THE ABSOLUTE GALOIS GROUP OF SUBFIELDS OF THE FIELD OF TOTALLY S-ADIC NUMBERS*

by

Dan Haran
School of Mathematics, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: haran@post.tau.ac.il

and

Moshe Jarden
School of Mathematics, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: jarden@post.tau.ac.il

and

Florian Pop
Department of Mathematics, University of Pennsylvania
Philadelphia, PA 19104-6395, USA
e-mail: pop@math.upenn.edu

Abstract

For a finite set S of primes of a global field K and for $\sigma_1,\ldots,\sigma_e \in \mathrm{Gal}(K)$ we denote the field of totally S-adic numbers by $K_{\mathrm{tot},S}$, the fixed field of $\sigma_1,\ldots,\sigma_e$ in $K_{\mathrm{tot},S}$ by $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$, and the maximal Galois extension of K in $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$ by $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$. We prove that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the absolute Galois group of $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is isomorphic to the free product of $\hat{F}_\omega$ and a free product of local factors over S.

MR Classification: 12E30

Directory: \Jarden\Diary\HJPe

23 October, 2007

---

* Research supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation.

Introduction

The absolute Galois group $\mathrm{Gal}(K)$ of a global field K is a very complicated object whose structure seems to be unattainable at the present knowledge of Galois theory. What we do understand is the structure of absolute Galois Groups of certain families of infinite extensions of K of a "semi-local type". The present work proves what is perhaps the ultimate word in a series of results in this subject that started forty years ago.

The first major result in this direction was discovered around 1970. For $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ we denote the fixed field of $\sigma_1, \ldots, \sigma_e$ in the separable closure K_s of K by $K_s(\boldsymbol{\sigma})$. We denote the maximal Galois extension of K in $K_s(\boldsymbol{\sigma})$ by $K_s[\boldsymbol{\sigma}]$. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ (in the sense of the Haar measure) $\mathrm{Gal}(K_s(\boldsymbol{\sigma}))$ is the free profinite group $\hat{F}_e$ on e generators [FrJ05, Thm. 18.5.6]. The case where $K = \mathbb{Q}$ and $e = 1$ is due to James Ax [Ax67, p. 177]. In addition, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ $\mathrm{Gal}(K_s[\boldsymbol{\sigma}])$ is isomorphic to the free profinite group $\hat{F}_\omega$ on countably many generators [Jar97, Thm. 2.7].

On the other hand we consider a finite set S of primes of K. For each $\mathfrak{p} \in S$ we choose a **$\mathfrak{p}$-closure** $K_\mathfrak{p}$ of K at $\mathfrak{p}$. This is a Henselian closure if $\mathfrak{p}$ is nonarchimedean, a real closure if $\mathfrak{p}$ is real archimedean, and the algebraic closure $\tilde{K}$ of K if $\mathfrak{p}$ is complex archimedean. Let

$$K_{\mathrm{tot},S} = \bigcap_{\mathfrak{p}\in S} \bigcap_{\rho\in\mathrm{Gal}(K)} K_\mathfrak{p}^\rho$$

be the field of **totally S-adic numbers**. By [Pop96, Thm. 3] there exists a closed subset R of $\mathrm{Gal}(K)$ such that

$$\mathrm{Gal}(K_{\mathrm{tot},S}) = \mathop{\prod\nolimits^{*}}_{\mathfrak{p}\in S} \mathop{\prod\nolimits^{*}}_{\rho\in R} \mathrm{Gal}(K_\mathfrak{p}^\rho),$$

where the right hand side is the inner free product in the sense of Melnikov (Definition 1.2). The case where S consists of archimedean primes only was proved in [FHV93, Cor. 6].

The next task is to combine the two results, that is to describe the absolute Galois groups of $K_{\mathrm{tot},S}(\boldsymbol{\sigma}) = K_s(\boldsymbol{\sigma}) \cap K_{\mathrm{tot},S}$ and $K_{\mathrm{tot},S}[\boldsymbol{\sigma}] = K_s[\boldsymbol{\sigma}] \cap K_{\mathrm{tot},S}$, again up to a set of $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ of Haar measure 0.

Main Theorem: *Let K be a global field, S a finite set of primes of K, and e a positive integer. Then the following statements hold for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$:*

(a) *For each $\mathfrak{p} \in S$ there exists a closed subset $R_\mathfrak{p}$ of $\mathrm{Gal}(K)$ such that $\mathrm{Gal}(K_{\mathrm{tot},S}(\boldsymbol{\sigma})) \cong \hat{F}_e * \mathop{\Large\ast}_{\mathfrak{p}\in S} \mathop{\Large\ast}_{\rho\in R_\mathfrak{p}} \mathrm{Gal}(K_\mathfrak{p}^\rho)$.*

(b) *For each $\mathfrak{p} \in S$ there exists a closed subset $R_\mathfrak{p}$ of $\mathrm{Gal}(K)$ such that $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) \cong \hat{F}_\omega * \mathop{\Large\ast}_{\mathfrak{p}\in S} \mathop{\Large\ast}_{\rho\in R_\mathfrak{p}} \mathrm{Gal}(K_\mathfrak{p}^\rho)$.*

(c) *The second free factor on the right hand side of both (a) and (b) depends (up to an isomorphism) only on K and S but not on the choice of the fields $K_\mathfrak{p}$ nor on $\boldsymbol{\sigma}$. In particular, that factor is isomorphic to $\mathrm{Gal}(K_{\mathrm{tot},S})$. Moreover, that factor is built from the groups $\mathrm{Gal}(K_\mathfrak{p})$, $\mathfrak{p} \in S$, in purely group theoretic terms.*

Note that $G = \mathrm{Gal}(K_{\mathrm{tot},S})$ is isomorphic to the second free component of (a) and (b). However, since G is a closed normal subgroup of $\mathrm{Gal}(K_{\mathrm{tot},S}(\boldsymbol{\sigma}))$ and $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}])$, the isomorphism does not map it onto that second component.

Part (a) of the main theorem is proved in [HJP06] in the case where K is a number field. Among others, the proof of [HJP06] uses that the groups $\mathrm{Gal}(K_\mathfrak{p})$ are finitely generated and the Ax-Kochen-Ershov theorem. The former fact is false and the latter one is unknown in positive characteristic. Thus, the proof of [HJP06] of (a) for number fields does not carry over to the general case and we needed a totally new idea.

The idea we found supports both (a) and (b) and gives (c) as a bonus. It is based on [Pop96, Thm. 2.8]. By that theorem, if E is an extension of K in $K_{\mathrm{tot},S}$ and E is both Hilbertian and ample (Definition 3.6) then $\mathrm{Gal}(E) \cong G * \hat{F}_\omega$, where G is a Cantor free product over S (Remark 3.7). On the other hand we prove a general principle for a free product $A * B$ of profinite group: Let $\pi\colon A * B \to B$ be the projection on the second factor, C a closed subgroup of B, and R a closed system of representatives for the left cosets of B modulo C. Then $\pi^{-1}(C) = C * \mathop{\Large\ast}_{r\in R} A^r$ (Lemma 2.4). Now we apply [GeJ02, Thm. A] and a theorem of Weissauer in order to find for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ an extension E of K in $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ which is both ample and Hilbertian. Moreover, using a lifting theorem for covers over ample fields due to Colliot-Thélène in characteristic 0 (the general case is proved in [HaJ00]) we prove that E can be chosen so that $\mathrm{Gal}(K_{\mathrm{tot},S}/K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) \cong \hat{F}_\omega$. Let R be a closed set of representatives for the left cosets of $\mathrm{Gal}(K_{\mathrm{tot},S}/K_{\mathrm{tot},S}[\boldsymbol{\sigma}])$ in $\mathrm{Gal}(K_{\mathrm{tot},S}/E)$. Then $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}])$ is the inverse image of $\mathrm{Gal}(K_{\mathrm{tot},S}/K_{\mathrm{tot},S}[\boldsymbol{\sigma}])$ in $\mathrm{Gal}(E)$ under the map $\mathrm{Gal}(E) \to \mathrm{Gal}(K_{\mathrm{tot},S}/E)$, hence is isomorphic to $\hat{F}_\omega * \mathop{\ast\!\!\prod}_{r\in R} \mathrm{Gal}(K_{\mathrm{tot},S})^r$. By Remark 3.7, the second factor is again isomorphic to the Cantor free product. This proves (b). The proof of (a) goes along the same lines. Here it is much easier to prove that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ we can choose E such that $\mathrm{Gal}(K_{\mathrm{tot},S}/K_{\mathrm{tot},S}(\boldsymbol{\sigma})) \cong \hat{F}_e$ (Section 4).

1. Sheaves of Profinite Groups

SHEAF
input, 11

We introduce the concept of a semi-constant free product as a special case of the concept of a free product of profinite groups in the sense of Melnikov [Mel90] and prove that each semi-constant free product is uniquely determined up to an isomorphism by its defining data.

Let T be a **profinite space**, i.e. an inverse limit of finite discrete spaces. A **sheaf of profinite groups over** T is a triple $\mathbf{X} = (X, \tau, T)$ in which X is a profinite space and $\tau\colon X \to T$ is a continuous map satisfying the following conditions:

(1a) For each $t \in T$ the fiber $X_t = \tau^{-1}(t)$ is a profinite group; thus, $X = \dot\bigcup_{t\in T} X_t$.

(1b) The group operations in X_t are **uniformly continuous**. That is, if we set

$$X^{(2)} = \{(x, y) \in X \times X \mid \tau(x) = \tau(y)\},$$

then the map $\mu\colon X^{(2)} \to X$ given by $\mu(x, y) = x^{-1}y$ is continuous.

A **morphism** of $\mathbf{X}$ into a profinite group A is a continuous map $\alpha\colon X \to A$ whose restriction to each of the fibers X_t is a homomorphism. We say that the morphism α is **rigid** if the restriction of α to each X_t is injective.

Let G be a profinite group. We denote the space of all closed subgroups of G by $\mathrm{Subgr}(G)$. The **strict topology** of $\mathrm{Subgr}(G)$ has a basis consisting of all subsets $\{H \in \mathrm{Subgr}(G) \mid HN = H_0N\}$, where N is an open normal subgroup of G and H_0 is a closed subgroup of G. Under this topology $\mathrm{Subgr}(G)$ is naturally isomorphic to $\varprojlim \mathrm{Subgr}(G/N)$, where N ranges over all open normal subgroups of G and the finite space $\mathrm{Subgr}(G/N)$ is equipped with the discrete topology. Thus, $\mathrm{Subgr}(G)$ equipped with the strict topology is a profinite space. In addition, $\mathrm{Subgr}(G)$ has a weaker topology called the **étale topology**. A basis for the étale topology is the family of all sets $\{H \in \mathrm{Subgr}(G) \mid H \le H_0\}$, where H_0 is an open subgroup of G.

A subfamily $(G_t)_{t\in T}$ of $\mathrm{Subgr}(G)$ is said to be **étale continuous** if the map $t \mapsto G_t$ of T into $\mathrm{Subgr}(G)$ is étale continuous. In other words, for each open subgroup H_0 of G the subset $\{t \in T \mid G_t \le H_0\}$ of T is open.

If $\mathbf{X} = (X, \tau, T)$ is a sheaf and $\omega\colon X \to G$ is a morphism, then the family $(\omega(X_t))_{t\in T}$ is étale continuous. Indeed, let H_0 be an open subgroup of G and put

$T_0 = \{t \in T \mid \omega(X_t) \le H_0\}$. Then $\omega^{-1}(H_0)$ is open in X, hence

$$\begin{aligned} T \smallsetminus T_0 &= \{t \in T \mid X_t \not\subseteq \omega^{-1}(H_0)\} = \{t \in T \mid X_t \cap (X \smallsetminus \omega^{-1}(H_0)) \ne \emptyset\} \\ &= \tau(X \smallsetminus \omega^{-1}(H_0)) \end{aligned}$$

is closed in T, because τ is a closed map. Hence T_0 is open in T.

LEMMA 1.1: *For each pair $(G, G_t)_{t\in T}$ consisting of a profinite group G and an étale continuous family of closed subgroups $(G_t)_{t\in T}$ there exists a sheaf (X, τ, T) with a rigid morphism ω: $X \to G$ such that $\omega(X_t) = G_t$ for each $t \in T$. Moreover, if (X', τ', T) is another sheaf over T and ω': $X' \to G$ is a rigid morphism such that $\omega'(X'_t) = G_t$ for each $t \in T$, then there exists a unique homeomorphism α: $X \to X'$ such that the following diagrams are commutative:* SHEa input, 95

(2)
$$\begin{tikzcd} X \arrow[r, "\omega"] \arrow[d, "\tau"'] \arrow[dr, "\alpha"] & G \\ T & X' \arrow[l, "\tau'"] \arrow[u, "\omega'"'] \end{tikzcd} \qquad \begin{tikzcd} X^{(2)} \arrow[r, "\mu"] \arrow[d, "\alpha^{(2)}"'] & X \arrow[d, "\alpha"] \\ (X')^{(2)} \arrow[r, "\mu'"] & X' \end{tikzcd}$$

Here $\mu'(x', y') = (x')^{-1}y'$, and $\alpha^{(2)}(x, y) = (\alpha(x), \alpha(y))$.

Proof: The proof naturally breaks up into two parts.

PART A: *Construction of X.* Consider the profinite space $G \times T$ and its subset

$$X = \{(g, t) \in G \times T \mid g \in G_t\}.$$

CLAIM: *X is closed in $G \times T$.* Indeed, let $(g_0, t_0) \in (G \times T) \smallsetminus X$. Then $g_0 \notin G_{t_0}$. Hence, there exists an open subgroup H_0 of G such that $G_{t_0} \le H_0$ and $g_0 \notin H_0$. Since the map $t \to G_t$ is étale continuous, T has an open neighbourhood T_0 of t_0 such that $G_t \le H_0$ for each $t \in T_0$. Thus, $g_0H_0 \times T_0$ is an open neighborhood of (g_0, t_0) in $G \times T$. Consider $(g, t) \in g_0H_0 \times T_0$. Then $G_t \le H_0$. If $(g, t) \in X$, then $g \in G_t$, so $g \in H_0$, hence $g_0H_0 = gH_0 = H_0$, and therefore $g_0 \in H_0$. We conclude from this contradiction that $(g, t) \notin X$. Consequently, $g_0H_0 \times T_0 \subseteq (G \times T) \smallsetminus X$, which proves the claim.

It follows from the claim that X is a profinite space. Let ω: $X \to G$ and τ: $X \to T$ be the projection maps. For each $t \in T$, ω maps $X_t = \tau^{-1}(t) = G_t \times \{t\}$ bijectively onto

G_t. Thus, X_t is a profinite group whose multiplication is given by the rule $(g_1, t)(g_2, t) = (g_1 g_2, t)$ for $g_1, g_2 \in G_t$. Moreover, ω maps X_t isomorphically onto G_t.

With this notation, $X^{(2)} = \{((g_1, t), (g_2, t)) \mid t \in T \text{ and } g_1, g_2 \in G_t\}$, the map μ: $X^{(2)} \to X$ maps each element $((g_1, t), (g_2, t))$ of $X^{(2)}$ onto the element $(g_1^{-1} g_2, t)$ of X. This map is continuous. Consequently, (X, τ, T) is a sheaf of profinite groups over T and ω: $X \to G$ is a rigid morphism.

Part B: *Uniqueness of X.* Suppose (X', τ', T) is another sheaf of profinite groups over T and ω': $X' \to G$ is a rigid morphism with $\omega'(X'_t) = G_t$ for each $t \in T$. Let α': $X' \to X$ be the continuous map defined by the rule $\alpha'(x') = (\omega'(x'), \tau'(x'))$ for each $x' \in X'$. If $\alpha'(x'_1) = \alpha'(x'_2)$, we set $t = \tau'(x'_1) = \tau'(x'_2)$. By assumption, $\omega'|_{X'_t}$ is a bijection, so $x'_1 = x'_2$. If $(g, t) \in X$, then $g \in G_t$, so there exists $x' \in X'_t$ with $\omega'(x') = g$. In addition, $\tau'(x') = t$, hence $\alpha'(x') = (g, t)$. Since both X and X' are profinite spaces, α' is a homeomorphism whose inverse $\alpha = (\alpha')^{-1}$ makes both diagrams in (2) commutative.

Finally, the commutativity of the left diagram in (2) forces the uniqueness of α', hence that of α. ∎

Definition 1.2: Free product of profinite groups. Let $\mathbf{X} = (X, \tau, T)$ be a sheaf of profinite groups. An **external free product** over $\mathbf{X}$ is a pair (G, ω) in which G is a profinite group and ω: $\mathbf{X} \to G$ is a morphism satisfying the following condition: SHEb input, 204

(3) For every morphism α of $\mathbf{X}$ into a profinite group A there is a unique homomorphism φ: $G \to A$ such that $\varphi \circ \omega = \alpha$.

For each sheaf $\mathbf{X}$ of profinite groups there is a unique free product (G, ω) over $\mathbf{X}$ [Mel90, Sec. 1.14]. Moreover, the morphism ω: $\mathbf{X} \to G$ is rigid [Mel90, Lemma 1.15].

On the other hand, let G be a profinite group and for each $t \in T$ let G_t be a closed subgroup of G. We say that G is the **internal free product** of the groups G_t, $t \in T$, and write $G = \mathop{\ast\!\!\!\prod}_{t \in T} G_t$ if the following conditions hold:

(4a) The map $t \mapsto G_t$ from T to $\mathrm{Subgr}(G)$ is étale continuous.

(4b) $G_s \cap G_t = 1$ for all $s, t \in T$, $s \neq t$.

(4c) Every continuous map α_0 of the space $\bigcup_{t \in T} G_t$ into a profinite group A, whose restriction to each G_t is a homomorphism, uniquely extends to a homomorphism $\alpha\colon G \to A$.

The two definitions of free products are equivalent in the following sense: Suppose (G, ω) is an external free product over the sheaf $\mathbf{X}$. For each $t \in T$ let $G_t = \omega(X_t)$. Then $G = \mathop{\boxed{*}}_{t\in T} G_t$ [Mel90, Sec. 1.17]. Conversely, suppose $G = \mathop{\boxed{*}}_{t\in T} G_t$. Then there exists a sheaf $\mathbf{X} = (X, \tau, T)$ of profinite groups over T and a morphism $\omega\colon X \to G$ such that (G, ω) is an external free product over $\mathbf{X}$ [Mel90, Sec. 1.16]. This $\mathbf{X}$ is unique up to an isomorphism, by Lemma 1.1. Finally we note that the uniqueness part in either (3) or (4c) implies that $G = \langle G_t \rangle_{t\in T}$. ∎

Construction 1.3: Semi-constant sheaf. Let S be a finite set. For each $\mathfrak{p} \in S$ let $T_\mathfrak{p}$ be a profinite space and $G_\mathfrak{p}$ a profinite group. We set $T = \dot{\bigcup}_{\mathfrak{p}\in S} T_\mathfrak{p}$, $X = \dot{\bigcup}_{\mathfrak{p}\in S} G_\mathfrak{p} \times T_\mathfrak{p}$, and define $\tau\colon X \to T$ by $\tau(g, t) = t$. Then $\mathbf{X} = (X, \tau, T)$ is a sheaf of profinite groups. The sheaf $\mathbf{X}$ is said to be **semi-constant**. If S consists of one element, $\mathbf{X}$ is a **constant sheaf** [Mel90, Sec. 1.13].

SHEc input, 259

A semi-constant sheaf naturally arises in the following situation: Let $\tilde{G}$ be a profinite group. For each $\mathfrak{p} \in S$ let $R_\mathfrak{p}$ be a closed subset and $G_\mathfrak{p}$ a closed subgroup of $\tilde{G}$. We choose a homeomorphic copy $T_\mathfrak{p}$ of $R_\mathfrak{p}$ and a homeomorphism $\lambda_\mathfrak{p}\colon T_\mathfrak{p} \to R_\mathfrak{p}$. As above we write $T = \dot{\bigcup}_{\mathfrak{p}\in S} T_\mathfrak{p}$, and for each $t \in T_\mathfrak{p}$ let $G_t = G_\mathfrak{p}^{\lambda_\mathfrak{p}(t)}$. Then the family $(G_t)_{t\in T}$ is ètale continuous; in fact, the map $T \to \mathrm{Subgr}(\tilde{G})$ given by $t \mapsto G_t$ is even strictly continuous. We let $\mathbf{X}$ be the corresponding semi-constant sheaf and define a map $\omega\colon X \to \tilde{G}$ by $\omega(g, t) = g^{\lambda_\mathfrak{p}(t)}$ for $g \in G_\mathfrak{p}$, $t \in T_\mathfrak{p}$ and $\mathfrak{p} \in S$. Then ω is a rigid morphism and $\omega(X_t) = G_t$ for each $\tau \in T$. Thus, $\mathbf{X}$ and ω satisfy the conditions of Lemma 1.1 with $\tilde{G}$ replacing G, so they are uniquely determined in the sense of that lemma.

Suppose G is a closed subgroup of $\tilde{G}$ so that $G = \mathop{\boxed{*}}_{\mathfrak{p}\in S} \mathop{\boxed{*}}_{\rho\in R_\mathfrak{p}} G_\mathfrak{p}^\rho$. Then $G = \mathop{\boxed{*}}_{\mathfrak{p}\in S} \mathop{\boxed{*}}_{t\in T_\mathfrak{p}} G_t = \mathop{\boxed{*}}_{t\in T} G_t$ [Mel90, statement after Thm. 1.5]. By Definition 1.2 and Lemma 1.1, (G, ω) is, up to an isomorphism, the external free product over $\mathbf{X}$. The importance of this observation is that a free product constructed this way is completely determined, up to an isomorphism, by the data $(G_\mathfrak{p}, R_\mathfrak{p})_{\mathfrak{p}\in S}$. In other words, if $G' =$

$\mathop{\boxed{\ast}}_{\mathfrak{p}\in S}\mathop{\boxed{\ast}}_{t\in R'_{\mathfrak{p}}}(G'_{\mathfrak{p}})^t$, and $R'_{\mathfrak{p}}\cong R_{\mathfrak{p}}$, $G'_{\mathfrak{p}}\cong G_{\mathfrak{p}}$, for each $\mathfrak{p}\in S$, then $G'\cong G$. ∎

The profinite spaces that appear in the free products arising in the field theoretic set up of this note are all homeomorphic to a special one.

Definition 1.4: Cantor space. The **weight** of an infinite profinite space X is the cardinality of the set of open-closed subsets of X [RiZ00, Prop. 2.6.1]. We say that X is a **Cantor space** if its weight is $\leq \aleph_0$ and X has no isolated points. Alternatively, X is homemomorphic to $2^{\mathbb{N}}$, or, also, to the Cantor middle third set [HaJ86, Lemma 1.2]. Thus, all Cantor spaces are homeomorphic to each other. Note that each disjoint union or cartesian products of finitely many Cantor spaces is again a Cantor space. ∎

WEIGHT
input, 329

Here is an example of a Cantor space:

LEMMA 1.5: *Let G be a profinite group of at most countable rank, H a closed subgroup of infinite index, and R a closed subset of representatives for the left cosets of G modulo H. Then G/H and R are Cantor spaces.*

ISOLATED
input, 346

Proof: As a closed subspace of G, the set R is a profinite space under the topology induced from that of G. The latter has a basis of at most countable cardinality, hence the weight of R (Definition 1.4) is at most $\aleph_0$. It remains to prove that R has no isolated points.

Indeed, the map $r\mapsto rH$ is a continuous bijection $R\to G/H$ of profinite spaces, hence it is a homeomorphism. If an element r of R is an isolated point, then rH is an isolated point of G/H. Hence, by the definition of the quotient topology, rH is an open subset of G. Therefore, H is a open subgroup of G, which means $(G:H)<\infty$. This contradiction to the assumption implies that r is not isolated in R. ∎

2. Free Products

GROUP
input, 12

Let A and B be profinite groups, π the projection of the free product $A * B$ onto B, and C a closed subgroup of B. We prove that $\pi^{-1}(C)$ is isomorphic to a free product of C with a free product in the sense of Section 1 of a family of conjugates of A in $A * B$. We start the proof of that statement with an alternative description of $A * B$.

Consider the constant sheaf of profinite groups $(A \times B, \mathrm{pr}, B)$ with the profinite space $A \times B$ and the projection pr on B (Construction 1.3). Let $(\hat{A}, \omega)$ be the free product over this sheaf. For each $b \in B$ the fiber $\mathrm{pr}^{-1}(b) = A \times \{b\}$ is a profinite group isomorphic to A; let $A_b = \omega(A \times \{b\})$. Then $\hat{A}$ is the inner free product $\mathop{\ast\!\!\!\prod}_{b \in B} A_b$ (Definition 1.2). Since ω is rigid, we may identify A_1 with A via $\omega(a, 1) \mapsto a$.

Lemma 2.1: *The group B acts on $\hat{A}$ so that*

ACTION
input, 39

$$\omega(a,b)^x = \omega(a,bx), \qquad a \in A,\ b, x \in B. \tag{1}$$

Proof: The continuous action $(a,b)^x = (a,bx)$ of B on $A \times B$ induces a right action of B on $\hat{A}$. Indeed, each $x \in B$ defines a continuous map $\mu_x\colon A \times B \to A \times B$ by

$$\mu_x(a,b) = (a,b)^x = (a,bx).$$

Condition (3) in Definition 1.2 gives a unique homomorphism $\hat{\omega}_x\colon \hat{A} \to \hat{A}$ such that

$$\begin{tikzcd}
A \times B \arrow[r, "\omega"] \arrow[d, "\mu_x"'] & \hat{A} \arrow[d, "\hat{\omega}_x"] \\
A \times B \arrow[r, "\omega"] & \hat{A}
\end{tikzcd}$$

commutes. For each $\hat{a} \in \hat{A}$ and each $x \in B$ we define

$$\hat{a}^x = \hat{\omega}_x(\hat{a}). \tag{2}$$

If y is another element of B, then $\mu_{xy} = \mu_y \circ \mu_x$. By the uniqueness of (3) in Definition 1.2, $\hat{\omega}_{xy} = \hat{\omega}_y \circ \hat{\omega}_x$, that is, $\hat{a}^{xy} = (\hat{a}^x)^y$ for every $\hat{a} \in \hat{A}$. In addition, $\hat{\omega}_1 = \mathrm{id}_{\hat{A}}$. Thus, (2) defines an action of B on $\hat{A}$ from the right. Property (1) follows from (2): $\omega(a,b)^x = \hat{\omega}_x(\omega(a,b)) = \omega(\mu_x(a,b)) = \omega(a,bx)$. ∎

The action of B on $\hat{A}$ established in Lemma 2.1 defines a semi-direct product $B \ltimes \hat{A}$.

LEMMA 2.2: *The homomorphism* $\alpha\colon A * B \to B \ltimes \hat{A}$ *defined by* FREESDP input, 98

$$\alpha(a) = \omega(a,1) \text{ for } a \in A \text{ and } \alpha(b) = b \text{ for } b \in B \tag{3}$$

is an isomorphism. Its inverse $\alpha'\colon B \ltimes \hat{A} \to A * B$ *is given by* $\alpha'(b) = b$ *on* B *and by* $\alpha'(\omega(a,b)) = a^b$ *on* $\hat{A} = \langle \omega(A \times B) \rangle$.

Proof: We break up the proof into two parts.

PART A: *α' is well defined.* The map $A \times B \to A * B$ defined by $(a,b) \mapsto a^b$ is continuous and its restriction to each fiber $A \times \{b\}$ is a homomorphism. By (3) of Section 1 there exists a unique homomorphism $\alpha'\colon \hat{A} \to A*B$ such that $\alpha'(\omega(a,b)) = a^b$. In order to extend α' from $B \cup \hat{A}$ to a homomorphism on $B \ltimes \hat{A}$, we have to prove that α' commutes with the action of B on $\hat{A}$, that is, that $\alpha'(\hat{a}^x) = \alpha'(\hat{a})^x$ for all $\hat{a} \in \hat{A}$ and $x \in B$. But, since $\omega(A \times B)$ generates $\hat{A}$, it suffices to prove this for $\hat{a} = \omega(a,b)$, for all $a \in A$ and $b \in B$. In this case, by (1),

$$\alpha'(\omega(a,b)^x) = \alpha'(\omega(a,bx)) = a^{bx} = (a^b)^x = (\alpha'(\omega(a,b)))^x.$$

PART B: *α and α' are inverse to each other.* By definition, both α and α' are the identity map on B. For $a \in A$ we have $\alpha'(\alpha(a)) = \alpha'(\omega(a,1)) = a^1 = a$. Conversely, in order to prove that $\alpha \circ \alpha'|_{\hat{A}} = \mathrm{id}_{\hat{A}}$ it suffices to prove $\alpha \circ \alpha'(\omega(a,b)) = \omega(a,b)$ for all $(a,b) \in A \times B$. This follows from the definitions and from (1):

$$\alpha(\alpha'(\omega(a,b))) = \alpha(a^b) = \alpha(a)^{\alpha(b)} = \omega(a,1)^b = \omega(a,1 \cdot b) = \omega(a,b). \qquad \blacksquare$$

LEMMA 2.3: (a) *The group* $B \ltimes \hat{A}$ *is the free product of its subgroups* $A_1 = A$ *and* B. GROa input, 177
(b) *Let* $K = \langle A^b \mid b \in B \rangle \leq A * B$. *Then* $K = \mathop{\ast}_{b \in B} A^b = \mathrm{Ker}(\pi)$ *and* $A * B = B \ltimes K$.

Proof of (a): The isomorphism α of Lemma 2.2 maps A onto A_1 and B onto B.

Proof of (b): We have $\hat{A} = \mathop{\ast}_{b \in B} A_b$. The isomorphism α' of Lemma 2.2 maps each A_b onto A^b, hence it maps $\hat{A}$ onto K, whence $K = \mathop{\ast}_{b \in B} A^b$. Furthermore, α' maps B identically onto itself, hence $A * B = \alpha'(B \ltimes \hat{A}) = B \ltimes K$. Since π is the identity on B and trivial on K, we conclude that $K = \mathrm{Ker}(\pi)$. $\blacksquare$

If C is a closed subgroup of a profinite group B, then the quotient map $b \mapsto bC$ is a continuous surjection $B \to B/C$ of profinite spaces. By [Rib70, p. 31, Prop. 3.5], this map has a continous section. Hence, B has a closed subset of representatives R for the collection of left cosets bC, $b \in B$.

In the following result we start from R and present $\pi^{-1}(C)$ as a free product of C and conjugates of A with exponents ranging on R.

LEMMA 2.4: *Let A and B be profinite group, $A*B$ their free product, and π: $A*B \to B$ the homomorphism defined by $\pi(a) = 1$ for $a \in A$ and $\pi(b) = b$ for $b \in B$. Consider a closed subgroup C of B and let R be a closed system of representatives of the left cosets bC of B modulo C. Let $H = \pi^{-1}(C)$. Then $H = C \ltimes \mathrm{Ker}(\pi)$ and $H = (\prod^{*}_{r\in R} A^r) * C$.*

GROb input, 220

Proof: Let $K = \mathrm{Ker}(\pi)$. Since π is injective on C, we have $H = C \ltimes K$.

The map $R \times C \to B$ given by $(r, c) \mapsto rc$ is a continuous bijection of profinite spaces, hence so is its inverse β: $B \to R \times C$. Hence, the composition of β with the projection on C is a continuous surjection δ: $B \to C$; it satisfies $\delta^{-1}(c) = Rc$ for each $c \in C$.

By Lemma 2.3(b), $K = \prod^{*}_{b\in B} A^b$. Hence by [Mel90, Theorems 1.4 and 1.5],

$$K = \prod^{*}_{c\in C}\Big(\prod^{*}_{b\in Rc} A^b\Big) = \prod^{*}_{c\in C}\Big(\prod^{*}_{r\in R} A^{rc}\Big) = \prod^{*}_{c\in C}\Big(\prod^{*}_{r\in R} A^{r}\Big)^c.$$

By Lemma 2.3(a) (with $\prod^{*}_{r\in R} A^r, C$ replacing A, B),

$$H = C \ltimes K = C \ltimes \prod^{*}_{c\in C}\Big(\prod^{*}_{r\in R} A^{r}\Big)^c = \Big(\prod^{*}_{r\in R} A^{r}\Big) * C. \qquad \blacksquare$$

3. Normally Generated Groups

NORMAL
input, 11

We fix a global field K, a finite set S of primes of K, a positive integer e, and consider the $\mathfrak{p}$-topology of K for each $\mathfrak{p} \in S$. The intersections of basic $\mathfrak{p}$-open subsets of K with $\mathfrak{p}$ ranging over S form a basis for the **S-adic topology**. For each non-archimedean $\mathfrak{p} \in S$ we choose a Henselian closure $K_\mathfrak{p}$ of K at $\mathfrak{p}$. For a real archimedean $\mathfrak{p} \in S$ we choose a real closure $K_\mathfrak{p}$ of K at $\mathfrak{p}$. Finally, if $\mathfrak{p} \in S$ is archimedean and complex, we set $K_\mathfrak{p}$ to be the algebraic closure $\tilde{K}$ of K. In each case we call $K_\mathfrak{p}$ a **$\mathfrak{p}$-closure** of K. Then

$$K_{\mathrm{tot},S} = \bigcap_{\mathfrak{p}\in S} \bigcap_{\rho\in \mathrm{Gal}(K)} K_\mathfrak{p}^\rho$$

is the maximal Galois extension of K in which each $\mathfrak{p} \in S$ splits.

We denote the separable closure of K by K_s and its absolute Galois group $\mathrm{Gal}(K_s/K)$ by $\mathrm{Gal}(K)$. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ we consider its fixed field in $K_{\mathrm{tot},S}$,

$$K_{\mathrm{tot},S}(\boldsymbol{\sigma}) = \{x \in K_{\mathrm{tot},S} \mid \ x^{\sigma_i} = x, \ \text{for } i = 1, \ldots, e\}.$$

Let $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ be the maximal Galois extension of K in $K_{\mathrm{tot},S}(\boldsymbol{\sigma})$. We prove in this section that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the absolute Galois group $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}])$ is the free product of $\hat{F}_\omega$ with the free product of some of the groups $\mathrm{Gal}(K_\mathfrak{p}^\rho)$. The latter factor depends only on S.

Note that $K_{\mathrm{tot},S}$ does not change if we omit all of the complex archimedean primes from S. Thus, without loss we assume that S contains none of those primes. In other words, $\mathrm{Gal}(K_\mathfrak{p})$ is nontrivial for each $\mathfrak{p} \in S$. This assumption is used in the proof of Lemma 3.2.

MAXMIN
input, 62

Notation 3.1: Let $\mathrm{AlgExt}(K,S) = \{K_\mathfrak{p}^\rho \mid \mathfrak{p} \in S, \ \rho \in \mathrm{Gal}(K)\}$ and $\mathcal{G}al(K,S) = \{\mathrm{Gal}(K_\mathfrak{p}^\rho) \mid \mathfrak{p} \in S, \ \rho \in \mathrm{Gal}(K)\}$. The map $K_\mathfrak{p}^\rho \mapsto \mathrm{Gal}(K_\mathfrak{p}^\rho)$ is a bijection of $\mathrm{AlgExt}(K,S)$ onto $\mathcal{G}al(K,S)$ that commutes with the action of $\mathrm{Gal}(K)$ from the right on those sets. We use that map to endow $\mathrm{AlgExt}(K,S)$ with the strict topology and the étale topology. Since the map $\rho \mapsto \mathrm{Gal}(K_\mathfrak{p}^\rho) = \mathrm{Gal}(K_\mathfrak{p})^\rho$ of $\mathrm{Gal}(K)$ into the profinite space

$\mathrm{Subgr}(\mathrm{Gal}(K))$ (in the strict topology) is continuous, $\mathcal{G}al(K,S)$ is profinite in the strict topology. Therefore, so is $\mathrm{AlgExt}(K,S)$. ∎

LEMMA 3.2: EFRAT input, 82

(a) *If primes* $\mathfrak{p}, \mathfrak{q}$ *of* K *and an element* $\rho \in \mathrm{Gal}(K)$ *satisfy* $K_\mathfrak{p} \neq K_\mathfrak{q}^\rho$, *then* $K_\mathfrak{p} K_\mathfrak{q}^\rho = K_s$

(b) *Every group in* $\mathcal{G}al(K,S)$ *is a maximal element of* $\mathcal{G}al(K,S)$.

(c) *The étale topology of* $\mathcal{G}al(K,S)$ *coincides with its strict topology.*

Proof of (a): The case where $\mathfrak{p}$ and $\mathfrak{q}$ are non-archimedean is a special case of [Efr06, Cor. 21.1.4]. If $\mathfrak{p}$ is non-archimedean and $\mathfrak{q}$ is archimedean, then $\mathrm{Gal}(K_\mathfrak{p})$ is isomorphic to an open subgroup of $\mathrm{Gal}(\mathbb{Q}_p)$ for some prime number p while $K_\mathfrak{q}$ is a real closed field. If in this case $F = K_\mathfrak{p} K_\mathfrak{q}^\rho \neq \tilde{K}$, then $F = K_\mathfrak{q}$ and $\mathrm{Gal}(\mathbb{Q}_p)$ has in involution. This contradicts [HJP06, Lemma 8.3]. If both $\mathfrak{p}$ and $\mathfrak{q}$ are archimedean, then $\mathrm{Gal}(K_\mathfrak{p})$ and $\mathrm{Gal}(K_\mathfrak{q}^\rho)$ are distinct subgroups of $\mathrm{Gal}(K)$ of order 2. Their intersection is therefore trivial.

Proof of (b) and (c): By (a), every pair of distinct groups in $\mathcal{G}al(K,S)$ intersects trivially. Since none of the groups in $\mathcal{G}al(K,S)$ is trivial, there are no inclusions between distinct groups in $\mathcal{G}al(K,S)$. Hence, every group in $\mathcal{G}al(K,S)$ is maximal. By [HJP07, Lemma 2.1], the étale topology of $\mathcal{G}al(K,S)$ coincides with its strict topology. ∎

Following Lemma 3.2(c), we omit the attributes "étale" and "strict" of the topologies of $\mathcal{G}al(K,S)$ and $\mathrm{AlgExt}(K,S)$. In particular, by Notation 3.1, a subset of $\mathcal{G}al(K,S)$ (or of $\mathrm{AlgExt}(K,S)$) is compact if and only if it is closed.

We apply Lemma 3.2 to give another useful example of a Cantor space.

LEMMA 3.3: *Let* M *be an infinite extension of* K *in* $K_{\mathrm{tot},S}$ *and* $\mathcal{R}$ *a compact set of representatives for the* $\mathrm{Gal}(M)$*-orbits of* $\mathcal{G}al(K,S)$. *Then:* CANTOR input, 139

(a) $\mathcal{R} = \dot\bigcup_{\mathfrak{p}\in S} \mathcal{R}_\mathfrak{p}$, *where each* $\mathcal{R}_\mathfrak{p}$ *is a closed set of representatives for the* $\mathrm{Gal}(M)$*-orbits of* $\mathcal{G}al(K,\mathfrak{p})$.

(b) $\mathcal{R}$ *is a Cantor space.*

(c) *For each* $\mathfrak{p} \in S$ *there exists a closed subset* $R_\mathfrak{p}$ *of* $\mathrm{Gal}(K)$ *such that* $\mathcal{R}_\mathfrak{p} = \{\mathrm{Gal}(K_\mathfrak{p})^\rho \mid \rho \in R_\mathfrak{p}\}$ *and the map* $\rho \to G_\mathfrak{p}^\rho$ *is a homeomorphism of* $R_\mathfrak{p}$ *onto* $\mathcal{R}_\mathfrak{p}$.

Proof: For each $\mathfrak{p} \in S$ we set $G_\mathfrak{p} = \mathrm{Gal}(K_\mathfrak{p})$ and break up the proof into three parts.

PART A: *Reduction to the case where S is a singleton.* For each $\mathfrak{p} \in S$ the set $\mathcal{G}al(K,\mathfrak{p}) = \{G_\mathfrak{p}^\rho \mid \rho \in \mathrm{Gal}(K)\}$ is a closed subset of the profinite space $\mathrm{Subgr}(\mathrm{Gal}(K))$, so $\mathcal{G}al(K,S) = \bigcup_{\mathfrak{p}\in S}^{\cdot} \mathcal{G}al(K,\mathfrak{p})$ is also a profinite space.

It follows that $\mathcal{R}$ is a profinite space, so also $\mathcal{R}_\mathfrak{p} = \mathcal{R} \cap \mathcal{G}al(K,\mathfrak{p})$ is a profinite space. Since $\mathcal{R} = \bigcup_{\mathfrak{p}\in S}^{\cdot} \mathcal{R}_\mathfrak{p}$, this proves (a). To complete the proof of (b), it remains to prove that each of the sets $\mathcal{R}_\mathfrak{p}$ is a Cantor space.

PART B: *$\mathcal{R}_\mathfrak{p}$ is a Cantor space.* First note that the weight of $\mathcal{R}_\mathfrak{p}$ is at most $\aleph_0$. Thus, we have to prove that $\mathcal{R}_\mathfrak{p}$ has no isolated points (Definition 1.4). To that end observe that the map $G \mapsto G^{\mathrm{Gal}(M)} = \{G^\mu \mid \mu \in \mathrm{Gal}(M)\}$ from $\mathcal{R}_\mathfrak{p}$ onto $\mathcal{G}al(K,\mathfrak{p})/\mathrm{Gal}(M)$ is a continuous bijection of profinite spaces. Therefore, it is a homeomorphism.

Next note that the map $\mathrm{Gal}(K) \to \mathrm{Subgr}(\mathrm{Gal}(K))$ given by $\rho \mapsto G_\mathfrak{p}^\rho$ is a continuous map of profinite spaces. Since $\mathrm{Aut}(K_\mathfrak{p}/K) = 1$ ([Jar91, Prop. 14.5] if $\mathfrak{p}$ is non-archimedean and [Lan93, p. 455, Thm. 2.9] if $\mathfrak{p}$ is archimedean), $G_\mathfrak{p}^{\rho_1} = G_\mathfrak{p}^{\rho_2}$ if and only if $\rho_2 \in G_\mathfrak{p}\rho_1$. Therefore, the above map induces a homeomorphism $G_\mathfrak{p}\backslash\mathrm{Gal}(K) \to \mathcal{G}al(K,\mathfrak{p})$ mapping $G_\mathfrak{p}\rho$ onto $G_\mathfrak{p}^\rho$. This map is compatible with the action of $\mathrm{Gal}(M)$ on both spaces (on $G_\mathfrak{p}\backslash\mathrm{Gal}(K)$ by multiplication from the right), hence induces a homeomorphism of the quotient profinite spaces $G_\mathfrak{p}\backslash\mathrm{Gal}(K)/\mathrm{Gal}(M) \to \mathcal{G}al(K,\mathfrak{p})/\mathrm{Gal}(M)$. Thus, by [HJP06, Lemma 2.2], it suffices to show that $G_\mathfrak{p}^\rho\mathrm{Gal}(M)$ is an open subset of $\mathrm{Gal}(K)$ for no $\rho \in \mathrm{Gal}(K)$. But $M \subseteq K_\mathfrak{p}^\rho$ and $[M : K] = \infty$, hence $G_\mathfrak{p}^\rho\mathrm{Gal}(M) = \mathrm{Gal}(M)$ is not open.

PART C: *The set $R_\mathfrak{p}$.* The map $\rho \mapsto G_\mathfrak{p}^\rho$ is a continuous surjection of α: $\mathrm{Gal}(K) \to \mathcal{G}al(K,\mathfrak{p})$. By Part B, α decomposes into the quotient map $\mathrm{Gal}(K) \to G_\mathfrak{p}\backslash\mathrm{Gal}(K)$ and a homeomorphism $G_\mathfrak{p}\backslash\mathrm{Gal}(K) \cong \mathcal{G}al(K,\mathfrak{p})$. By [Rib70, p. 31, Prop. 3.5], the quotient map has a continuous section. Hence, also α has a continuous section α': $\mathcal{G}al(K,\mathfrak{p}) \to \mathrm{Gal}(K)$. Since $\mathcal{R}_\mathfrak{p}$ is closed in $\mathcal{G}al(K,\mathfrak{p})$, its image $R_\mathfrak{p}$ under α' is a closed subset of $\mathrm{Gal}(K)$. It satisfies the requirements of (c). ∎

We say that a finite group G is **normally generated by one element** if there exists $g \in G$ such that $G = \langle g^x \mid x \in G\rangle$.

LEMMA 3.4: *Let G be a finite group, L a finite Galois extension of K in $K_{\mathrm{tot},S}$, and e a positive integer, Suppose that there exist elements x, y such that* EL input, 279

(1a) *x is transcendental over L,*

(1b) *y is integral over $L[x]$,*

(1c) *$L(x,y)$ is Galois over $L(x)$ with Galois group G,*

(1d) *$L(x,y)$ is regular over L,*

(1e) *$L(x,y)$ has an L-place φ with $a = \varphi(x) \in L$ and $\varphi(L(x,y)) \subseteq K_{\mathrm{tot},S} \cup \{\infty\}$.*

Then

(a) *there exists an infinite sequence $L_1, L_2, L_3, \ldots$ of linearly disjoint Galois extensions of L with Galois group G contained in $K_{\mathrm{tot},S}$; hence*

(b) *if G is normally generated by one element, then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(L)^e$, the field $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ has a Galois extension in $K_{\mathrm{tot},S}$ with Galois group G.*

Proof of (a): By assumption there exists an absolutely irreducible polynomial $f \in L[X,Y]$, monic and Galois in Y over $L(X)$, such that $f(x,Y) = \mathrm{irr}(y, L(x))$ [FrJ05, Cor. 10.2.2]. By [FrJ05, Lemma 13.1.1], L has a separable Hilbert subset H such that $f(a',Y)$ is Galois over L and $\mathrm{Gal}(f(a',Y),L) \cong G$ for each $a' \in H$ [FrJ05, Lemma 13.1.1]. By (1e), the splitting field of $f(a,Y)$ over L is contained in $K_{\mathrm{tot},S}$. We denote the set of all primes of L lying over S by S_L and note that $L_{\mathrm{tot},S_L} = K_{\mathrm{tot},S}$. By [Jar91, Prop. 12.3] in the non-archimedean case and [Jar91, Prop. 16.7] in the real case, there exists for each $\mathfrak{p} \in S_L$ a $\mathfrak{p}$-open neighborhood $U_{\mathfrak{p}}$ of a in L such that if $a' \in U_{\mathfrak{p}}$ for each $\mathfrak{p} \in S_L$, then the splitting field of $f(a',Y)$ over L is contained in $L_{\mathfrak{p}}$, hence in $K_{\mathrm{tot},S}$.

Suppose, by induction, we have found linearly disjoint Galois extensions $L_1, \ldots, L_n$ of L contained in $K_{\mathrm{tot},S}$ with Galois group G. Let L' be their compositum. Since $f(X,Y)$ is absolutely irreducible, it is irreducible over L'. The separable Hilbert set $H_{L'}(f)$ defined by f over L' contains a Hilbert subset of L [FrJ05, Cor. 12.2.3]. By Geyer [Gey78, Lemma 3.4], the Hilbert subsets of L are dense in the S-adic topology. Hence, there exists $a' \in H \cap \bigcap_{\mathfrak{p} \in S} U_{\mathfrak{p}}$ such that $f(a',Y)$ is irreducible over L'. Let L_{n+1} be the splitting field of $f(a',Y)$ over L. Then L_{n+1} is Galois over L with Galois group G, $L_{n+1} \subseteq K_{\mathrm{tot},S}$, and $[L'L_{n+1} : L'] = \deg(f(a',Y)) = [L_{n+1} : L]$, hence L_{n+1} is linearly disjoint from L' over L.

Proof of (b): For each i choose $\lambda_i \in \mathrm{Gal}(L_i/L)$ which normally generates $\mathrm{Gal}(L_i/L)$. Then let $\Sigma_i = \{\boldsymbol{\sigma} \in \mathrm{Gal}(L)^e \mid \sigma_1|_{L_i} = \lambda_i\}$. If $\boldsymbol{\sigma} \in \mathrm{Gal}(L)^e$, then $L \subseteq K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ because $L \subseteq K_{\mathrm{tot},S}$ and L/K is Galois. Hence, if $\boldsymbol{\sigma} \in \Sigma_i$, then $K_{\mathrm{tot},S}[\boldsymbol{\sigma}] \cap L_i = L$. Hence, $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]L_i \subseteq K_{\mathrm{tot},S}$ and $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}]L_i/K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) \cong \mathrm{Gal}(L_i/L) \cong G$. To conclude the proof we note by Borel-Cantelli [FrJ05, Lemma 18.5.3] that the Haar measure in $\mathrm{Gal}(L)^e$ of $\bigcup_{i=1}^{\infty} \Sigma_i$ is 1. ∎

LEMMA 3.5: *For almost all $(\boldsymbol{\sigma}, \tau) \in \mathrm{Gal}(K)^{e+1}$ the field $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is an infinite extension of K and a proper extension of $K_{\mathrm{tot},S}[\boldsymbol{\sigma}, \tau]$.* SQUARE input, 375

Proof: Let $f(T,X) = X^2 - X - T$ and $a = 0$. Then $f(T,X)$ is an absolutely irreducible polynomial and $f(a,X)$ has two distinct roots in K. Therefore Lemma 3.4 gives a linearly disjoint sequence $L_1, L_2, L_3, \ldots$ of quadratic extensions of K in $K_{\mathrm{tot},S}$. For each n let $\bar{\tau}_n$ be the generator of $\mathrm{Gal}(L_n/K)$. By Borel-Cantelli [FrJ05, Lemma 18.5.3], for almost all $(\boldsymbol{\sigma}, \tau) \in \mathrm{Gal}(K)^{e+1}$ there exist infinitely many positive integers n such that $\sigma_1, \ldots, \sigma_e \in \mathrm{Gal}(L_n)$ and $\tau|_{L_n} = \bar{\tau}_n$. Thus, $L_n \not\subseteq K_{\mathrm{tot},S}[\boldsymbol{\sigma}, \tau]$ and $L_n \subseteq K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$. Consequently, $K_{\mathrm{tot},S}[\boldsymbol{\sigma}, \tau]$ is properly contained in $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ and $(K_{\mathrm{tot},S}[\boldsymbol{\sigma}] : K) = \infty$. ∎

Definition 3.6: Strongly projective, PSC, and ample. Let G be a profinite group and $\mathcal{G}$ a subset of $\mathrm{Subgr}(G)$. A **finite $\mathcal{G}$-embedding problem** for G is a triple (φ: $G \to A$, α: $B \to A, \mathcal{B}$), where A and B are finite groups, φ and α are epimorphism and $\mathcal{B}$ is a subset of $\mathrm{Subgr}(B)$ closed under conjugation such that for each $G_0 \in \mathcal{G}$ there exists a homomorphism γ_0: $G \to B$ such that $\alpha \circ \gamma_0 = \varphi$ and $\gamma_0(G_0)$ is a subgroup of some $B_0 \in \mathcal{B}$. A **solution** to the problem is a homomorphism γ: $G \to B$ such that $\alpha \circ \gamma = \varphi$. The solution is **strong** if in addition for each $G_0 \in \mathcal{G}$ there exists $B_0 \in \mathcal{B}$ such that $\gamma(G_0) \le B_0$. We say that G is **$\mathcal{G}$-projective** if every $\mathcal{G}$-embedding problem for G is solvable. We say that G is **strongly $\mathcal{G}$-projective** if every finite $\mathcal{G}$-embedding problem for G has a strong solution. Note that if $\mathcal{G}$ is closed under conjugation with elements of G and $\mathcal{R}$ is a set of representatives for the G-orbits of $\mathcal{G}$, then G is (strongly) $\mathcal{G}$-projective if and only if G is (strongly) $\mathcal{R}$-projective. AMPLE input, 404

A field extension E of K in $K_{\mathrm{tot},S}$ is said to be **PSC** if every absolutely irreducible variety V defined over E with a simple $K_{\mathfrak p}^{\rho}$-point for all $\mathfrak p \in S$ and $\rho \in \mathrm{Gal}(K)$ has an E-rational point.

A field E is said to be **ample** (or **large**, in the terminology of [Pop96]) if every absolutely irreducible curve defined over E with an E-rational simple point has infinitely many E-rational points. By [Pop96, Prop. 3.1], every PSC field is ample. ∎

Remark 3.7: Cantor free products. We consider the special case of Construction 1.3, CFP input, 445 where S is the finite set of prime divisors of K that we have fixed in this section and $\tilde G = \mathrm{Gal}(K)$. Moreover, for each $\mathfrak p \in S$ the closed subset $R_{\mathfrak p}$ of $\tilde G$ that we consider is now a Cantor space and $G_{\mathfrak p} = \mathrm{Gal}(K_{\mathfrak p})$. Then the corresponding semi-constant sheaf $\mathbf{X} = (\dot{\bigcup}_{\mathfrak p\in S} R_{\mathfrak p} \times G_{\mathfrak p}, \tau, \bigcup_{\mathfrak p\in S} R_{\mathfrak p})$ depends up to an isomorphism only on S (assuming K is fixed). We call X a **Cantor semi-constant sheaf**. If a closed subgroup G of $\mathrm{Gal}(K)$ is isomorphic to $\mathop{\boxed{\ast}}_{\mathfrak p\in S} \mathop{\boxed{\ast}}_{\rho\in R_{\mathfrak p}} G_{\mathfrak p}^{\rho}$, then G depends up to an isomorphism only on S. We say that G is a **Cantor free product** over S. ∎

LEMMA 3.8: *For almost all $\boldsymbol\sigma \in \mathrm{Gal}(K)^e$ each finite proper extension E of $K_{\mathrm{tot},S}[\boldsymbol\sigma]$ in* OMEGA input, 466 *$N = K_{\mathrm{tot},S}$ is ample, there exists a closed set of representatives $\mathcal R$ for the $\mathrm{Gal}(E)$-orbits of $\mathcal{G}al(K,S)$ such that $\mathcal R$ is a Cantor space, and there exists a commutative diagram of profinite groups*

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Ker}(\pi) \arrow[r] & \hat F_\omega * C \arrow[r, "\pi"] & \hat F_\omega \arrow[r] & 1 \\
1 \arrow[r] & \mathrm{Gal}(N) \arrow[r] \arrow[u] & \mathrm{Gal}(E) \arrow[r, "\mathrm{res}"] \arrow[u, "\alpha"'] & \mathrm{Gal}(N/E) \arrow[r] \arrow[u] & 1,
\end{tikzcd} \tag{2}$$

where C is the free inner product over $\mathcal R$, π is the projection map, the horizontal sequences are exact, and the vertical arrows are isomorphisms.

Proof: For almost all $\boldsymbol\sigma \in \mathrm{Gal}(K)^e$ the field $K_{\mathrm{tot},S}[\boldsymbol\sigma]$ is PSC [GeJ02, Thm. A]. By definition, $K_{\mathrm{tot},S}[\boldsymbol\sigma]/K$ is Galois. Let E be a finite proper extension of $K_{\mathrm{tot},S}[\boldsymbol\sigma]$ in N. By Weissauer [FrJ05, Thm. 13.9.1], E is Hilbertian. By [HJP06, Lemma 12.2], E is PSC, hence ample (Definition 3.6). Since $\mathrm{AlgExt}(K,S)$ is compact, $\mathrm{Gal}(E)$ is $\mathcal{G}al(K,S)$-projective [HJP05, Prop. 4.1]. By the first part of [Pop96, Thm. 2.8], $\mathrm{Gal}(E)$ is strongly $\mathcal{G}al(K,S)$-projective.

Since E is countable, the second part of [Pop96, Thm. 2.8] asserts that the $\mathrm{Gal}(E)$-orbits of $\mathcal{G}al(K,S)$ have a compact set of representatives $\mathcal{R}$ and there exists an isomorphism $\alpha\colon \mathrm{Gal}(E) \to \hat{F}_\omega * C$, where C is the inner free product over $\mathcal{R}$. Moreover, by [Pop96, Thm. 2.7], α maps the family $\mathcal{R}$ as a subset of $\mathrm{Subgr}(\mathrm{Gal}(E))$ onto the family $\mathcal{R}$ as a subset of $\mathrm{Subgr}(\hat{F}_\omega * C)$. By Lemma 3.3, $\mathcal{R} = \bigcup_{\mathfrak{p}\in S} \mathcal{R}_\mathfrak{p}$ is a Cantor space, where each $\mathcal{R}_\mathfrak{p}$ is a closed set of representatives for the $\mathrm{Gal}(E)$-orbits of $\mathcal{G}al(K,\mathfrak{p})$. Moreover, $\mathrm{Gal}(K)$ has a closed subset $R_\mathfrak{p}$ such that $\mathcal{R}_\mathfrak{p} = \{\mathrm{Gal}(K_\mathfrak{p})^\rho \mid \rho \in R_\mathfrak{p}\}$ and the map $\rho \mapsto \mathrm{Gal}(K_\mathfrak{p})^\rho$ is a homeomorphism of $R_\mathfrak{p}$ onto $\mathcal{R}_\mathfrak{p}$. By Construction 1.3,

$$C = \mathop{{\prod}^{*}}\limits_{G\in\mathcal{R}} G = \mathop{{\prod}^{*}}\limits_{\mathfrak{p}\in S} \mathop{{\prod}^{*}}\limits_{G\in\mathcal{R}_\mathfrak{p}} G = \mathop{{\prod}^{*}}\limits_{\mathfrak{p}\in S} \mathop{{\prod}^{*}}\limits_{\rho\in R_\mathfrak{p}} \mathrm{Gal}(K_\mathfrak{p})^\rho.$$

Since $E \subseteq N = K_{\mathrm{tot},S}$, the closed normal subgroup of $\mathrm{Gal}(E)$ generated by $\mathcal{R}$ is $\mathrm{Gal}(N)$. Moreover, the closed normal subgroup of $\hat{F} * C$ generated by $\mathcal{R}$ is $\mathrm{Ker}(\pi)$. Hence, $\alpha(\mathrm{Gal}(N)) = \mathrm{Ker}(\pi)$, so α induces an isomorphism of $\mathrm{Gal}(N/E)$ onto $\hat{F}_\omega$ such that Diagram (2) is commutative. ∎

Our next goal is to prove that $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol{\sigma}]/K_{\mathrm{tot},S}[\boldsymbol{\sigma},\tau]) \cong \hat{F}_\omega$ for almost all $(\boldsymbol{\sigma},\tau) \in \mathrm{Gal}(K)^{e+1}$.

LEMMA 3.9: *Let G be a finite group which is normally generated by one element. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the field $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ has a Galois extension in $K_{\mathrm{tot},S}$ with Galois group G.* GROUP input, 558

Proof: For a fixed indeterminate x let $\mathcal{L}$ be the set of all triples (G,L,y), where G is a finite group normally generated by one element, L is a finite Galois extension of K in $K_{\mathrm{tot},S}$, and y is an element of $K(x)_s$ satisfying Conditions (1b)–(1e). We denote the set of all $\boldsymbol{\sigma} \in \mathrm{Gal}(L)^e$ such that $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ has a Galois extension in $K_{\mathrm{tot},S}$ with Galois group G by $\Sigma(G,L,y)$. By Lemma 3.4, the measure of $\Sigma(G,L,y)$ in $\mathrm{Gal}(L)^e$ is 1. Therefore, since $\mathcal{L}$ is countable, the measure of

$$\Sigma_1 = \mathrm{Gal}(K)^e \smallsetminus \bigcup_{(G,L,y)\in\mathcal{L}} \Big[\mathrm{Gal}(L)^e \smallsetminus \Sigma(G,L,y)\Big]$$

in $\mathrm{Gal}(K)^e$ is 1.

Let Σ_2' be the set of all $(\boldsymbol{\sigma},\tau) \in \mathrm{Gal}(K)^{e+1}$ with the following properties: each finite extension of $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ in $K_{\mathrm{tot},S}$ is ample, $K_{\mathrm{tot},S}[\boldsymbol{\sigma},\tau]$ is Galois over K, $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is a proper extension of $K_{\mathrm{tot},S}[\boldsymbol{\sigma},\tau]$, and $(\boldsymbol{\sigma},\tau)$ satisfies the conclusion of Lemma 3.8 with e replaced by $e+1$. By Lemmas 3.5 and 3.8, the measure of Σ_2' is 1. By Fubini, the projection Σ_2 of Σ_2' on the first e coordinates has measure 1 in $\mathrm{Gal}(K)^e$. Therefore, the measure of $\Sigma = \Sigma_1 \cap \Sigma_2$ in $\mathrm{Gal}(K)^e$ is 1.

We consider $\boldsymbol{\sigma} \in \Sigma$ and choose $\tau \in \mathrm{Gal}(K)$ with $(\boldsymbol{\sigma},\tau) \in \Sigma_2'$. Then there exists a proper finite extension E of $K_{\mathrm{tot},S}[\boldsymbol{\sigma},\tau]$ in $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$. By the conclusion of Lemma 3.8, $\mathrm{Gal}(K_{\mathrm{tot},S}/E) \cong \hat{F}_\omega$, so E has a finite Galois extension F in $K_{\mathrm{tot},S}$ with Galois group G.

In addition, E is an ample field, so by [HaJ00, Theorem B], E has field extensions $E(x) \subseteq E(x,y)$, $E(x,y)/E$ regular, and $E(x,y)/E(x)$ Galois with Galois group G. Further, we may choose y to be integral over $E[x]$ and such that $E(x,y)$ has an E-rational place φ with $\varphi(E(x)) = E \cup \{\infty\}$ and $\varphi(E(x,y)) = F \cup \{\infty\}$.

All of this data can be pushed down. That is, K has a finite extension L contained in E such that $L(x,y)/L$ is regular, $L(x,y)/L(x)$ is Galois with Galois group G, y is integral over $L[x]$, L has a Galois extension L' in $K_{\mathrm{tot},S}$ with Galois group G (such that $EL' = F$ and $E \cap L' = L$), $\varphi(L(x)) = L \cup \{\infty\}$, and $\varphi(L(x,y)) = L' \cup \{\infty\}$. The field L need not be Galois over K. However, since $L \subseteq K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$, we may replace L by its Galois closure of K to assume that L/K is Galois (note however, that L need not be contained in E any more). Therefore, $(G,L,y) \in \mathcal{L}$. Since $\boldsymbol{\sigma} \in \Sigma_1 \cup \mathrm{Gal}(L)^e \subseteq \Sigma(G,L,y)$, $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ has a Galois extension in $K_{\mathrm{tot},S}$ with Galois group G, as contended. ∎

LEMMA 3.10: *For almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ has a subfield E and there exists a commutative diagram (2) such that the horizontal rows are short exact sequences, the vertical arrows are isomorphisms, C is a Cantor free product over S, and* $\mathrm{Gal}(K_{\mathrm{tot},S}/K_{\mathrm{tot},S}[\boldsymbol{\sigma}]) \cong \hat{F}_\omega$.

MELNIKOV
input, 647

Proof: Let Σ' be the set of all $(\boldsymbol{\sigma},\tau) \in \mathrm{Gal}(K)^{e+1}$ that satisfy the following conditions:

(3a) $M = K_{\mathrm{tot},S}[\boldsymbol{\sigma}]$ is a proper extension of $K_{\mathrm{tot},S}[\boldsymbol{\sigma},\tau]$.

(3b) For each finite proper extension E of $K_{\mathrm{tot},S}[\boldsymbol{\sigma},\tau]$ in $N = K_{\mathrm{tot},S}$ we have $\mathrm{Gal}(E) \cong$

$\hat F_\omega * C$, where C is a Cantor free product over S and $\mathrm{Gal}(N/E) \cong \hat F_\omega$.

(3c) For each finite group G which is normally generated by one element there exists a finite Galois extension M' of M in N with $\mathrm{Gal}(M'/M) \cong G$.

Note that there are only countably many finite groups (up to isomorphism). Hence, by Lemma 3.5, Lemma 3.8 (with $e+1$ replacing e), and Lemma 3.9 the measure of Σ' in $\mathrm{Gal}(K)^{e+1}$ is one. By Fubini, the measure of the projection Σ of Σ' on the first e coordinates is also 1.

We consider $\boldsymbol\sigma \in \Sigma$ and choose a $\tau \in \mathrm{Gal}(K)$ with $(\boldsymbol\sigma, \tau) \in \Sigma'$. Using (3a) we choose a finite proper extension E of $K_{\mathrm{tot},S}[\boldsymbol\sigma,\tau]$ in $M = K_{\mathrm{tot},S}[\boldsymbol\sigma]$. By (3b), $\mathrm{Gal}(E) \cong \hat F_\omega * C$, where C is a Cantor free product over S and $\mathrm{Gal}(N/E) \cong \hat F_\omega$. Now note that for each prime number p the cyclic group $\mathbb{Z}/p\mathbb{Z}$ is normally generated by one element. Moreover, if B is a finite nonabelian simple group and n is a positive integer, then B^n is normally generated by one element. Indeed, by [Hup67, p. 51], B^n is normally generated by each $(s_1, \ldots, s_n) \in S^n$ with $s_1, \ldots, s_n \neq 1$. It follows from (3c) that each of these groups is realizable as a Galois group over M in N. In addition, $\mathrm{Gal}(N/M) \triangleleft \mathrm{Gal}(N/E)$. Consequently, by [Jar97, Lemma 2.1], $\mathrm{Gal}(N/M) \cong \hat F_\omega$. ∎

THEOREM 3.11: *Let K be a global field, S a finite set of primes of K, and e a positive integer. Then, for almost all $\boldsymbol\sigma \in \mathrm{Gal}(K)^e$ we have $\mathrm{Gal}(K_{\mathrm{tot},S}[\boldsymbol\sigma]) \cong \hat F_\omega * C$, where C is a Cantor free product over S.*

FREEPRODUCT■
input, 710

Proof: Let $N = K_{\mathrm{tot},S}$. By Lemma 3.10, for almost all $\boldsymbol\sigma \in \mathrm{Gal}(K)^e$ the field $M = K_{\mathrm{tot},S}[\boldsymbol\sigma]$ has a subfield E and there exists a commutative diagram

(4)
$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Ker}(\pi) \arrow[r] & \hat F_\omega * C \arrow[r, "\pi"] & \hat F_\omega \arrow[r] & 1 \\
1 \arrow[r] & \mathrm{Gal}(N) \arrow[r] \arrow[u] & \mathrm{Gal}(E) \arrow[r, "\mathrm{res}"] \arrow[u] & \mathrm{Gal}(N/E) \arrow[r] \arrow[u] & 1 \\
1 \arrow[r] & \mathrm{Gal}(N) \arrow[r] \arrow[u, equal] & \mathrm{Gal}(M) \arrow[r, "\mathrm{res}"] \arrow[u] & \mathrm{Gal}(N/M) \arrow[r] \arrow[u] & 1
\end{tikzcd}$$

such that C is a Cantor free product over S, $\pi|_{\hat F_\omega} = \mathrm{id}_{\hat F_\omega}$, $\pi|_C = 1$, the lower vertical arrows are inclusions, the upper vertical arrows are isomorphisms, and $\mathrm{Gal}(N/M) \cong$

$\hat{F}_\omega$. Identifying $\mathrm{Gal}(N/M)$ as a subgroup of $\hat{F}_\omega$ via the right arrows, we obtain that $\mathrm{Gal}(M) \cong \pi^{-1}(\mathrm{Gal}(N/M))$. By Lemma 2.4, $\mathrm{Gal}(M) \cong \mathrm{Gal}(N/M) * \mathop{\ast}_{\rho\in R} C^\rho$, where R is a closed system of representatives for the left cosets of $\mathrm{Gal}(N/E)$ modulo $\mathrm{Gal}(N/M)$, that is $\mathrm{Gal}(N/E) = \bigcup_{\rho\in R} \rho\mathrm{Gal}(N/M)$. If $[M:E] < \infty$, then R is finite, otherwise R is a Cantor subspace of $\mathrm{Gal}(E)$ (Lemma 1.5).

By Remark 3.7, for each $\mathfrak{p} \in S$ there exists a closed Cantor subspace $R_\mathfrak{p}$ of $\mathrm{Gal}(K)$ such that $C = \mathop{\ast}_{\mathfrak{p}\in S} \mathop{\ast}_{\rho\in R_\mathfrak{p}} G_\mathfrak{p}^\rho$, where $G_\mathfrak{p} = \mathrm{Gal}(K_\mathfrak{p})$. Using the associativity of the free product and the ability to change the order of the free product operation (all of which are special cases of the remark succeeding [Mel90, Thm. 1.5]), we rewrite the second free factor of $\mathrm{Gal}(M)$ in the following way:

$$(5) \qquad \mathop{\ast}\limits_{\rho'\in R} C^{\rho'} = \mathop{\ast}\limits_{\rho'\in R} \mathop{\ast}\limits_{\mathfrak{p}\in S} \mathop{\ast}\limits_{\rho\in R_\mathfrak{p}} G_\mathfrak{p}^{\rho\rho'} = \mathop{\ast}\limits_{\mathfrak{p}\in S} \mathop{\ast}\limits_{\rho'\in R} \mathop{\ast}\limits_{\rho\in R_\mathfrak{p}} G_\mathfrak{p}^{\rho\rho'} = \mathop{\ast}\limits_{\mathfrak{p}\in S} \mathop{\ast}\limits_{(\rho,\rho')\in R_\mathfrak{p}\times R} G_\mathfrak{p}^{\rho\rho'}$$

Since nontrivial free factors in a free product are distinct, the map $R_\mathfrak{p} \times R \mapsto R_\mathfrak{p} R$ given by $(\rho, \rho') \mapsto \rho\rho'$ is a continuous bijection of profinite spaces, so it is a homeomorphism. Therefore $R_\mathfrak{p} R$ is a Cantor space and the right hand side of (5) can be rewritten as $\mathop{\ast}_{\mathfrak{p}\in S} \mathop{\ast}_{\mu\in R_\mathfrak{p} R} G_\mathfrak{p}^\mu$. Consequently, the second factor of $\mathrm{Gal}(M)$ is a Cantor free product over S, as desired. ∎

POP input, 805

Remark 3.12: The absolute Galois group of $K_{\mathrm{tot},S}$. The group $\mathrm{Gal}(K_{\mathrm{tot},S})$ is proved to be a Cantor free product over S (in our terminology) in [Pop96]. This is also an easy consequence of our results.

Indeed, as in the proof of Theorem 3.11, let E be an extension of K in $N = K_{\mathrm{tot},S}$ such that $\mathrm{Gal}(E) \cong C * \hat{F}_\omega$, where C is a Cantor free product over S. Then $\mathrm{Gal}(K_{\mathrm{tot},S})$ is isomorphic to the kernel of the projection $C * \hat{F}_\omega$ on $\hat{F}_\omega$. Hence, by Lemma 2.3, $\mathrm{Gal}(K_{\mathrm{tot},S}) \cong \mathop{\ast}_{f\in\hat{F}_\omega} C^f$. It follows as in the last paragraph of the proof of Theorem 3.11 that $\mathrm{Gal}(K_{\mathrm{tot},S})$ is a Cantor free product over S. ∎

4. Finitely Generated Groups

SIGMA input, 9

As in Section 3, we fix a global field K, a finite set S of primes of K, and a positive integer e. We set $N = K_{\mathrm{tot},S}$. Building on our previous results, we prove in this section that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the group $\mathrm{Gal}(N(\boldsymbol{\sigma}))$ is isomorphic to the free product of $\hat{F}_e$ and the Cantor free product over S. The proof of this statement utilizes the following result rather than the deeper Lemmas 3.8 and 3.9.

Lemma 4.1: *For almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ *we have* $\mathrm{Gal}(N/N(\boldsymbol{\sigma})) \cong \hat{F}_e$.

SYMMETRIC input, 22

Proof: For each $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the group $\mathrm{Gal}(N/N(\boldsymbol{\sigma}))$ is generated by $\sigma_1|_N, \ldots, \sigma_e|_N$. Thus, by [FrJ05, Lemma 17.7.1], it suffices to prove that for each finite group B which is generated by e elements and for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the field $N(\boldsymbol{\sigma})$ has a Galois extension in N with Galois group B.

Indeed, consider B as a subgroup of S_n, where $n = |B|$. Let $c_0, \ldots, c_{n-1}$ be integers such that $X^n + c_{n-1}X^{n-1} + \cdots + c_0 = (X-1)(X-2)\cdots(X-n)$. By [Jar91, Propositions 12.3 and 16.7], $\mathbf{c} = (c_0, \ldots, c_{n-1})$ has an open S-adic neighborhood A in K^n such that if $(a_0, \ldots, a_{n-1}) \in A$, then $X^n + a_{n-1}X^{n-1} + \cdots + a_0$ splits into linear factors over each $K_{\mathfrak{p}}$ with $\mathfrak{p} \in S$, hence it splits over N. Now consider the general polynomial $f(\mathbf{T}, X) = X^n + T_{n-1}X^{n-1} + \cdots + T_0$ of degree n, having S_n as its Galois group over $L(\mathbf{T})$ for each field extension L of K.

Inductively suppose we have constructed linearly disjoint finite Galois extensions $L_1, \ldots, L_n$ of K in N with Galois group S_n. Set $L = L_1 \cdots L_n$. By [FrJ05, Cor. 12.2.3 and Lemma 13.1.1], K^n has a separable Hilbert subset H such that $\mathrm{Gal}(f(\mathbf{a}, X), K) \cong \mathrm{Gal}(f(\mathbf{a}, X), L) \cong S_n$ for each $\mathbf{a} \in H$. By [Gey78, Lemma 3.4], there exists $\mathbf{a} \in H \cap A$. The splitting field L_{n+1} of $f(\mathbf{a}, X)$ over K has Galois group S_n, is linearly disjoint from L over K, and is contained in N. This completes the induction.

By construction, there are for each n elements $\sigma_{n,1}, \ldots, \sigma_{n,e} \in \mathrm{Gal}(L_n/K)$ such that $\langle \sigma_{n,1}, \ldots, \sigma_{n,e} \rangle \cong B$. By Borel-Cantelli, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ there exists n such that $\sigma_i|_{L_n} = \sigma_{n,i}$, $i = 1, \ldots, e$ [FrJ05, Lemma 18.5.3]. Therefore, $N(\boldsymbol{\sigma})L_n \subseteq N$ and $\mathrm{Gal}(N(\boldsymbol{\sigma})L_n/N(\boldsymbol{\sigma})) \cong \mathrm{Gal}(L_n/L_n(\boldsymbol{\sigma}_n)) \cong B$, as claimed. ∎

LEMMA 4.2: *For almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ *the field* $N = K_{\mathrm{tot},S}$ *has a subfield* E *such that* $\mathrm{Gal}(E) \cong \hat{F}_\omega * C$*, where* C *is a Cantor free product over* S *and* $\mathrm{Gal}(N/K_{\mathrm{tot},S}(\boldsymbol{\sigma})) \cong \hat{F}_e$*.*

EMELNIKOV
input, 81

Proof: Almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ satisfy the conclusions of Lemmas 3.10 and 4.1. Let $\boldsymbol{\sigma}$ be one of them. Then $N[\boldsymbol{\sigma}]$ has a subfield E containing K such that $\mathrm{Gal}(E) \cong \hat{F}_\omega * C$, where C is a Cantor free product over S. Moreover, $\mathrm{Gal}(N/N(\boldsymbol{\sigma})) \cong \hat{F}_e$. Since $N(\boldsymbol{\sigma})$ contains $N[\boldsymbol{\sigma}]$, it contains E, as desired. ∎

THEOREM 4.3: *Let* K *be a global field,* S *a finite set of primes of* K*, and* e *a positive integer. Then, for almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ *there is a is a Cantor free product* C *over* S *such that* $\mathrm{Gal}(K_{\mathrm{tot},S}(\boldsymbol{\sigma})) \cong \hat{F}_e * C$*,*

EPRODUCT
input, 102

Proof: Repeat the proof of Theorem 3.11 with $\mathrm{Gal}(N/M) \cong \hat{F}_e$ replacing $\mathrm{Gal}(N/M) \cong \hat{F}_\omega$. ∎

References

[Ax67] J. Ax, *Solving diophantine problems modulo every prime,* Annals of Mathematics **85** (1967), 161–183.

[Efr06] I. Efrat, *Valuations, Orderings, and Milnor K-Theory,* Mathematical surveys and monogrphs **124**, American Mathematical Society, Providence, 2006.

[FHV93] M. D. Fried, D. Haran, and H. Völklein, *The absolute Galois group of the totally real numbers,* Comptes Rendus de l'Académie des Sciences **317** (1993), 995–999.

[FrJ05] M. D. Fried and M. Jarden, *Field Arithmetic, Second Edition, revised and enlarged by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2005.

[Gey78] W.-D. Geyer, *Galois groups of intersections of local fields,* Israel Journal of Mathematics **30** (1978), 382–396.

[GeJ02] W.-D. Geyer and M. Jarden, *PSC Galois extensions of Hilbertian fields,* Mathematische Nachrichten **236** (2002), 119–160.

[Har87] D. Haran, *On closed subgroups of free products of profinite groups,* Proceedings of the London Mathematical Society **55** (1987), 266–298.

[HaJ86] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed algebraic field,* Pacific Journal of Mathematics **123** (1986), 55–69.

[HaJ00] D. Haran and M. Jarden, *Regular lifting of covers over ample fields,* manuscript, Tel Aviv (2000), http://www.tau.ac.il/∼jarden/Notes.

[HJP05] D. Haran, M. Jarden, and F. Pop, *P-Adically projective groups as absolute Galois groups,* International Mathematics Research Notices **32** (2005), 1957–1995.

[HJP06] D. Haran, M. Jarden, and F. Pop, *The absolute Galois group of the field of totally S-adic numbers,* manuscript, Tel Aviv, 2006.

[HJP07] D. Haran, M. Jarden, and F. Pop, *Projective group structures as absolute Galois structures with block approximation,* Memoirs of the AMS **189** (2007), 1–56.

[Hup67] B. Huppert, *Endliche Gruppen I,* Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen **134**, Springer, Berlin, 1967.

[Jar91] M. Jarden, *Intersection of local algebraic extensions of a Hilbertian field (A. Barlotti et al., eds),* NATO ASI Series C **333** 343–405, Kluwer, Dordrecht, 1991.

[Jar97] M. Jarden, *Large normal extensions of Hilbertian fields,* Mathematische Zeitschrift **224** (1997), 555–565.

[Lan93] S. Lang, *Algebra, Third Edition,* Eddison-Wesley, Reading, 1993.

[Mel90] O.V. Melnikov, *Subgroups and homology of free products of profinite groups*, Mathematics USSR Izvestija **34** (1990), 97–119.

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

[Rib70] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology,* Queen's papers in Pure and Applied Mathematics **24**, Queen's University, Kingston, 1970.

[RiZ00] L. Ribes and P. Zalesskii, *Profinite Groups,* Ergebnisse der Mathematik (3) **40**, Springer, Berlin, 2000.