathbb{Q}_{\mathrm{symm}}/\mathbb{Q}) \cong \mathrm{Gal}(K_{\mathrm{symm}}/K)$. □

**Remark 7.6.** For a Hilbertian field $K$, [1, Theorem 3.2] implies that every field $M$ between $K$ and $K_{\mathrm{symm}}$ is Hilbertian.

## 8. Decidability

Let $K$ be a *presented field* in the sense of [9, p. 404, Def. 19.1.1]. This is a field which is "explicitly constructed" from the ring $\mathbb{Z}$ of integers, one has "effective recipes" to add and multiply given elements and to "effectively compute" the inverse of each given nonzero element. An element $z$ of a field extension $F$ of $K$

is *presented over* $K$ if either $z$ is algebraic over $K$ and $\mathrm{irr}(z, K)$ is explicitly given or it is known that $z$ is transcendental over $K$.

We say that $K$ has a *splitting algorithm* if $K$ has an effective algorithm for factoring each polynomial in $K[X]$ of positive degree into a product of irreducible factors. By [9, p. 409, Lemma 19.2.4], every presented finitely generated separable extension of a field $K$ with a splitting algorithm has a splitting algorithm. Given a separable polynomial $f(X)$ with coefficients in a presented field $K$, we can present the splitting field $L$ of $f$ over $K$ and compute the Galois group $\mathrm{Gal}(L/K)$ as a group of permutations of the roots of $f$. Moreover, we can find all of the subgroups of $\mathrm{Gal}(L/K)$ and compute their fixed fields in $L$ [9, p. 412, Lemma 19.3.2].

If every finitely generated presented extension of $K$ has a splitting algorithm, we say that $K$ has *elimination theory.* By [9, p. 411, Cor. 19.2.10], if $K_0$ is a presented perfect field with a splitting algorithm, then $K_0$ has elimination theory. In particular, since each of the fields $\mathbb{Q}$ and $\mathbb{F}_p$ (where $p$ is a prime number) has a splitting algorithm, every finitely generated presented field extension $K$ of its prime field has elimination theory.

We denote the maximal purely inseparable extension of a field $F$ by $F_{\mathrm{ins}}$.

**Lemma 8.1.** *Let $K$ be a presented field with elimination theory and let $f$ be a polynomial of positive degree in $K[X]$. Then,*

(a) *we can effectively check whether $f$ has a root in $K_{\mathrm{symm}}$, and*
(b) *we can effectively check whether $f$ has a root in $K_{\mathrm{symm,ins}}$.*

*Proof.* Since $K$ has elimination theory, we can effectively decompose $f$ over $K$ into a product of irreducible polynomials, $f = \prod_{i=1}^r f_i$. Then, $f$ has a root in $K_{\mathrm{symm}}$ if and only if at least one of the polynomials $f_i$ has a root in $K_{\mathrm{symm}}$. Thus, we may assume without loss that $f$ is irreducible in $K[X]$.

In this case, all roots of $f$ are in $K_{\mathrm{sep}}$ if and only if $f' \neq 0$. By [9, p. 412, Lemma 19.3.2], we may effectively construct the splitting field $N$ of $f$ over $K$. Moreover, we can effectively find all symmetric extensions $L_1, \ldots, L_r$ of $K$ in $N$ and check whether $N = \prod_{i=1}^r L_i$. By Lemma 7.1, $f$ has a root in $K_{\mathrm{symm}}$ if and only if $N = \prod_{i=1}^r L_i$. This proves (a).

Next assume that $p = \mathrm{char}(K) > 0$ and find a power $q$ of $p$ and a separable polynomial $g \in K[X]$ such that $f(X) = g(X^q)$. Then, $f$ has a root in $K_{\mathrm{symm,ins}}$ if and only if $g$ has a root in $K_{\mathrm{symm}}$. The latter can be effectively checked by (a). □

**Remark 8.2.** Given a presented field $K$, we write $\mathcal{L}(\mathrm{ring}, K)$ for the first order language of the theory of rings with a constant symbol for each element of $K$ [9, p. 135, Example 7.3.1]. If $M$ is an extension of $K$, we write $\mathrm{Th}(M)$ for the set of all first order sentences in $\mathcal{L}(\mathrm{ring}, K)$ that are true in $M$ and $\mathrm{Root}(M/K)$ for the set of monic polynomials in $K[X]$ that have a root in $M$. Finally, we write $\tilde{K}$ for a fixed algebraic closure of $K$ containing $K_{\mathrm{symm}}$ and $K_{\mathrm{ins}}$ and note that it can also be effectively presented [9, p. 413, Lemma 19.4.1]. Every other algebraic extension of $K$ is considered to be contained in $\tilde{K}$.

We write FiniteGroups for the set of all finite groups up to isomorphisms. We also write $\hat{F}_\omega$ for the free profinite group with countably many generators and note that, by [9, p. 568, Lemma 24.3.3], $\hat{F}_\omega$ has the embedding property. Moreover, $\mathrm{Im}(\hat{F}_\omega) = \mathrm{FiniteGroups}$.

Recall that a field $M$ is *PAC* if every absolutely integral algebraic variety over $M$ has an $M$-rational point.

**Lemma 8.3** ([14, Lemma 3.3])**.** *Let $K$ be a presented field with elimination theory. Let $M$ be an extension of $K$ in $\tilde{K}$. Suppose that $M$ is perfect and PAC,* $\mathrm{Gal}(M)$ *has the embedding property, and* $\mathrm{Im}(\mathrm{Gal}(M))$ *is a primitive recursive subset of* FiniteGroups*. Further, suppose that the set* $\mathrm{Root}(M/K)$ *is primitive recursive. Then,* $\mathrm{Th}(M)$ *is primitive recursive.*

By Remark 8.2, $\hat{F}_\omega$ has the embedding property. Since the set $\mathrm{Im}(\hat{F}_\omega)$ consists of all finite groups, it is primitive recursive. Thus, the following result is a special case of Lemma 8.3.

**Lemma 8.4.** *Let $K$ be a presented field with elimination theory. Let $M$ be an extension of $K$ in $\tilde{K}$. Suppose that $M$ is perfect, PAC, and* $\mathrm{Gal}(M) \cong \hat{F}_\omega$*. Further, suppose that the set* $\mathrm{Root}(M/K)$ *is primitive recursive. Then,* $\mathrm{Th}(M)$ *is primitive recursive.*

With this we reach our next main result.

**Theorem 8.5.** *Let $K$ be a Hilbertian presented field with elimination theory. Then:*

(a) $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$*, so* $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}})) = \mathrm{FiniteGroups}$.
(b) $\mathrm{Th}(K_{\mathrm{symm,ins}})$ *is primitive recursive.*
(c) *If* $\mathrm{char}(K) \neq 2$*, then* $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}}/K))$ *is primitive recursive.*

*Proof.* By [9, p. 396, Thm. 18.10.4], $K_{\mathrm{symm}}$ is PAC and Hilbertian. Since $K$ is presented, $K$ is countable [9, p. 404], so $K_{\mathrm{symm}}$ is countable. By [10, Thm. A] (in case $\mathrm{char}(K) = 0$), or [15, Thm. 1], [11, Cor. 4.7], and [13, p. 90, Thm. 5.10.3] (in general), $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$. Since $K_{\mathrm{symm,ins}}/K_{\mathrm{symm}}$ is a purely inseparable extension, we also have $\mathrm{Gal}(K_{\mathrm{symm,ins}}) \cong \hat{F}_\omega$. It follows from [9, p. 195, Thm. 11.2.3] that $K_{\mathrm{symm,ins}}$ is also PAC. In addition, $K_{\mathrm{symm,ins}}$ is a perfect field.

By Lemma 8.1, the set $\mathrm{Root}(K_{\mathrm{symm,ins}}/K)$ is primitive recursive. It follows from Lemma 8.4 that $\mathrm{Th}(K_{\mathrm{symm,ins}})$ is primitive recursive.

Finally, if $\mathrm{char}(K) \neq 2$, then, by Theorem 7.5, $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}}/K)) = \mathcal{SP}$. It follows from Remark 3.6 that $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}}/K))$ is primitive recursive. □

**Remark 8.6.** In a subsequent paper, we prove that the theory of the ring of integers of $\mathbb{Q}_{\mathrm{symm}}$ and the theory of the ring of integers of $\mathbb{F}_p(t)_{\mathrm{symm,ins}}$ are primitive recursive.

## 9. More examples

It turns out that the same methods that led to Theorems 7.5 and 8.5 lead to a decreasing sequence of field extensions of $K$ with similar properties to those of $K_{\mathrm{symm}}$.

**Example 9.1.** Let $K$ be a field and $m$ a positive integer. We define $K_{\mathrm{symm}}^{(m)}$ as the compositum of all Galois extensions of $K$ with Galois groups $S_n$ for some $n \geq m$. In particular, $K_{\mathrm{symm}} = K_{\mathrm{symm}}^{(2)}$. Also, $K_{\mathrm{symm}}^{(m+1)} \subseteq K_{\mathrm{symm}}^{(m)}$ for each $m$.

Suppose that $K$ is Hilbertian. Then, by [9, p. 396, Thm. 18.10.4], $K_{\mathrm{symm}}$ is PAC and Hilbertian. A mild change of the proof of that theorem proves that for each positive integer $m$ also $K_{\mathrm{symm}}^{(m)}$ is PAC and Hilbertian. Indeed, if $C$ is an absolutely integral affine plane curve over $K$ with function field $F$, then $F/K$ has a separating transcendence element $t$ such that $[F : K(t)] = n \geq m$ and the Galois hull $\hat{F}$ of $F/K(t)$ satisfies $\mathrm{Gal}(\hat{F}/K(t)) \cong S_n$, see [9, p. 391, Thm. 18.9.3]. By the Hilbertianity of $K$, there exists $a \in K$ such that the specialization $t \to a$ extends to a $K$-place of $F$ into $K_{\mathrm{symm}}^{(m)}$ that leads to a $K_{\mathrm{symm}}^{(m)}$-rational point of $C$ [9, p. 231, Lemma 13.1.1]. This implies that $K_{\mathrm{symm}}^{(m)}$ is PAC.

By applying Haran's diamond theorem, one proves as in [FrJ08, p. 396, Thm. 18.10.4] that $K_{\mathrm{symm}}^{(m)}$ is Hilbertian. Alternatively, one may apply Remark 7.6. If in addition, $K$ is countable, then so is $K_{\mathrm{symm}}^{(m)}$. Hence, by [13, p. 89, Thm. 5.10.2 (c)], $\mathrm{Gal}(K_{\mathrm{symm}}^{(m)}) \cong \hat{F}_\omega$. In particular, $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}}^{(m)}))$ is the set of all finite groups. As in Remark 3.6, one observes that $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm}}^{(m)}/K))$ is a primitive recursive set of finite groups.

If in addition, $K$ is a presented field with elimination theory, then the proof of Lemma 8.1 can be applied to primitive recursively decide whether a given separable polynomial $f \in K[X]$ has a root in $K_{\mathrm{symm,ins}}^{(m)}$.

By Lemma 8.3, $\mathrm{Th}(K_{\mathrm{symm,ins}}^{(m)})$ is primitive recursively decidable.

**Remark 9.2.** Let $K$ be a countable Hilbertian field with $\mathrm{char}(K) \neq 2$ and let $m \geq 5$ be an integer. By Lemma 5.3 and Proposition 5.5, every $S_2$-extension of $K$ can be embedded in an $S_m$-extension of $K$. Similarly to the notation $\mathcal{SP}$ introduced in Remark 7.3, let $\mathcal{SP}^{(m)}$ be the formation of all subdirect products of the groups $S_2, S_m, S_{m+1}, S_{m+2}, \ldots$, and let $\hat{F}_\omega(\mathcal{SP}^{(m)})$ be the free pro-$\mathcal{SP}^{(m)}$-group of rank $\aleph_0$. As in Theorem 7.5, we can prove that $\mathrm{Gal}(K_{\mathrm{symm}}^{(m)}/K) \cong \hat{F}_\omega(\mathcal{SP}^{(m)})$.

We add the following observation:

**Proposition 9.3.** *Let $K$ be a Hilbertian field of characteristic $\neq 2$. Let $K^{(2)}$ be the compositum of all quadratic extensions of $K$. Then, $\bigcap_{m\geq 5} K_{\mathrm{symm}}^{(m)} = K^{(2)}$.*

*Proof.* Let $N = \bigcap_{m\geq 5} K_{\mathrm{symm}}^{(m)}$. By Lemma 5.3 and Proposition 5.5, for each $m \geq 3$, every quadratic extension of $K$ can be embedded into an $S_m$-extension of $K$. Hence, $K^{(2)} \subseteq N$.

On the other hand, let $G$ be a finite quotient of $\mathrm{Gal}(N/K)$. For each $m \geq 5$, we set $\mathcal{Q}_m = \{S_2, A_m, A_{m+1}, A_{m+2}, \ldots\}$. Then, there exist Galois extensions

$L_1, \dots, L_r$ of $K$ such that $\mathrm{Gal}(L_i/K) \cong S_{n_i}$, with $n_i \geq m$ for $i = 1, \dots, r$, and $G$ is a quotient of $\mathrm{Gal}(L/K)$, where $L = L_1 \cdots L_r$. By Set-up 1.1 (a), the composition factors of each $S_{n_i}$ are $A_{n_i}$ and $S_2$. Hence, the composition factors of $\mathrm{Gal}(L/K)$ belong to $\mathcal{Q}_m$, therefore so are the composition factors of $G$. Since $\bigcap_{m=5}^{\infty} \mathcal{Q}_m = \{S_2\}$, every composition factor of $G$ is isomorphic to $S_2$.

By Lemma 7.1, $G$ is symmetrically presentable. Thus, $G$ is contained in a direct product $\prod_{j \in J} S_{n_j}$, where $J$ is a finite set and $n_j \geq 2$ is an integer for each $j \in J$. Moreover, each $S_{n_j}$ is a quotient of $G$. Since $A_3$ is a composition factor of both $S_3$ and $S_4$, it follows from the preceding paragraph that $n_j = 2$ for each $j \in J$. Therefore, $G \cong S_2^p$ for some nonnegative integer $p$. We conclude that $N = K^{(2)}$, as claimed. □

**Example 9.4** (Galois extensions of $\mathbb{Q}$ with Galois group $S = \prod_{n=2}^{\infty} S_n$)**.** Remark 1 of [10] yields a sequence of irreducible polynomials $f_2, f_3, f_4, \dots$ in $\mathbb{Q}[X]$ with linearly disjoint splitting fields $N_2, N_3, N_4, \dots$ having Galois groups $S_2, S_3, S_4, \dots$. Thus, with $N = \prod_{n=2}^{\infty} N_n$, we have $\mathrm{Gal}(N/\mathbb{Q}) \cong \prod_{n=2}^{\infty} S_n$. Moreover, $N$ is both PAC and Hilbertian. It follows from [10, Thm. A] that $\mathrm{Gal}(N) \cong \hat{F}_\omega$. Hence, $\mathrm{Im}(\mathrm{Gal}(N)) = \mathrm{FiniteGroups}$ is primitive recursive.

Next note that if $\phi$ is an epimorphism of $S$ onto a finite group $G$, then $G$ is generated by the subgroups $G_n = \phi(S_n)$, $n = 2, 3, 4, \dots$, of $G$,

(1) every $G_n$ is normal in $G$,
(2) for all $m < n$, the elements of $G_m$ commute with the elements of $G_n$.

Moreover, by Fact 1.1 (a), (b),

(3a) $G_2 = \mathbf{1}$ or $G_2 = S_2$,
(3b) $G_3 = \mathbf{1}$, or $G_3 = S_2$, or $G_3 = S_3$,
(3c) $G_4 = \mathbf{1}$, or $G_4 = S_2$, or $G_4 = S_3$, or $G_4 = S_4$, and
(3d) for all $n \geq 5$, $G_n = \mathbf{1}$, or $G_n = S_2$, or $G_n = S_n$.

Conversely, if a finite group $G$ is generated by subgroups $G_2, G_3, G_4, \dots$, only finitely of them are nontrivial, and they satisfy conditions (1), (2), and (3), then $G$ is a quotient of $S$. It follows that also $\mathrm{Im}(\mathrm{Gal}(N/\mathbb{Q}))$ is a primitive recursive subset of FiniteGroups.

It is conceivable that one may construct $N$ such that, in addition to the above mentioned properties, it will be a primitive recursive extension of $\mathbb{Q}$. One possible way to do it is, for every effectively given finitely generated regular extension $F$ of $\mathbb{Q}$ of transcendence degree 1 and for every positive integer $n_0$, to effectively construct a transcendental element $t$ for $F/\mathbb{Q}$ and effectively compute an integer $n \geq n_0$ such that the Galois closure $\hat{F}$ of $F/\mathbb{Q}(t)$ will be regular over $\mathbb{Q}$ and $\mathrm{Gal}(\hat{F}/\mathbb{Q}(t)) \cong S_n$. To this end, one may try to effectivize the noneffective proof of this statement given in [8] combined with [10, Remark 1]. In addition, one would have at some point to use an effective version of Hilbert irreducibility theorem (e.g., [16]).

Obviously, this task goes beyond the scope of the present work.

**Acknowledgement.** The authors thank the anonymous referee for his thoughtful comments and advise.

## References

[1] L. Bary-Soroker, A. Fehm, and G. Wiese, Hilbertian fields and Galois representations, J. Reine Angew. Math. **712** (2016), 123–139. MR3466550

[2] G. Birkhoff, Subdirect unions in universal algebra, Bull. Amer. Math. Soc. **50** (1944), 764–768. MR0010542

[3] D. Brink, On alternating and symmetric groups as Galois groups, Israel J. Math. **142** (2004), 47–60. MR2085710

[4] L. van den Dries, New decidable fields of algebraic numbers, Proc. Amer. Math. Soc. **77** (1979), no. 2, 251–256. MR0542093

[5] Yu. L. Ershov, Nice local-global fields I, Algebra and Logic **35** (1996), no. 4, 229–235; translated from Algebra i Logika **35** (1996), no. 4, 411–423, 497. MR1444427

[6] A. Fehm, The elementary theory of large fields of totally $\mathfrak{S}$-adic numbers, J. Inst. Math. Jussieu **16** (2017), no. 1, 121–154. MR3591963

[7] M. D. Fried, D. Haran, and H. Völklein, Real Hilbertianity and the field of totally real numbers, in *Arithmetic geometry (Tempe, AZ, 1993)*, 1–34, Contemp. Math., 174 (1994), Amer. Math. Soc., Providence, RI, 1994. MR1299732

[8] M. D. Fried and M. Jarden, Diophantine properties of subfields of $\tilde{\mathbb{Q}}$, Amer. J. Math. **100** (1978), no. 3, 653–666. MR0501232

[9] M. D. Fried and M. Jarden, *Field arithmetic*, third edition, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 11, Springer-Verlag, Berlin, 2008. MR2445111

[10] M. D. Fried and H. Völklein, The embedding problem over a Hilbertian PAC-field, Ann. of Math. (2) **135** (1992), no. 3, 469–481. MR1166641

[11] D. Haran and H. Völklein, Galois groups over complete valued fields, Israel J. Math. **93** (1996), 9–27. MR1380632

[12] D. Harbater, Fundamental groups and embedding problems in characteristic $p$, in *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, 353–369, Contemp. Math., 186, Amer. Math. Soc., Providence, RI, 1995. MR1352282

[13] M. Jarden, *Algebraic patching*, Springer Monographs in Mathematics, Springer, Heidelberg, 2011. MR2768285

[14] M. Jarden and A. Shlapentokh, Decidable algebraic fields, J. Symb. Log. **82** (2017), no. 2, 474–488. MR3663413

[15] F. Pop, Embedding problems over large fields, Ann. of Math. (2) **144** (1996), no. 1, 1–34. MR1405941

[16] Y. Walkowiak, Théorème d'irréductibilité de Hilbert effectif, Acta Arith. **116** (2005), no. 4, 343–362. MR2110508

Received July 23, 2018; accepted October 15, 2018

Wulf-Dieter Geyer
Universität Erlangen, Cauerstr. 11, 91058 Erlangen, Germany
E-mail: geyer@mi.uni-erlangen.de

Moshe Jarden
Tel Aviv University, Ramat Aviv, Tel Aviv, Israel
E-mail: jarden@post.tau.ac.il

Aharon Razon
Elta Industry, Ashdod, Israel
E-mail: razona@elta.co.il