Composita of Symmetric Extensions of $\mathbb{Q}$

by

Wulf-Dieter Geyer, Erlangen University, geyer@mi.uni-erlangen.de,
Moshe Jarden, Tel Aviv University, jarden@post.tau.ac.il, and
Aharon Razon, Elta, razona@elta.co.il

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

MR Classification: 12E30
Directory: \Jarden\Diary\Composita
14 October 2018

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 [Hrb95, Cor. 4.2], [Pop96, Thm. 1], [HaV96, Cor. 4.7], and also [Jar11, 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 [Feh17, Thm. 1.1]. Moreover, if S and S' are finite sets of prime numbers such that $S \cap S' \neq \emptyset$, then also $\mathbb{Q}_{\mathrm{tot},S}\mathbb{Q}_{\mathrm{tot},S'}$ is decidable [Ers96, Theorem' below Proposition 5].

In addition, every finite extension of the above mentioned fields is decidable [Dri79, Sec. 3, Cor.].

Taking $S = \emptyset$, 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 [FrJ08, p. 168, Thm. 9.3.1(c)] and [FHV94, 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 [JaS17, 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 [FrJ08, 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_{symm} replacing K_{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 [FrJ08, Section 17.3]. Hence, there exists a unique (up to isomorphism) **free pro-$\mathcal{C}$-group** $\hat{F}_\omega(\mathcal{SP})$ of rank $\aleph_0$ [FrJ08, 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 proof of Theorem 8.5).

Finally, we realize that K_{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_{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.

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

1. Symmetric Groups

SYMM
input, 15

As usual, for each positive integer n we denote the group of all permutations of the set $\{1, \ldots, n\}$ 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 $\{1, \ldots, n\}$. We also mention the **Klein four-group** $V_4 = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

FACt
input, 38

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) *$S_2 \cong C_2$ is abelian. Hence, the center $Z(S_2)$ of S_2 is S_2. If $n \geq 3$, then $Z(S_n) = \mathbf{1}$.*

(d) *For $n = 3$ we have $A_3 \cong C_3$. If $n \geq 5$, then A_n is non-abelian. In both cases A_n is a simple group.*

(e) *The only normal subgroups of A_4 are $\mathbf{1}$, V_4, and A_4 with respective quotients A_4, A_3, and $\mathbf{1}$.*

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

PROa
input, 87

LEMMA 1.2: *Every quotient group of a symmetric group is a symmetric group.*

Recall that a non-trivial 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

MINi input, 99

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

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 non-abelian simple group (Fact 1.1(d)). 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

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

Notation 1.4: A direct product of symmetric groups has the form

DIRa input, 131

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

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 ith coordinate. Thus, for $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_r)$ we have $\mathrm{pr}_i(\boldsymbol{\sigma}) = \sigma_i$. The kernel of 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

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

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

SIGa input, 162

Since $A_3 \cong C_3$ (Fact 1.1(d)), $\mathrm{Aut}(A_3) \cong C_2$ 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 σ 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 $\mathbf{1} \longrightarrow A_3 \longrightarrow S_3 \stackrel{\text{sgn}}{\longrightarrow} \text{Aut}(A_3) \longrightarrow \mathbf{1}$. Since $\text{sgn}(1\,2) = -1$, we also have that sgn maps S_2 bijectively onto $\text{Aut}(A_3)$.

For $n = 4$ and for $\sigma \in S_4$, we define $\text{Sgn}(\sigma)$ to be the automorphism of V_4 defined by conjugation with σ. Since V_4 is abelian, $V_4 \leq \text{Ker}(\text{Sgn})$. 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 $|\text{Aut}(V_4)| = 6 = |S_3|$. Hence, Sgn maps S_3 bijectively onto $\text{Aut}(V_4)$. Finally, since $(S_4 : V_4) = 6$ (Fact 1.1(b)), we find that $V_4 = \text{Ker}(\text{Sgn})$. This leads to the following short exact sequence $\mathbf{1} \longrightarrow V_4 \longrightarrow S_4 \stackrel{\text{Sgn}}{\longrightarrow} \text{Aut}(V_4) \longrightarrow \mathbf{1}$. ∎

2. Semi-direct Products.

AUTOM
input, 14

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 $\alpha \in \text{Aut}(A)$ we write a^α for the image of a under α. Thus, $(ab)^\alpha = a^\alpha b^\alpha$ for $a, b \in A$ and $a^{\alpha\beta} = (a^\alpha)^\beta$. ∎

AUTa
input, 20

Remark 2.2: Semi-direct Products.

AUTb
input, 28

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

Indeed, each $n \in M \cap N$ satisfies $\varphi(n) \in \bar{M} \cap \bar{N}$, hence $\varphi(n) = 1$, 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 $\varphi(g) = \bar{m}\varphi(n)$. Thus, $\varphi(gn^{-1}) = \bar{m} \in \bar{M}$, 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. AUTc input, 97

(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,

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

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

BIRK input, 14

Garrett Birkhoff refers to an algebra B as a "sub-direct product of algebras $B_1, \ldots, B_r$" 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 $i = 1, \ldots, r$ [Bir44, p. 175]. We introduce a similar notion for finite groups and finitely many symmetric groups.

Setup 3.1: Let $I = \{1, \ldots, r\}$ 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 ith 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. PREa input, 23

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

$$\iota\colon G \to S \tag{1}$$

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

We identify G with its image in S under ι and assume that ι 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

(2)
$$\begin{array}{ll} & G^{(i)} = \mathrm{pr}^{(i)}(G) \\ G^{[i]} = S^{(i)} \cap G = \mathrm{Ker}(\mathrm{pr}_i|_G) & G_i = S_{n_i} \cap G = \mathrm{Ker}(\mathrm{pr}^{(i)}|_G) \\ N^{[i]} = S^{(i)} \cap N = \mathrm{Ker}(\mathrm{pr}_i|_N) & N_i = S_{n_i} \cap N = \mathrm{Ker}(\mathrm{pr}^{(i)}|_N) \\ N_{(i)} = \mathrm{pr}_i(N) & N^{(i)} = \mathrm{pr}^{(i)}(N). \end{array}$$

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

(3)
$$\begin{array}{ccccccccc} \mathbf{1} & \longrightarrow & S^{(i)} & \longrightarrow & S & \xrightarrow{\mathrm{pr}_i} & S_{n_i} & \longrightarrow & \mathbf{1} \\ & & \downarrow & & \downarrow & & \| & & \\ \mathbf{1} & \longrightarrow & G^{[i]} & \longrightarrow & G & \longrightarrow & S_{n_i} & \longrightarrow & \mathbf{1} \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \mathbf{1} & \longrightarrow & N^{[i]} & \longrightarrow & N & \xrightarrow{\pi_i} & N_{(i)} & \longrightarrow & \mathbf{1} \end{array} \qquad \begin{array}{ccccccccc} \mathbf{1} & \longrightarrow & S_{n_i} & \longrightarrow & S & \xrightarrow{\mathrm{pr}^{(i)}} & S^{(i)} & \longrightarrow & \mathbf{1} \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \mathbf{1} & \longrightarrow & G_i & \longrightarrow & G & \longrightarrow & G^{(i)} & \longrightarrow & \mathbf{1} \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \mathbf{1} & \longrightarrow & N_i & \longrightarrow & N & \longrightarrow & N^{(i)} & \longrightarrow & \mathbf{1}. \end{array}$$

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 Setup 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.* PREb input, 129

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 (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 $I = \emptyset$. PREc input, 162

If (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 non-trivial group G, as in (1). Then, $|I| \geq 1$ and for each $i \in I$ we have $n_i \geq 2$ and the group G_i is non-trivial and normal in S_{n_i}.* GEYa input, 177

Proof: Since G is non-trivial, S is non-trivial, 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 ι. This contradicts the minimality of ι. 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)) and 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 ι. It follows that $G_i \neq \mathbf{1}$. ∎

LEMMA 3.5: *Suppose that the symmetric presentation $\iota\colon G \to S$ in (1) is minimal and assume that ι is the inclusion map. Let $A = \prod_{i\in I} A_{(n_i)}$ be the normal subgroup of S introduced in Notation 1.4.* BIRa input, 208

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 non-trivial 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. BIRb input, 233

We make a list $N_1, \ldots, N_r$ of all normal subgroups of G such that $G/N_i \cong S_{n_i}$ for some positive integer n_i with $n_i! \leq |G|$, $i = 1, \ldots, r$. 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 $G \to \prod_{i=1}^{r} G/N_i \cong \prod_{i=1}^{r} S_{n_i}$ of G. ∎

4. Quotients of Symmetrically Presentable Groups

PRES
input, 14

We prove that every quotient of a symmetrically presentable group is symmetrically presentable. Throughout, we use Notation 1.3 and the notation introduced in Setup 3.1, in particular the notation of Diagrams (3) in the latter setup.

PREe
input, 24

LEMMA 4.1: *Let G be a finite non-trivial 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 $|J| > 1$, there are 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*

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

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, $N^{[j]} \triangleleft G$. It follows from the minimality of N that $N^{[j]} = \mathbf{1}$. Thus,

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

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,

(2) $N_{(j)} = A_{(n_j)}$ for each $j \in J$.

Since $\mathrm{pr}_i(N) = N_{(i)} = \mathbf{1}$ for each $i \in I \setminus J$, we have $N \leq S_J = \prod_{j\in J} S_{n_j}$. Therefore, (a) is a consequence of (1) and (2).

In order to prove (b) we assume that

$$|J| > 1. \tag{3}$$

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

$$|N| = |A_{(m)}|. \tag{4}$$

CLAIM: $m \leq 4$. Otherwise $m \geq 5$, so by Fact 1.1(d), $A_{(m)} = A_m$ is a non-abelian simple group. By Lemma 3.5, $A_m^{|J|} = \prod_{j\in J} A_{(n_j)} \triangleleft G$. Since $N \leq A_m^{|J|}$ and $N \triangleleft G$, we have that $N \triangleleft A_m^{|J|}$. By (2) and [FrJ08, p. 374, Lemma 18.3.9], $N \cong A_m^{|J|}$. Hence, by (4), $|J| = 1$. This contradiction to (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* NORa input, 117

$$N = \{(a,\dots,a) \in S \mid\ a \in A_{(m)}\} \tag{5}$$

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

$$\mathbf{1} \longrightarrow A_{(m)} \longrightarrow S_m \xrightarrow{\mathrm{sg}} \mathrm{Aut}(A_{(m)}) \longrightarrow \mathbf{1} \tag{6}$$

such that

$$\mathrm{sg}(S_{m-1}) = \mathrm{Aut}(A_{(m)}). \tag{7}$$

CLAIM A: *The normalizer of N in S is*

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

Indeed, consider $\boldsymbol{\sigma} = (\sigma_1,\dots,\sigma_r) \in S_m^r$. For each $j \in \{1,\dots,r\}$ we set $\tau_j = \mathrm{sg}(\sigma_j)$ and let $\boldsymbol{\tau} = (\tau_1,\dots,\tau_r)$. Then, for each $\mathbf{a} = (a,\dots,a) \in N$ 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 $j = 1,\dots,r$. Since $\tau_1,\dots,\tau_r$ are automorphisms of $A_{(m)}$, this is true for all $\mathbf{a} \in N$ if and only if $\tau_j = \tau_1$ for $j = 1,\dots,r$. 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, (6) yields a short exact sequence

$$\mathbf{1} \longrightarrow A \longrightarrow \tilde{G} \xrightarrow{\mathrm{sg}_1} \mathrm{Aut}(A_{(m)}) \longrightarrow \mathbf{1}, \tag{8}$$

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 (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 (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 (6) and (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.* GEYe input, 246

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 ι is the inclusion map. Then, in the notation of Setup 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 $|I| > 1$.* By Lemma 4.1(b), there are 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 $N = \{(a^{\gamma_i})_{i \in I} \in S \mid a \in A_{(m)}\}$. Then, in the notation of the second paragraph of the proof of Lemma 4.2 and by (6), there exists for each $i \in I$ an element $\delta_i \in S_m$ such that $\mathrm{sg}(\delta_i) = \gamma_i$. Hence, $\boldsymbol{\delta} = (\delta_i)_{i \in I} \in S$, $N' = N^{\boldsymbol{\delta}^{-1}} = \{(a)_{i \in I} \mid a \in A_{(m)}\}$ 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 Setup 3.1, in particular by the left diagram of (3) in that setup, $\mathrm{pr}_{j'}(N) = \mathbf{1}$ for each $j' \in J'$, so $N \leq S_J$. Since 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 κ, 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 λ 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 λ is well defined, therefore λ 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 κ is injective, $gN = \mathrm{pr}_J(g)N = 1$. Therefore, λ is injective.

Since κ 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 λ 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.* GEYf input, 352

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

EMBED
input, 9

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 [FrJ08, p. 303, Def. 16.4.1]. QUOa
input, 19
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 α 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 $t_1, \ldots, t_r$ over K and set $\mathbf{t} = (t_1, \ldots, t_r)$. 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 α over $K(\mathbf{t})$. We refer to a proper solution field F of $\alpha_{\mathbf{t}}$ as a **proper regular solution** of α if F/L is regular. We say that α is **properly and regularly solvable** if there are $t_1, \ldots, t_r$ 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 Γ is a pair EMPa
input, 54

$$(\rho\colon \Gamma \to \bar{G},\ \alpha\colon G \to \bar{G}), \tag{1}$$

where G is a finite group and both ρ and α are epimorphisms. A **proper solution** of (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_{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 [FrJ08, Section 16.4].

Lemma 5.3 ([FrJ08, 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 α is properly and regularly solvable, then α has a proper solution field N which is linearly disjoint from M over L.* QUOb
input, 73

Lemma 5.4 ([FrJ08, 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, π is properly and regularly solvable.* QUOc
input, 82

We also quote a result of David Brink.

PROPOSITION 5.5 ([Br04, 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.* QUOd input, 92

Next, we recall that a commutative diagram

$$\begin{array}{ccc} D & \xrightarrow{\delta} & C \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\gamma} \\ B & \xrightarrow{\alpha} & A \end{array} \tag{2}$$

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

Note that the map ε of D onto the **fiber product**

$$B \times_A C = \{(b, c) \in B \times C \mid \alpha(b) = \gamma(c)\} \tag{3}$$

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 $\mathrm{pr}_C \circ \varepsilon = \delta$ [FrJ08, p. 499, Prop. 22.2.1].

We say that the fiber product (3) has **surjective homomorphisms** if both α and γ are surjective.

LEMMA 5.6 ([FrJ08, p. 500, Lemma 22.2.4]): *Let (2) be a commutative diagram of epimorphisms of profinite groups. Then, (2) is cartesian if and only if* $\mathrm{Ker}(\alpha \circ \beta) = \mathrm{Ker}(\delta) \times \mathrm{Ker}(\beta)$. QUOf input, 174

Here is the field theoretic counterpart of Lemma 5.6:

LEMMA 5.7 ([FrJ08, 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* QUOh input, 185

$$\begin{array}{ccc} \mathrm{Gal}(N/K) & \longrightarrow & \mathrm{Gal}(M'/K) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(M/K) & \longrightarrow & \mathrm{Gal}(L/K) \end{array}$$

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.* QUOj input, 207

Proof: We consider a cartesian diagram (2) with surjective homomorphisms. 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 λ: $D \to \prod_{i\in I} S_{n_i} \times \prod_{j\in J} S_{n_j}$ 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 $D = B \times_A C$, β is the projection of D on B, and δ 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 λ 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 λ is a symmetric presentation of D. ∎

6. Embedding Problems for the Absolute Galois Group of a Hilbertian Field GALOIS input, 15

We prove in this section that every finite embedding problem

$$(\rho\colon \mathrm{Gal}(K) \to \bar{G},\ \alpha\colon G \to \bar{G}) \tag{1}$$

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 (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.* WULa input, 25

Proof: As in Setup 3.1, let ι: $G \to S$ be a minimal symmetric presentation for G with $S = \prod_{i\in I} S_{n_i}$, where ι 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 (1) has a proper solution.

We may therefore assume that N is non-abelian. 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 non-abelian, 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

$$S = S_n \times S' \text{ with } S' = \prod_{i \neq 1} S_{n_i} \text{ and } A = A_n \times A' \text{ with } A' = \prod_{i \neq 1} A_{(n_i)} \tag{2}$$

such that the projection $\varphi = \mathrm{pr}_1|_G \colon G \to S_n$ is surjective. Note that φ 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 $\mathrm{sgn}(\varphi(a)) = \mathrm{sgn}(a) = 1$. Therefore, there exists a homomorphism $\psi \colon \bar{G} \to \{\pm 1\}$ that makes Diagram (3) below commutative.

(3)
$$\begin{array}{ccc} G & \xrightarrow{\alpha} & \bar{G} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ S_n & \xrightarrow{\mathrm{sgn}} & \{\pm 1\} \end{array}$$

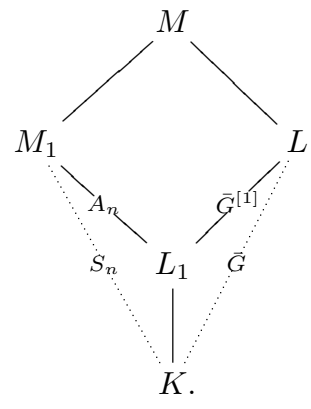
CLAIM B: *The square (3) is cartesian.* Since sgn, φ, and α are surjective, so is ψ. Let $\beta = \psi \circ \alpha = \mathrm{sgn} \circ \varphi$. Since $\mathrm{Ker}(\varphi) \leq \mathrm{Ker}(\mathrm{pr}_1) = S'$ and $\mathrm{Ker}(\alpha) = N = A_n \leq S_n$, we have $\mathrm{Ker}(\varphi) \cap \mathrm{Ker}(\alpha) = \mathbf{1}$. Thus, by Lemma 5.6, it suffices to prove that $\mathrm{Ker}(\beta) = \mathrm{Ker}(\varphi)\mathrm{Ker}(\alpha)$.

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

$$g = as, \text{ with } a \in S_n \text{ and } s \in S'. \tag{4}$$

Hence, $\varphi(g) = \mathrm{pr}_1(g) = a$, so $\mathrm{sgn}(a) = \mathrm{sgn}(\varphi(g)) = \beta(g) = 1$. Therefore, $a \in A_n = \mathrm{Ker}(\alpha) \leq G$, so by (4), $s = a^{-1}g \in G$. Therefore, $\varphi(s) = \varphi(a)^{-1}\varphi(g) = a^{-1}\varphi(g) = 1$, so $s \in \mathrm{Ker}(\varphi)$, which proves our claim.

PART C: *Solving Embedding problem (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 sgn: $S_n \to \{\pm 1\}$ is the only epimorphism from S_n to $\{\pm 1\}$, the restriction map res_{M_1/L_1} coincides with sgn: $S_n \to \{\pm 1\}$. Finally, we set $M = M_1 L$ and have the following diagram of Galois extensions:

(5)


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

$$\begin{array}{ccc} \mathrm{Gal}(M/K) & \longrightarrow & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(M_1/K) & \longrightarrow & \mathrm{Gal}(L_1/K), \end{array} \tag{6}$$

where all maps are restrictions, is cartesian (Lemma 5.7). Hence, Diagram (3) is the Galois theoretic counterpart of Diagram (6), so M is a proper solution field of our embedding problem. ∎

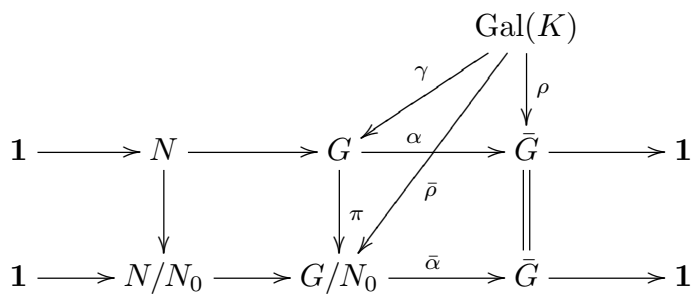
PROPOSITION 6.2: *Let K be a Hilbertian field with* $\mathrm{char}(K) \neq 2$. *Then, every finite embedding problem* GALb input, 164

$$(\rho\colon \mathrm{Gal}(K) \to \bar{G},\ \alpha\colon G \to \bar{G}) \tag{7}$$

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

Proof: Let $N = \mathrm{Ker}(\alpha)$. If $N = \mathbf{1}$, then α is an isomorphism, so $\alpha^{-1} \circ \rho$ is a proper solution of (7). If N is a minimal normal subgroup of G, then Lemma 6.1 yields a proper solution of (7). Therefore, we may assume that N is neither $\mathbf{1}$ nor minimal normal.

Then, G has a non-trivial 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 $\pi \circ \gamma = \bar{\rho}$.



Then, $\alpha \circ \gamma = \bar{\alpha} \circ \pi \circ \gamma = \bar{\alpha} \circ \bar{\rho} = \rho$, so γ is a proper solution of the embedding problem (7). ∎

7. The Maximal Symmetric Extension of a Field

COMPOS input, 14

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_{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.* FSEa input, 24

(a) *L is a composition 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_{symm}.*

Proof of (a) $\Longrightarrow$ (b): Suppose that L is a compositum of symmetric extensions $L_1, \ldots, L_r$ of K. Then, the map $\sigma \mapsto (\mathrm{res}_{L/L_1}(\sigma), \ldots, \mathrm{res}_{L/L_r}(\sigma))$ 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 $i = 1, \ldots, r$. Hence, $\mathrm{Gal}(L/K)$ is symmetrically presentable.

Proof of (b)$\Longrightarrow$(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 ι 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.

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

Proof of (c)$\Longrightarrow$(a): Suppose that L is a finite Galois extension of K in K_{symm}. Then, there exist symmetric extensions $N_1, \ldots, N_r$ of K such that $N = N_1 \cdots N_r$ contains L. By "(a)$\Longrightarrow$(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)$\Longrightarrow$(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 $\mathrm{Gal}(K_{\mathrm{symm}}/K)$.* MSFc input, 80 ∎

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 conclude from the preceding paragraph that G is a quotient of $\mathrm{Gal}(K_{\mathrm{symm}}/K)$. ∎

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 [FrJ08, p. 344], $\mathcal{SP}$ is a **formation of finite groups**. It is the smallest formation of finite groups that contains all symmetric groups. MSFd input, 109

Each inverse limit of $\mathcal{SP}$-groups in which the connecting homomorphisms are epimorphisms is a **pro-$\mathcal{SP}$-group** [FrJ08, 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 $\iota\colon X \to \hat{F}_X(\mathcal{SP})$ which converges to 1 such that $\iota(X)$ generates $\hat{F}_X(\mathcal{SP})$ and for each map φ of X into a pro-$\mathcal{SP}$-group G which converges to 1 and satisfies $G = \langle \varphi(X) \rangle$ there exists a unique epimorphism $\hat{\varphi}\colon \hat{F}_X(\mathcal{SP}) \to G$ with $\hat{\varphi} \circ \iota = \varphi$.

Since $S_2^n \in \mathcal{SP}$ for each positive integer n, it follows from [FrJ08, 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 $(\varphi\colon G \to A,\ \alpha\colon B \to A)$ with $B \in \mathrm{Im}(G)$ has a proper solution [FrJ08, p. 564, Def. 24.1.2]. ∎ MSFe input, 143

THEOREM 7.5: *Let K be a countable Hilbertian field with* $\mathrm{char}(K) \neq 2$. *Then,* MSFf input, 155

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

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 that $\mathrm{Gal}(K_{\mathrm{symm}}/K) \cong \hat{F}_\omega(\mathcal{SP})$ [FrJ08, p. 581, Thm. 24.8.1]. 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, Theorem 3.2 of [BFW16] implies that every field M between K and K_{symm} is Hilbertian. ∎ MSFg input, 193

8. Decidability

DECD
input, 10

Let K be a **presented field** in the sense of [FrJ08, 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 non-zero 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 [FrJ08, 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 [FrJ08, 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 [FrJ08, 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_{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,*

COMb
input, 53

(a) *we can effectively check whether f has a root in K_{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_{symm} if and only if at least one of the polynomials f_i has a root in K_{symm}. Thus, we may assume without loss that f is irreducible in $K[X]$.

In this case, all roots of f are in K_{sep} if and only if $f' \neq 0$. By [FrJ08, 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_{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 $K_{\rm symm}$. The latter can be effectively checked by (a). ∎

Remark 8.2: Given a presented field K we write $\mathcal{L}(\text{ring}, K)$ for the first order language of the theory of rings with a constant symbol for each element of K [FrJ08, p. 135, Example 7.3.1]. If M is an extension of K we write $\text{Th}(M)$ for the set of all first order sentences in $\mathcal{L}(\text{ring}, K)$ that are true in M and $\text{Root}(M/K)$ 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 $K_{\rm symm}$ and $K_{\rm ins}$ and note that it can also be effectively presented [FrJ08, p. 413, Lemma 19.4.1]. Every other algebraic extension of K is considered to be contained in $\tilde{K}$. NOTa input, 92

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 [FrJ08, p. 568, Lemma 24.3.3], $\hat{F}_\omega$ has the embedding property. Moreover, $\text{Im}(\hat{F}_\omega) = \text{FiniteGroups}$. ∎

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

LEMMA 8.3 ([JaS17, 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,* $\text{Gal}(M)$ *has the embedding property, and* $\text{Im}(\text{Gal}(M))$ *is a primitive recursive subset of* FiniteGroups. *Further, suppose that the set* $\text{Root}(M/K)$ *is primitive recursive. Then,* $\text{Th}(M)$ *is primitive recursive.* STRc input, 123

By Remark 8.2, $\hat{F}_\omega$ has the embedding property. Since the set $\text{Im}(\hat{F}_\omega)$ 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* $\text{Gal}(M) \cong \hat{F}_\omega$. *Further, suppose that the set* $\text{Root}(M/K)$ *is primitive recursive. Then,* $\text{Th}(M)$ *is primitive recursive.* DECa input, 142

With this we reach our next main result.

THEOREM 8.5: *Let K be a Hilbertian presented field with elimination theory. Then:* DECb input, 153
(a) $\text{Gal}(K_{\rm symm}) \cong \hat{F}_\omega$, *so* $\text{Im}(\text{Gal}(K_{\rm symm})) = \text{FiniteGroups}$.
(b) $\text{Th}(K_{\rm symm,ins})$ *is primitive recursive.*
(c) *If* $\text{char}(K) \neq 2$, *then* $\text{Im}(\text{Gal}(K_{\rm symm}/K))$ *is primitive recursive.*

Proof: By [FrJ08, p. 396, Thm. 18.10.4], $K_{\rm symm}$ is PAC and Hilbertian. Since K is presented, K is countable [FrJ08, p. 404], so $K_{\rm symm}$ is countable. By [FrV92, Thm. A] (in case $\text{char}(K) = 0$), or [Pop96, Thm. 1], [HaV96, Cor. 4.7], and [Jar11, 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 [FrJ08, 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. ∎

DECd input, 193

9. More Examples

SUMM input, 12

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_{symm}.

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

SUMb input, 19

Suppose that K is Hilbertian. Then, by [FrJ08, p. 396, Thm. 18.10.4], K_{symm} is PAC and Hilbertian. A mild change of the proof of that theorem proves that for each positive integer m also $K^{(m)}_{\mathrm{symm}}$ 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 $\mathrm{Gal}(\hat{F}/K(t)) \cong S_n$ [FrJ08, 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 $K^{(m)}_{\mathrm{symm}}$ that leads to a $K^{(m)}_{\mathrm{symm}}$-rational point of C [FrJ08, p. 231, Lemma 13.1.1]. This implies that $K^{(m)}_{\mathrm{symm}}$ is PAC.

Applying Haran's diamond theorem, one proves as in [FrJ08, p. 396, Thm. 18.10.4] that $K^{(m)}_{\mathrm{symm}}$ is Hilbertian. Alternatively, one may apply Remark 7.6. If in addition, K is countable, then so is $K^{(m)}_{\mathrm{symm}}$. Hence, by [Jar11, p. 89, Thm. 5.10.2(c)], $\mathrm{Gal}(K^{(m)}_{\mathrm{symm}}) \cong \hat{F}_\omega$. In particular, $\mathrm{Im}(\mathrm{Gal}(K^{(m)}_{\mathrm{symm}}))$ is the set of all finite groups. As in Remark 3.6, one observes that $\mathrm{Im}(\mathrm{Gal}(K^{(m)}_{\mathrm{symm}}/K))$ 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 $K^{(m)}_{\mathrm{symm,ins}}$.

By Lemma 8.3, $\mathrm{Th}(K^{(m)}_{\mathrm{symm,ins}})$ 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 $\mathrm{Gal}(K^{(m)}_{\mathrm{symm}}/K) \cong \hat{F}_\omega(\mathcal{SP}^{(m)})$. ∎ GEYb input, 124

We conclude our work with 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, $\bigcap_{m\geq 5} K^{(m)}_{\mathrm{symm}} = K^{(2)}$.* SUMc input, 143

Proof: Let $N = \bigcap_{m\geq 5} K^{(m)}_{\mathrm{symm}}$. By Lemma 5.3 and Proposition 5.5, for each $m \geq 3$ every quadratic extension of K can be embedded in 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 $L_1, \ldots, L_r$ of K such that $\mathrm{Gal}(L_i/K) \cong S_{n_i}$ with $n_i \geq m$ for $i = 1, \ldots, r$ and G is a quotient of $\mathrm{Gal}(L/K)$, where $L = L_1 \cdots L_r$. By Setup 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 non-negative 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 [FrV92] yields a sequence of irreducible polynomials $f_2, f_3, f_4, \ldots$ in $\mathbb{Q}[X]$ with linearly disjoint splitting fields $N_2, N_3, N_4, \ldots$ having Galois groups $S_2, S_3, S_4, \ldots$. 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 [FrV92, Thm. A] that $\mathrm{Gal}(N) \cong \hat{F}_\omega$. Hence, $\mathrm{Im}(\mathrm{Gal}(N)) =$ FiniteGroups is primitive recursive. SUMd input, 187

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

(1) every G_n is normal in G, and

(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 for all $n \geq 5$,
(3d) $G_n = \mathbf{1}$, or $G_n = S_2$, or $G_n = S_n$.

Conversely, if a finite group G is generated by subgroups $G_2, G_3, G_4, \ldots$, only finitely of them are non-trivial, 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 non-effective proof of this statement given in [FrJ78] combined with [FrV92, Remark 1]. In addition, one would have at some point to use an effective version of Hilbert irreducibility theorem (e.g. [Wal05]).

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

References

[BFW16] L. Bary-Soroker, A. Fehm, and G. Wiese, *Hilbertian fields and Galois representations,* Journal für die reine und angewandte Mathematik **712** (2016), 123–139.

[Bir44] G. Birkhoff, *Subdirect unions in univeral algebra,* Bulletin of the American Mathematical Society **50** (1944), 764–768.

[Br04] D. Brink, *On alternating and symmetric groups as Galois groups,* Israel Journal of Mathematics **142** (2004), 47-60.

[Dri79] L. v. d. Dries, *New decidable fields of algebraic numbers,* Proceeding of the American Mathematical Society **77** (1979), 251–256.

[Ers96] Yu. L. Ershov, *Nice local-global fields I,* Algebra and Logic **35** (1996), 229–235.

[Feh17] A. Fehm, *The elementary theory of large fields of totally $\mathfrak{S}$-adic numbers,* Journal of the Institute of Mathematics of Jussieu **16** (2017), 121–154.

[FHV94] M. D. Fried, D. Haran, H. Völklein, *Real hilbertianity and the field of totally real numbers,* Contemporary Mathematics **174** (1994), 1–34.

[FrJ78] M. Fried and M. Jarden, *Diophantine properties of subfields of $\tilde{\mathbb{Q}}$,* American Journal of Mathematics **100** (1978), 653–666.

[FrJ08] M. Fried and M. Jarden, *Field Arithmetic (3rd Edition)*, Ergebnisse der Mathematik (3), **11**, Springer, Heidelberg, 2008.

[FrV92] M. D. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field*, Annals of Mathematics **135** (1992), 469–481.

[HaV96] D. Haran and H. Völklein, *Galois groups over complete valued fields*, Israel Journal of Mathematics **93** (1996), 9–27.

[Hrb95] D. Harbater, *Fundamental groups and embedding problems in characteristic p*, Contemporary Mathematics **186** (1995), 353-369.

[Jar11] M. Jarden, *Algebraic Patching*, Springer Monographs in Mathematics, Springer 2011.

[JaS17] M. Jarden and A. Shlapentokh, *Decidable algebraic fields*, Journal of Symbolic Logic **82** (2017), 474-488.

[Pop96] F. Pop, *Embedding problems over large fields*, Annals of Mathematics **144** (1996), 1–34.

[Wal05] Y. Walkowiak, *Théorème d'irréductibilité de Hilbert effectif*, Acta Arithmetica **116** (2005), 343–362.