Tel-Aviv University

The Raymond and Beverly Sackler

Faculty of Exact Sciences
School of Mathematical Sciences

Hilbertianity under algebraic extensions and Haar measure

A thesis submitted in partial fulfillment of graduation requirements
of the degree of M.Sc. in Tel-Aviv University

By

Bary Lior

Prepared under the supervision of Prof. Dan Haran

July, 2004

Abstract

We give a new proof to the following A. Razon's theorem:

Theorem . *Let K be a countable Hilbertian field and let $e \geq 2$ be an integer. Let M be an abelian extension of K such that the set* $\{\mathrm{ord}(a) \mid a \in \mathrm{Gal}\,(M/K)\}$ *is unbounded. Then for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}\,(K)^e$, every field between $K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ and M is Hilbertian.*

1 Introduction

An algebraic separable field extension M of a Hilbertian field K is Hilbertian, if it satisfies the following essentially group theoretic condition: For certain embedding problems with twisted wreath product there should be **no** solutions contained in a certain Galois extension of K containing M [Ha, Thm. 3.2]. In [Ha] from 1999, D. Haran claims that the hitherto known results in this subject summarized in [JL] in 1992 - e.g., every abelian extension of a Hilbertian field is Hilbertian, Weissauer's Theorem [FrJ, Prop. 15.5], etc - follow from this condition. Haran also proves a new result which produce new Hilbertian algebraic separable field extensions:
Haran's Diamond Theorem *If M_1, M_2 are two Galois extensions of K such that $M_1 \not\subseteq M_2$ and $M_2 \not\subseteq M_1$, then every field extension M of K satisfying $M \subseteq M_1M_2$ and $M \not\subseteq M_i$, $i = 1, 2$, is Hilbertian.*

However, in 1997, shortly before Haran's paper was submitted, in [Ra] A. Razon builds algebraic separable extensions of Hilbertian field which, a-priori, do not follows from Haran's condition.
Theorem 1.(Razon) *Let K be a countable Hilbertian field and let $e \geq 2$ be an integer. Let M be an abelian extension of K such that the set* $\{\mathrm{ord}(a) \mid a \in \mathrm{Gal}\,(M/K)\}$ *is unbounded. Then for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}\,(K)^e$ every field between $K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ and M is Hilbertian.*

Actually, Razon proves that for every abelian extension M' of K that contains M, the field $M'K_s(\boldsymbol{\sigma})$ is Hilbertian *over* M'. Razon also shows that one can replace Hilbertian fields with Hilbertian rings [Ra, Def 2.2]. In this paper we are only interested in Hilbertian fields, hence we focus on Theorem 1 (which follows from the above more general result).

In order to prove Theorem 1, Razon uses the notion of *Pseudo Algebraic Closed (PAC) Field over a field (ring)* [Ra, Def. 1.1] which generalizes the notion of a PAC field. Here are several known properties of PAC fields (see [FrJ]). In the brackets we state the generalization of those properties to PAC fields over a field (see [Ra], [JR]).

a. If E is PAC (over K) and E' is an algebraic extension of E ($E' = EM$, where M/K an algebraic extension), then E' is PAC (over M).

b. If K is a Hilbertian countable field then for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}\,(K)^e$ the field $K_s(\boldsymbol{\sigma})$ is PAC (over K).

c. If E is PAC (over K) and ω-free, then E is a Hilbertian field (over K).

It follows from (a),(b), that for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}\,(K)$ and for every abelian extension M' of K containing M, the field $M'K_s(\boldsymbol{\sigma})$ is PAC over M. A known fact is that for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}\,(G)^e$ the field $K_s(\boldsymbol{\sigma})$ is e- free [FrJ, Thm. 16.13]. From this one can derive that $M'K_s(\boldsymbol{\sigma})$ is ω-free. Thus, by (c), the field $M'K_s(\boldsymbol{\sigma})$ is Hilbertian over M'. Hence, every intermediate field between $M'K_s(\boldsymbol{\sigma})$ to M' is Hilbertian [Ra, Lemma 2.3]. So we get a proof of Theorem 1.

It seems that Razon's proof does not use anything similar to Haran's condition. Moreover, it is not obvious whether one can use Haran's methods in this case.

In this paper, we modify the methods that appeared in [Ha] to this case, i.e., to "agree" with measure theory. For this purpose we can no longer work with a twisted wreath product, but with its subgroups which occur with "high probability".

In Chapter 2 we discuss the twisted wreath product $A\,\mathrm{wr}_{G'}\,G$. We are mostly interested in subgroups of rank 2 which are *full* (Definition 2.2.3). Those subgroups satisfy two important properties. Roughly speaking, the image of such subgroups under certain quotient maps stays noncommutative (unless it is trivial) and the second property is the ability to "recover" the structure of A from the subgroup. We show that there are many such subgroups. In this chapter we also translate the results of group theory to results about fields via Galois theory.

In Chapter 3 we discuss measure theory of pro-finite groups in general, and measure theory of *unbounded groups* (Definition 3.3.1) in particular.

In Chapter 4 we combine group theory with measure theory. We show (using the result from Chapter 3) that one can choose the subgroups of rank 2 (discussed in Chapter 2) with "high probability".

We start from an irreducible polynomial $f(T, X) \in K_s[T, X]$. Then we realize the wreath product $A \,\mathrm{wr}_{G'}\, G$ over the Hilbertian field K, where A is the Galois group of f over $K_s(T)$.

After that, we adjoin a "random field" (i.e. the field $K_s(\boldsymbol{\sigma})$ where $\boldsymbol{\sigma}$ is chosen with probability 1) to the realization of the wreath product, and get a realization of full subgroup of $A \,\mathrm{wr}_{G'}\, G$ over $K_s(\boldsymbol{\sigma})$.

The ability to "recover" the structure of A ensures that the polynomial f remains irreducible over the $K_s(\boldsymbol{\sigma})$. Finally, we compose the field under consideration with the abelian closure of K. The quotient of the full subgroup contained in this abelian extension $(K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})/K_s(\boldsymbol{\sigma}))$ is commutative. By the first property of full subgroups, this quotient must be trivial. This implies that the polynomial remains irreducible even if we compose it with the abelian closure of K.

2 The Twisted Wreath Product

In this section we show that if there is an element in G of large "order" in G/G', then the twisted wreath product $A \,\mathrm{wr}_{G'}\, G$ has a subgroup with rank 2 which is "almost" twisted wreath product. Obviously, we have to explain exactly what we mean "order" of an element in the set G/G' which is not a group, and the meaning of the phrase "almost" wreath product.

2.1 Notations and Definitions

Let A and G be finite groups and let G' be a subgroup of G. Assume that G' acts on A (from the right). Denote $A \,\mathrm{wr}_{G'}\, G = G \ltimes \mathrm{Ind}_{G'}^G(A)$ the twisted wreath product [FrJ, Def. 13.7.2]. More precisely,

$$\mathrm{Ind}_{G'}^G(A) = \{\zeta\colon G \to A \mid \zeta(\sigma\rho) = \zeta(\sigma)^\rho, \forall\sigma \in G\ \forall\rho \in G'\},$$

with pointwise product, $(\xi\zeta)(\sigma) = \xi(\sigma)\zeta(\sigma)$. G acts on $\mathrm{Ind}_{G'}^G(A)$ by the formula $(\zeta^\tau)(\sigma) = \zeta(\tau\sigma)$, $zeta \in \mathrm{Ind}_{G'}^G(A)$, $\sigma, \tau \in G$. Both the group $A \,\mathrm{wr}_{G'}\, G$ and the projection $\mathrm{pr}\colon A \,\mathrm{wr}_{G'}\, G \to G$ called **twisted wreath product**. One can embed A in $\mathrm{Ind}_{G'}^G(A)$ by $a \mapsto \zeta_a$ where $\zeta_a(\rho) = \begin{cases} a^\rho & \rho \in G' \\ 1 & \rho \notin G' \end{cases}$. Choose a set of representatives Σ of right cosets $G'\sigma$ in G, contains the unit element. Then for every $\sigma \in \Sigma$,

$$A^\sigma = \{\zeta \in \mathrm{Ind}_{G'}^G(A) \mid \zeta(G \setminus \sigma^{-1}G') = 1\}.$$

Then $\mathrm{Ind}_{G'}^{G}(A) = \prod_{\sigma\in\Sigma} A^{\sigma}$. Let $N_G = \prod_{\sigma\neq 1} A^{\sigma}$ be the kernel of the projection of $\mathrm{Ind}_{G'}^{G}(A)$ on the first component, i.e., $\zeta \mapsto \zeta(1)$.

Let $\bar{A}$ be a non trivial quotient group of A and let $M = \ker(A \to \bar{A}$. Denote $\bar{a}$ the image of $a \in A$ under the mapping $A \to \bar{A}$. If $M^{G'} = M$ then G' acts on $\bar{A}$ and there is a natural epimorphism mapping element (σ, ζ) of $A \,\mathrm{wr}_{G'}\, G$ to $\overline{(\sigma, \zeta)} = (\sigma, \bar{\zeta})$ of $\bar{A} \,\mathrm{wr}_{G'}\, G$. Here $\bar{\zeta}(\sigma) = \overline{\zeta}(\sigma)$.

Definition 2.1.1. Let $G' \leq G$ be finite groups, and let $\beta \in G$. Define $\mathrm{ord}_{G'}(\beta)$ to be the order of β in the group $\langle\beta\rangle/\langle\beta\rangle \cap G'$.

Proposition 2.1.2. *Let $G' \leq G$ be finite groups and $\beta \in G$.*

(2a) $\mathrm{ord}_{G'}(\beta) = (\langle\beta\rangle : \langle\beta\rangle \cap G') = \min(k \geq 1 \mid \beta^k \in G')$.

(2b) $\beta^k \in G' \iff \mathrm{ord}_{G'}(\beta) \mid k$.

(2c) Let $d = \mathrm{ord}_{G'}(\beta)$. *Then* $\mathrm{ord}_{G'}(\beta^{n_0}) = \frac{d}{\gcd(n_0,d)}$. *Thus* $\mathrm{ord}_{G'}(\beta^{n_0}) \geq \frac{d}{n_0}$.

(2d) If $G' \triangleleft G$, then $\mathrm{ord}_{G'}(\beta)$ *is the order of the image of β in the quotient group G/G'.*

(2e) $\mathrm{ord}_1(\beta) = \mathrm{ord}(\beta)$.

(2f) If $G'' \leq G' \leq G$, then $\mathrm{ord}_{G'}(\beta) \mid \mathrm{ord}_{G''}(\beta)$, *in particular* $\mathrm{ord}_{G'}(\beta) \leq \mathrm{ord}_{G''}(\beta)$.

Proof. Claim $(2a)$ to $(2e)$ are clear. For $(2f)$, consider the exact sequence $\langle\beta\rangle/(\langle\beta\rangle \cap G'') \longrightarrow \langle\beta\rangle/(\langle\beta\rangle \cap G') \longrightarrow 1$. Thus $(\langle\beta\rangle : (\langle\beta\rangle \cap G')) \mid (\langle\beta\rangle : (\langle\beta\rangle \cap G''))$. Conclude, using $(2a)$, that $\mathrm{ord}_{G'}(\beta) \mid \mathrm{ord}_{G''}(\beta)$. ☐

2.2 Ranked 2 subgroups of the twisted wreath product

Lemma 2.2.1. *Let G, H, N, M be finite group such that G acts on N and H acts on M. Assume there exists monomorphisms $j\colon M \to N$, $i\colon H \to G$. We says that the monomorphisms are compatible if $j(m^h) = j(m)^{i(h)}$ for each $h \in H$, $m \in M$. Then*
We can lift i, j to monomorphism $\psi\colon H \ltimes M \to G \ltimes N$ if and only if i, j compatible. Moreover one can choose ψ such that

(1a) $\psi(H \ltimes M) \cap G = \psi(H)$,

(1b) $\psi(H \ltimes M) \cap N = \psi(M)$.

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] & G \ltimes N \arrow[r] & G \arrow[r] & 1 \\ 1 \arrow[r] & M \arrow[r] \arrow[u, hook, "j"] & H \ltimes M \arrow[r] \arrow[u, hook, "\psi"] & H \arrow[r] \arrow[u, hook, "i"] & 1 \end{tikzcd}$$

Proof. Abbreviate (g,n) by gn with product law $ng = gn^g$ and inverse $(gn)^{-1} = g^{-1}n^{-(g^{-1})}$.

If i, j are compatible we define $\psi\colon H \ltimes M \to G \ltimes N$ by

$$\psi(h,m) = (i(h), j(m)) = i(h)j(m).$$

Simple check ensures that ψ is homomorphism:

$$\begin{aligned} &\psi((h_1m_1)(h_2m_2)) = \\ &= \psi(h_1h_2m_1^{h_2}m_2) = i(h_1h_2)j(m_1^{h_2}m_2) = \\ &= i(h_1)i(h_2)j(m_1)^{i(h_2)}j(m_2) = i(h_1)j(m_1)i(h_2)j(m_2) = \end{aligned}$$

Also, ψ is injective. Indeed, if $i(h_1)j(m_1) = i(h_2)j(m_2)$, follows that $i(h_1) = i(h_2)$ and $j(m_1) = j(m_2)$. Since i, j are injective we conclude that $h_1 = h_2$ and $m_1 = m_2$.

Viceversa, if we can lift i, j to embedding $\psi\colon H \ltimes M \to G \ltimes N$, then

$$\begin{aligned} \psi(mh) &= \psi(m)\psi(h) = j(m)i(h) = i(h)j(m)^{i(h)} \\ \psi(mh) &= \psi(hm^h) = i(h)j(m^h) \end{aligned}$$

Hence $j(m^h) = j(m)^{i(h)}$, i.e., i, j are compatible.

Let $gn = \psi(hm)$ be an element of$\psi(H \ltimes M) \cap G$. Since ψ injective follows $g = \psi(h) = i(h)$ and $n = \psi(m) = j(m)$. If $n = 1$, then $m = 1$. Hence (2.2.1a) follows. If $g = 1$, then $h = 1$. Hence (2.2.1b) follws. □

Consider the wreath product $A \operatorname{wr}_{G'} G$. Recall that N_G is the kernel of the projection $\operatorname{Ind}_{G'}^G(A) \to A$ defined by $\zeta \mapsto \zeta(1)$.

Proposition 2.2.2. *Let H be subgroup of G and let $H' = H \cap G'$. Then H' acts on A and $A \operatorname{wr}_{H'} H$ can be embedded in $A \operatorname{wr}_{G'} G$ with the following properties.*

(2a) $A \operatorname{wr}_{H'} H \cap G = H$,

(2b) $A \,\mathrm{wr}_{H'} H \cap \mathrm{Ind}_{G'}^{G}(A) = \mathrm{Ind}_{H'}^{H}(A)$,

(2c) $A \,\mathrm{wr}_{H'} H \cap N_G = \mathrm{Ind}_{H'}^{H}(A) \cap N_G = N_H$.

Proof. For each $\zeta \in \mathrm{Ind}_{H'}^{H}(A)$ we define $\hat{\zeta} \in \mathrm{Ind}_{G'}^{G}(A)$ in the following way. For every $\sigma \in H$ we define $\hat{\zeta}(\sigma) = \zeta(\sigma)$. Extend the definition of $\hat{\zeta}$ to left cosets hG' by $\hat{\zeta}(\sigma\rho) = \zeta(\sigma)^{\rho}$ where $\sigma \in H$ and $\rho \in G'$. Finally we define $\hat{\zeta}(\sigma) = 1$ for every $\sigma \in G \setminus \bigcup_{\tau \in H} \tau G'$. The function $\hat{\zeta}$ is well defined since if $\sigma_1\rho_1 = \sigma_2\rho_2$, where $\sigma_1, \sigma_2 \in H$ and $\rho_1, \rho_2 \in G'$, then $\rho_1\rho_2^{-1} = \sigma_1^{-1}\sigma_2 \in H$ and thus $\rho_1\rho_2^{-1} \in H'$. Hence

$$\hat{\zeta}(\sigma_1\rho_1) = \zeta(\sigma_1)^{\rho_1} = \zeta(\sigma_1)^{\rho_1\rho_2^{-1}\rho_2} = \zeta(\sigma_1\rho_1\rho_2^{-1})^{\rho_2} = \zeta(\sigma_2)^{\rho_2} = \hat{\zeta}(\sigma_2\rho_2).$$

Let $i\colon H \to G$ be the inclusion map. Let $j\colon \mathrm{Ind}_{H'}^{H}(A) \to \mathrm{Ind}_{G'}^{G}(A)$ be the map $\zeta \in \mathrm{Ind}_{H'}^{H}(A) \mapsto \hat{\zeta} \in \mathrm{Ind}_{G'}^{G}(A)$. It is clear that j is injective. Next we show that i, j are compatible, i.e., for each $\zeta \in \mathrm{Ind}_{H'}^{H}(A)$ and for each $\sigma \in H$, $j(\zeta^{\sigma}) = j(\zeta)^{i(\sigma)}$. If $\upsilon \notin \bigcup_{\tau \in H} \tau G'$, then $j(\zeta^{\sigma})(\upsilon) = j(\zeta)^{i(\sigma)}(\upsilon) = 1$. For $\tau \in H$, $\rho \in G'$ we have

$$j(\zeta^{\sigma})(\tau\rho) = \zeta^{\sigma}(\tau)^{\rho} = \zeta(\sigma\tau)^{\rho} = j(\zeta)^{i(\sigma)}(\tau\rho).$$

Use lemma 2.2.1 to conclude that $A \,\mathrm{wr}_{H'} H$ can be embedded in $A \,\mathrm{wr}_{G'} G$. (2.2.2a), (2.2.2b) and (2.2.2c) follows from the definition of this embedding. $\square$

Definition 2.2.3. Let $A \,\mathrm{wr}_{G'} G$ be the twisted wreath product and let $\boldsymbol{S}$ be a subgroup of $A \,\mathrm{wr}_{G'} G$. Put $H = \mathrm{pr}(\boldsymbol{S})$, $H' = H \cap G'$ and consider $A \,\mathrm{wr}_{H'} H$ as a subgroup of $A \,\mathrm{wr}_{G'} G$ via the embedding of proposition 2.2.2. Then $\boldsymbol{S}$ called a **full** if $\boldsymbol{S} \le A \,\mathrm{wr}_{H'} H$ and the following requirement satisfied:

(3a) For every non trivial quotient group $\bar{A} \cong A/M$ of A with $M^{H'} = M$, the group $\bar{\boldsymbol{S}}$ is not commutative. ($\bar{\boldsymbol{S}}$ is the image of $\boldsymbol{S}$ under the epimorphism $A \,\mathrm{wr}_{H'} H \to \bar{A} \,\mathrm{wr}_{H'} H$).

(3b) Let φ be the projection $\mathrm{Ind}_{G'}^{G}(A) \to A$ defined by $\zeta \mapsto \zeta(1)$. Then $\varphi\left(\boldsymbol{S} \cap \mathrm{Ind}_{H'}^{H}(A)\right) = A$.

Lemma 2.2.4. *Let $G' \le G$ and A be finite groups. Put $n = \mathrm{rank} A$. Assume that G' acts on A and let $A \,\mathrm{wr}_{G'} G$ be the twisted wreath product. Let $\beta \in \mathrm{Z}(G)$ with $\mathrm{ord}_{G'}(\beta) \ge 2n$. Then there exist $\zeta \in \mathrm{Ind}_{G'}^{G}(A)$ such that for every $\alpha \in G$ the subgroup $\langle \beta, \alpha\zeta \rangle$ is full.*

Proof. Let $a_1, \dots, a_n$ be a set of generators of A. Put $m = \mathrm{ord}_{G'}(\beta)$. Then $\beta, \dots, \beta^m$ are representative of the left cosets of $\langle\beta\rangle \cap G'$ in $\langle\beta\rangle$. Define ζ as a function from $\langle\beta\rangle$ to A in the following way.

$$\zeta(\beta^k) = \begin{cases} a_i & 1 \le i \le n \text{ and } k = 2i \\ 1 & \text{otherwise} \end{cases}$$

For $\sigma = \beta^k\rho$, where $\rho \in \langle\beta\rangle \cap G'$ and $1 \le k \le m$, define $\zeta(\sigma) = \zeta(\beta^k)^\rho$.

Let $\alpha \in G$ and $\boldsymbol{S} = \langle\beta, \alpha\zeta\rangle$. From the construction it is obvious that $\zeta \in \mathrm{Ind}_{\langle\beta\rangle\cap G'}^{\langle\beta\rangle}(A)$. In particular, $\zeta \in \mathrm{Ind}_{\langle\beta,\alpha\rangle\cap G'}^{\langle\beta,\alpha\rangle}(A)$. Conclude that $\boldsymbol{S} \le A \,\mathrm{wr}_{H'} H$ where $H = \langle\beta,\alpha\rangle = \mathrm{pr}(\boldsymbol{S})$ and $H' = H \cap G'$. Let $\bar{A} \neq 1$ be a quotient group of A such that the action of G' fixed the kernel of $A \to \bar{A}$. There exist i with $\bar{a}_i \neq \bar{1}$. Since $\beta \in \mathrm{Z}(G)$ we have $(\alpha\zeta)^\beta = \alpha^\beta\zeta^\beta = \alpha\zeta^\beta$. But

$$\bar{\zeta}(\beta^{2i-1}) = \bar{1} \neq \bar{a}_i = \bar{\zeta}(\beta^{2i}) = \bar{\zeta}^\beta(\beta^{2i-1}).$$

Thus $\overline{(\alpha\zeta)^\beta} \neq \overline{(\alpha\zeta)}$, i.e., $\bar{\boldsymbol{S}}$ is not commutative. this proves (2.2.3a).

For every $1 \le i \le n$ define

$$h_i = (\alpha\zeta)^{-\beta}(\alpha\zeta)^{\beta^{2i}} = \zeta^{-\beta}\zeta^{\beta^{2i}}.$$

Hence $h_i(1) = \zeta^{-\beta}(1)\zeta(\beta^{2i}) = \zeta^{-1}(\beta)a_i = a_i$. Since $h_i \in \boldsymbol{S} \cap \mathrm{Ind}_{H'}^{H}(A)$ we conclude that the image of $\boldsymbol{S} \cap \mathrm{Ind}_{H'}^{H}(A)$ via φ is all A. This proves (2.2.3b). $\square$

2.3 Interpretation in Fields

Definition 2.3.1. Let $K \subseteq K' \subseteq L$ be a tower of finite field extensions. Assume that L/K is Galois extension. Put $G = \mathrm{Gal}(L/K)$ and $G' = \mathrm{Gal}(L/K')$. Let $\beta \in G$. We define $\mathrm{ord}_{K'}(\beta) = \mathrm{ord}_{G'}(\beta)$ (see 2.1.1).

The following proposition follows immediately from proposition 2.1.2 via Galois theory.

Proposition 2.3.2. *Let $K \subseteq K' \subseteq K'' \subseteq L$ be a tower of finite fields extensions and assume that L/K is Galois. Let $\beta \in \mathrm{Gal}(L/K)$. Then*

(2a) $\mathrm{ord}_{K'}(\beta) = (\langle\beta\rangle : \langle\beta\rangle \cap \mathrm{Gal}(L/K')) = \min(k \ge 1 \mid \beta^k|_{K'} = \mathrm{id})$.

(2b) Let $d = \mathrm{ord}_{K'}(\beta)$. Then $\mathrm{ord}_{K'}(\beta^{n_0}) = \frac{d}{\gcd(n_0,d)}$. Thus $\mathrm{ord}_{K'}(\beta^{n_0}) \ge \frac{d}{n_0}$,

(2c) If K'/K is Galois, then $\mathrm{ord}_{K'}(\beta)$ *is the order of* $\beta|_{K'}$ *in the group* $\mathrm{Gal}\,(K'/K)$*,*

(2d) $\mathrm{ord}_{K'}(\beta) \mid \mathrm{ord}_{K''}(\beta)$*, in particular* $\mathrm{ord}_{K'}(\beta) \leq \mathrm{ord}_{K''}(\beta)$*.*

Assume that K'/K is separable algebraic extension, and assume that F/K' is Galois. For K-embedding, $\sigma\colon K' \to K_s$, we denote F^σ the field $F^{\hat{\sigma}}$ where $\hat{\sigma}$ is an lifting of σ to $\mathrm{Gal}\,(K)$. It is well defined. We denote $\mathcal{E}(K'/K)$ the family of all K-embedding, $K' \to K_s$.

Remark 2.3.3. We say the a tower of finite fields extensions $K \subseteq K' \subseteq L \subseteq F \subseteq \hat{F}$ **realize** $A \,\mathrm{wr}_{G'}\, G$ if [FrJ, Remark 13.7.6]:

(3a) L/K, F/K' and $\hat{F}/K$ are Galois.

(3b) The fields $\{F^\sigma\}_{\sigma\in\mathcal{E}(K'/K)}$ are linearly disjoint over L and

$$\hat{F} = \prod_{\sigma\in\mathcal{E}(K'/K)} F^\sigma.$$

(3c) There exist field extension $\hat{K}$ of K such that $L \cap \hat{K} = K$ and $L\hat{K} = \hat{F}$.

(3d) $G \cong \mathrm{Gal}\left(\hat{F}/\hat{K}\right) \cong \mathrm{Gal}\,(L/K)$, $A = \mathrm{Gal}\,(F/L)$. If we put $F' = F \cap (K'\hat{K})$, then $G' \cong \mathrm{Gal}\,(L/K') \cong \mathrm{Gal}\,(F/F') \cong \mathrm{Gal}\left(\hat{F}/K'\hat{K}\right)$.

$$\begin{tikzcd}
& F^\sigma \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[r, dash, "A"'] \arrow[d, dash, "G'"] & F \arrow[r, dash, "N"'] \arrow[d, dash, "G'"] & \hat{F} \arrow[d, dash, "G'"] \\
K' \arrow[r, dash, "A"'] \arrow[d, dash] & F' \arrow[r, dash] & K'\hat{K} \arrow[d, dash] \\
K \arrow[rr, dash] & & \hat{K}
\end{tikzcd}$$

The group $G' = \mathrm{Gal}\,(F/F')$ acts on the $A \lhd \mathrm{Gal}\,(F/K')$ by conjugation in $\mathrm{Gal}\,(F/K')$ and $G = \mathrm{Gal}\left(\hat{F}/\hat{K}\right)$ acts on $\mathrm{Ind}_{G'}^{G}(A) = \mathrm{Gal}\left(\hat{F}/L\right)$ by conjugation in $\mathrm{Gal}\left(\hat{F}/K\right)$. By Galois theory we conclude that $\mathrm{Gal}\left(\hat{F}/K\right) \cong G \ltimes \mathrm{Ind}_{G'}^{G}(A) = A \,\mathrm{wr}_{G'}\, G$.

Viceversa, assume that $\mathrm{Gal}\left(\hat{F}/K\right) \cong A \,\mathrm{wr}_{G'}\, G$. Let F, L, $\hat{K}$ be the fixed fields of N_G, $\mathrm{Ind}_{G'}^{G}(A)$ and $\hat{K}$ respectively. Let K' be the fixed field of the image of G' under the isomorphism $\mathrm{res}_L \colon G \to \mathrm{Gal}\,(L/K)$. Then the above conditions fulfilled.

Assume that $K, K', L, F, \hat{F}$ realize $A \,\mathrm{wr}_{G'}\, G$, where A, G finite groups and G' subgrouop of G which acts on A. For every Galois extension $L \subsetneq P \subseteq F$ of K' with Galois group $\bar{A} = \mathrm{Gal}\,(P/L)$ put $\hat{P} = \prod_{\sigma \in \mathcal{E}(K'/K)} P^{\sigma}$. Then $K, K', L, P, \hat{P}$ realize $\bar{A} \,\mathrm{wr}_{G'}\, G$. In particular $\hat{P}$ is the Galois closure of P over K.

Proposition 2.3.4. *Let $K, K', L, F, \hat{F}$ be a tower of fields which realize $A \,\mathrm{wr}_{G'}\, G$ for some $G' \leq G$, A and an action of G' on A. Let $H \leq G$ and $H' = H \cap G'$. By proposition 2.2.2 $A \,\mathrm{wr}_{H'}\, H$ embedd in $A \,\mathrm{wr}_{G'}\, G$. Let D be the fixed field of $A \,\mathrm{wr}_{H'}\, H$ in $\hat{F}$. Then $D, K'D, LD, FD, \hat{F}$ realize $A \,\mathrm{wr}_{H'}\, H$.*

Proof. Proposition 2.2.2 and Galois theory implies that

$$\begin{aligned}
\mathrm{Gal}\left(\hat{F}/D\right) &\cong A \,\mathrm{wr}_{H'}\, H, \\
\mathrm{Gal}\left(\hat{F}/LD\right) &= \mathrm{Ind}_{G'}^{G}(A) \cap A \,\mathrm{wr}_{H'}\, H = \mathrm{Ind}_{H'}^{H}(A), \\
\mathrm{Gal}\left(\hat{F}/FD\right) &= N_G \cap A \,\mathrm{wr}_{H'}\, H = N_H, \\
\mathrm{Gal}\left(\hat{F}/\hat{K}D\right) &= G \cap A \,\mathrm{wr}_{H'}\, H = H, \\
\mathrm{Gal}\,(LD/K'D) &= \mathrm{Gal}\left(\hat{F}/K'\hat{K}D\right) = G' \cap A \,\mathrm{wr}_{H'}\, H = G' \cap H = H'.
\end{aligned}$$

Then by remark 2.3.3 we conclude that $D, K'D, LD, FD, \hat{F}$ realize $A \,\mathrm{wr}_{H'}\, H$. □

Proposition 2.3.5. *Let E/K fields extension. We identify $\mathrm{Gal}\left(\hat{F}E/E\right)$ and $\mathrm{Gal}\left(\hat{F}/\hat{F} \cap E\right)$ via the restriction map. Assume that $\mathrm{Gal}\left(\hat{F}/K\right) \cong A \,\mathrm{wr}_{G'}\, G$ and put $\boldsymbol{S} = \mathrm{Gal}\left(\hat{F}E/E\right)$. Let $A \,\mathrm{wr}_{H'}\, H \leq A \,\mathrm{wr}_{G'}\, G$, where $H = \mathrm{pr}(\boldsymbol{S})$ and $H' = H \cap G'$. Let D be the fixed field of $A \,\mathrm{wr}_{H'}\, H$ in $\hat{F}$. Then $\boldsymbol{S}$ is full subgroup of $A \,\mathrm{wr}_{G'}\, G$ if and only if the following conditions satisfied :*

(5a) For every P as above the group $\mathrm{res}_{\hat{P}} \boldsymbol{S} \cong \mathrm{Gal}\left(\hat{P}E/E\right)$ is not commutative.

(5b) $\mathrm{Gal}\,(FE/LE) \cong \mathrm{Gal}\,(F/L) = A$, *i.e,* $[FE : LE] = [F : L]$.

(5c) $D \subseteq E$.

Proof. By Galois theory $\boldsymbol{S} \leq A \,\mathrm{wr}_{H'}\, H$ if and only if $D \subseteq \hat{F} \cap E$. Since $D \subseteq \hat{F}$ follows that $D \subseteq \hat{F} \cap E$ if and only if $D \subseteq E$. Thus condition (5 c) is equivalent to the condition $\boldsymbol{S} \leq A \,\mathrm{wr}_{H'}\, H$ in definition 2.2.3.

By Galois theory there is a bijection between Galois extensions P of L contained in F to normal subgroups M of A. $L \neq P$ if and only if $M \neq A$ and P is Galois over K' if and only if $M^{G'} = M$. Thus there is bijection between $L \subsetneq P \subseteq F$ which are Galois over K' to normal subgroups $M \neq A$ of A satisfying $M^{G'} = M$. If P corresponds to M, write $\bar{A} = A/M \neq 1$, Then $\mathrm{Gal}\left(\hat{P}/K\right) \cong \bar{A} \,\mathrm{wr}_{G'}\, G$. Thus $\mathrm{res}_{\hat{P}} \boldsymbol{S} = \bar{\boldsymbol{S}}$ and therefore (2.2.3a) is equivalent to (5 a).

Consider the group $\mathrm{Gal}\left(\hat{F}/K\right)$. The field F is the fixed field of $N = N_G$, the kernel of the projection $\zeta \mapsto \zeta(1)$ from $\mathrm{Ind}_{G'}^{G}(A)$ to A. The field L is the fixed field of $\mathrm{Ind}_{G'}^{G}(A)$, and thus $[F : L] = (\mathrm{Ind}_{G'}^{G}(A) : N) = |A|$. Consider $\boldsymbol{S} \cap N$ and $\boldsymbol{S} \cap \mathrm{Ind}_{G'}^{G}(A)$ as subgroups of $\boldsymbol{S} \cong \mathrm{Gal}\left(\hat{F}E/E\right)$. By Galois theory FE, LE are the fixed fields of $\boldsymbol{S} \cap N$, $\boldsymbol{S} \cap \mathrm{Ind}_{G'}^{G}(A)$ in $\hat{F}E$ respectively. Thus, $[FE : LE] = (\boldsymbol{S} \cap \mathrm{Ind}_{G'}^{G}(A) : \boldsymbol{S} \cap N)$.

$$\begin{tikzcd}
\hat{F} \arrow[r, dash] \arrow[d, dash, "N"'] & \hat{F}E \arrow[d, dash] \\
F \arrow[r, dash] \arrow[d, dash, "A"'] & FE \arrow[d, dash, "A"] \\
L \arrow[r, dash] \arrow[d, dash] & LE \arrow[d, dash] \\
K \arrow[r, dash] & E
\end{tikzcd}$$

Since $\mathrm{Gal}\,(FE/LE) \leq \mathrm{Gal}\,(F/L)$ follows that $\mathrm{Gal}\,(FE/LE) = \mathrm{Gal}\,(F/L)$ if and only if $[FE : LE] = [F : L]$. Thus

$$\mathrm{Gal}\,(FE/LE) = \mathrm{Gal}\,(F/L) \Longleftrightarrow (\boldsymbol{S} \cap \mathrm{Ind}_{G'}^{G}(A) : \boldsymbol{S} \cap N) = |A|.$$

we conclude that (5 b) equivalent to (2.2.3b). □

In order to prove the main theorem we need to implement 2.2.4 in fields.

Lemma 2.3.6. *Let $\boldsymbol{S} \leq A \operatorname{wr}_{G'} G$ be full subgroup such that the projection on G, $\operatorname{pr}(\boldsymbol{S})$, is commutative. Assume that $K, K', L, F, \hat{F}$ realize $A \operatorname{wr}_{G'} G$. Let E/K be fields extension such that $\hat{F} \cap E$ contained in the fixed field of $\boldsymbol{S}$ in $\hat{F}$ and let M/E be abelian extension with $K'E \subseteq M$. Then $[FM : LM] = [F : L]$.*

Proof. Part A: We can assume that $\boldsymbol{S} \cong \operatorname{Gal}\left(\hat{F}E/E\right)$.

Indeed, Let E' be the fixed field of $\boldsymbol{S}$ in $\hat{F}E$. if $E \subsetneq E'$, then replace E with E' and M with ME'. If $[FME' : LME'] = [F : L]$, then in particular $[FM : LM] = [F : L]$.

Part B: We can assume that $\operatorname{pr}(\boldsymbol{S}) = G$.

Indeed, Put $H = \operatorname{pr}(\boldsymbol{S})$, $H' = H \cap G'$. Let D be the fixed field of $A \operatorname{wr}_{H'} H$ in $\hat{F}$. Then $D, DK', DL, DF, \hat{F}$ realize $A \operatorname{wr}_{H'} H$ (proposition 2.3.4). Replace $K \subseteq K' \subseteq L \subseteq F \subseteq \hat{F}$ with $D \subseteq DK' \subseteq DL \subseteq DF \subseteq \hat{F}$. Since $D \subseteq E$ (proposition 2.3.5), follows that $K'D \subseteq K'E \subseteq M$. Since $[DF : DL] = |A| = [F : L]$, it is enough to show that $[DFM : DLM] = [DF : DL]$.

$$
\begin{tikzcd}[arrows=dash]
\hat{F} \arrow[r] \arrow[d] & \hat{F}E \arrow[r] \arrow[d] & \hat{F}M \arrow[d] \\
F \arrow[r] \arrow[d] & FE \arrow[r] \arrow[d] & FM \arrow[d] \\
L \arrow[r] \arrow[d] & LE \arrow[r] \arrow[d] & LM \arrow[d] \\
K' \arrow[r] \arrow[d] & K'E \arrow[r] \arrow[d] & M \\
K \arrow[r] & E &
\end{tikzcd}
$$

Part C: Conclusion of the proof.

(2.3.5 b) implies that $[F : L] = [FE : LE]$. By Part A, $\boldsymbol{S} = \operatorname{Gal}\left(\hat{F}E/E\right)$. Hence $\operatorname{pr}(\boldsymbol{S}) = \operatorname{Gal}(LE/E)$. On the other hand, by Part B, $\operatorname{pr}(\boldsymbol{S}) = G = \operatorname{Gal}(L/K)$. Hence $[L : K] = [LE : E]$. We conclude that

$$[F : K'] = [F : L][L : K'] = [FE : LE][LE : K'E] = [FE : K'E].$$

In the above calculation we used the fact that if $[L:K]=[LE:E]$, then for every field K' between L and K, $[L:K']=[LE:K'E]$. Moreover, since $\mathrm{Gal}(FE/K'E) \leq \mathrm{Gal}(F/K')$ follows $\mathrm{Gal}(F/K') = \mathrm{Gal}(FE/K'E)$.

Assume that $FE \cap LM \neq LE$. The intersection $FE \cap LM$ is sub extension of $FE/K'E$ containing LE. Thus there exist P satisfying $L \subseteq P \subseteq F$, $PE = FE \cap LM$ and P/K' Galois. Since $PE \neq LE$ follows that $P \neq L$. $\hat{P} = \prod_{\sigma \in G} P^\sigma = \prod_{\sigma \in \mathcal{E}(K'/K)} P^\sigma$ is the Galois closure of P over K. More over, $\hat{P}E$ is the Galois closure of PE over E. Indeed, the Galois closure of PE over E is the composition of all the conjugates fields, i.e.,

$$\prod_{\sigma \in \boldsymbol{S}} (PE)^\sigma = \prod_{\sigma \in \mathrm{pr}(\boldsymbol{S})} (PE)^\sigma = \prod_{\sigma \in G} P^\sigma E = \hat{P}E.$$

Here we used that $\mathrm{pr}(\boldsymbol{S}) = G$, PE/LE is Galois and thus $(PE)^\sigma$ depends only on the restriction of $\sigma \in \boldsymbol{S}$ to LE.

Since $\hat{P}E$ is the Galois closure of PE over E and since $PE \subseteq LM$, we conclude that $\hat{P}E \subseteq LM$. In Part B we showed that $\mathrm{Gal}(LE/E) = \mathrm{pr}(\boldsymbol{S})$ and thus LE/E is abelian extension. By assumption M/E is abelian extension. Thus LM/E is abelian extension. In particular $\mathrm{Gal}\left(\hat{P}E/E\right)$ is abelian. But by (2.3.5b) $\mathrm{Gal}\left(\hat{P}E/E\right)$ is not abelian. Contradiction!

From the contradiction we conclude that $FE \cap LM = LE$ and thus FE, LM are linearly disjoint over LE. In particular $[FM:LM] = [FE:LE] = [F:L]$. $\square$

Corollary 2.3.7. *Let $n_0 \in \mathbb{N}$ and $A \,\mathrm{wr}_{G'}\, G$ be wreath product of finite groups. Let $n = \mathrm{rank} A$. Assume that $K, K', L, F, \hat{F}$ realize $A \,\mathrm{wr}_{G'}\, G$. Let $\beta \in G$ such that* $\mathrm{ord}_{K'}(\beta) \geq 2nn_0$ *and $\beta^{n_0} \in \mathrm{Z}(G)$. Then there exist $\zeta \in \mathrm{Ind}_{G'}^{G}(A)$ such that for all $\sigma_1, \sigma_2 \in \mathrm{Gal}(K)$ with $\sigma_2|_{\hat{F}} \in G\zeta$, $\sigma_1|_{\hat{F}} = \beta$, if $M/K_s(\boldsymbol{\sigma})$ is an abelian extension containing K', then $[FM:LM] = [F:L]$.*

Proof. Let $\beta_0 = \beta^{n_0}$. (2.3.2b) implies that $\mathrm{ord}_{K'}(\beta_0) \geq 2n$. For β_0 take the suitable $\zeta \in \mathrm{Ind}_{G'}^{G}(A)$ from 2.2.4. Let σ_1, σ_2 be such that $\sigma_1|_{\hat{F}} = \beta$, $\sigma_2|_{\hat{F}} = \alpha\zeta$ for some $\alpha \in G$. The subgroup $\boldsymbol{S} = \langle \beta_0, \alpha\zeta \rangle$ of $A \,\mathrm{wr}_{G'}\, G$ is full (lemma 2.2.4). $\mathrm{pr}(\boldsymbol{S})$ is abelian since $\beta_0 \in \mathrm{Z}(G)$.

Let $E = K_s(\boldsymbol{\sigma})$. Since $\langle \sigma_1^{n_0}, \sigma_2 \rangle \leq \langle \sigma_1, \sigma_2 \rangle$ follows that $E \subseteq K_s(\sigma_1^{n_0}, \sigma_2)$. Hence $\hat{F} \cap E$ is contained in the fixed field of $\boldsymbol{S}$ in $\hat{F}$. By using the previous lemma, we get that $[FM:LM] = [F:L]$ for every abelian extension $M/K_s(\boldsymbol{\sigma})$ that contains K'. $\square$

3 Haar Measure of Profinite Groups

3.1 Notation and definitions

We define the Haar measure, μ, of a profinite group A as in [FrJ, Chapter 16], i.e., normalized Haar measure on a compact group.

Two subsets X, Y of a profinite group A called **independent** if $\mu(X \cap Y) = \mu(X)\mu(Y)$. Family of subsets $\{X_i\}_{i\in I}$ of A called **independence** if $\mu(\cap_{j\in J} X_j) = \prod_{j\in J} \mu(X_j)$ for every finite subset $J \subseteq I$.

For a field K we consider the measure of the absolute Galois group of K, i.e., the measure of the group $\mathrm{Gal}\,(K) = \mathrm{Gal}\,(K_s/K)$. Usually we write this measure by μ.

Two fields extensions L_1, L_2 of K called **linearly disjoint over** K if every linearly independence set $\{x_1, \ldots, x_n\}$ of elements of L_1 over K remains linearly independent over L_2 [La, VIII,§3]. This definition is not dependent in the order of the fields [FrJ, lemma 2.5.1]. Finite collection of fields extensions $\{L_1, \ldots, L_n\}$, $n > 2$, of K called **linearly disjoint over** K if $\{L_1, \ldots, L_{n-1}\}$ is linearly disjoint over K and L_n is linearly disjoint from $L_1 \cdots L_{n-1}$ over K. In this case the order is irrelevant for the definition. A family of fields extensions $\{L_1, L_2, L_3, \ldots\}$ of K is called **linearly disjoint over** K if every finite subset is linearly disjoint over K.

There is firm connection between linearly disjoint extensions of K and independence subsets of $\mathrm{Gal}\,(K)$. Examples for this connections can be found in [FrJ, 9.61] or in the following lemma 3.2.1.

3.2 Probabilistic independence in semi direct products

Lemma 3.2.1. *For each $i \in \mathbb{N}$ let $K \subseteq N \subseteq M_i$ be a tower of finite Galois extensions over K. Assume that $\{M_i\}$ are linearly disjoint over N. Let $S_i \subseteq \mathrm{Gal}\,(M_i/K)$ be a set such that* $\mathrm{res}\colon \mathrm{Gal}\,(M_i/K) \to \mathrm{Gal}\,(N/K)$ *maps S_i bijectively on* $\mathrm{Gal}\,(N/K)$. *Then $X_i = \{\sigma \in \mathrm{Gal}\,(K) \mid \mathrm{res}_{M_i}(\sigma) \in S_i\}$ are μ-independence.*

Proof. We need to show that for every $n \in \mathbb{N}$ and for every $i_1, \ldots, i_n$ different natural numbers, $\mu(\bigcap_{j=1}^n X_{i_j}) = \prod_{j=1}^n \mu(X_{i_j})$. For simplicity of notations assume that $i_j = j$.

Since $X_i = \mathrm{res}_{M_i}^{-1}(S_i)$ and since the Haar measure of a finite group is the normal counting measure, we get that $\mu(X_i) = \frac{\#S_i}{[M_i:K]} = \frac{[N:K]}{[M_i:K]} = \frac{1}{[M_i:N]}$.

Put $\hat{M} = M_1 \cdots M_n$. Since the fields $\{M_i\}$ are linearly disjoint over N, follows, by Galois theory, that

$$\begin{aligned}\mathrm{Gal}\left(\hat{M}/K\right) &\cong \{(\sigma_1, \ldots, \sigma_n) \in \prod_{i=1}^{n} \mathrm{Gal}\,(M_i/K) \mid \mathrm{res}_N\sigma_1 = \cdots = \mathrm{res}_N\sigma_n\},\\ \mathrm{Gal}\left(\hat{M}/N\right) &\cong \mathrm{Gal}\,(M_1/N) \times \cdots \times \mathrm{Gal}\,(M_n/N)\,.\end{aligned}$$

Here the isomorphism is defined by $\sigma \mapsto (\sigma_1, \ldots, \sigma_n)$, where $\sigma_i = \mathrm{res}_{M_i}\sigma$ for $1 \leq i \leq n$.

Let $S = \{\sigma \in \mathrm{Gal}\left(\hat{M}/K\right) \mid \forall i\ \sigma_i \in S_i\}$. We count the elements of S. Let $\alpha \in \mathrm{Gal}\,(N/K)$ and let $1 \leq i \leq n$. Since S_i maps bijectively onto $\mathrm{Gal}\,(N/K)$ there exist unique $\sigma_i \in S_i$ mapping to α. Thus there exist unique element of S that his restriction to N is α. We conclude that S has $[N : K]$ element. Write μ' the measure of $\mathrm{Gal}\left(\hat{M}/K\right)$ and get

$$\mu(\bigcap_{i=1}^{n} X_i) = \mu'(S) = \frac{[N : K]}{[\hat{M} : K]} = \frac{1}{[\hat{M} : N]} = \prod_{i=1}^{n} \frac{1}{[M_i : N]} = \prod_{i=1}^{n} \mu(X_i).$$

$\square$

Lemma 3.2.2. *[FrJ, 902] Let H, G be profinite groups and $G \times H$ be their direct product. Let $X_i \subseteq G$, $i \in \mathbb{N}$, be a family of independence sets with respect to G and $Y_j \subseteq H$, $j \in \mathbb{N}$, be a family of independence sets with respect to H. Then $\{X_i \times Y_i\}$ is independence with respect to the product $G \times H$.*

Proof. We need to show that the measure of the intersection of finite collection of $X_i \times Y_i$ is equal to the product of the measures. Indeed,

$$\begin{aligned}\mu\left(\bigcap_{i=1}^{N}(X_i \times Y_i)\right) &= \mu\left(\left(\bigcap_{i=1}^{N} X_i\right) \times \left(\bigcap_{i=1}^{N} Y_i\right)\right) =\\ &= \mu_G\left(\bigcap_{i=1}^{N} X_i\right) \cdot \mu_H\left(\bigcap_{i=1}^{N} Y_i\right) = \prod_{i=1}^{N} \mu_G\left(X_i\right) \cdot \prod_{i=1}^{N} \mu_H\left(Y_i\right) =\\ &= \prod_{i=1}^{N} \mu_G(X_i) \cdot \mu_H(Y_i) = \prod_{i=1}^{N} \mu(X_i \times Y_i)\end{aligned}$$

Thus the family $\{X_i \times Y_i\}$ is independence. $\square$

Corollary 3.2.3. *For each $i \in \mathbb{N}$ let $K \subseteq N \subseteq M_i$ ce a tower of finite Galois extensions over K with Galois groups $G, G \ltimes I$ respectively. Let $c_1, c_2 \in I$. For $i \in \mathbb{N}$ let G_i, c_{i1}, c_{i2} be the images of G, c_1, c_2 under the isomorphism $G \ltimes I \to \mathrm{Gal}(M_i/K)$. If $\{M_i\}$ is linearly disjoint over N, then for almost every $\boldsymbol{\sigma} = (\sigma_1, \sigma_2) \in \mathrm{Gal}(K)^2$, there are infinitely many i's with $\mathrm{res}_{M_i}(\sigma_1, \sigma_2) \in (G_i c_{i1}, G_i c_{i2})$.*

Proof. We apply lemma 3.2.1 to the sets

$$X_i = \{\sigma \in \mathrm{Gal}(K) \mid \sigma|_{M_i} \in G_i c_{i1}\}, \quad Y_i = \{\sigma \in \mathrm{Gal}(K) \mid \sigma|_{M_i} \in G_i c_{i2}\}.$$

The conditions of the lemma fulfill and thus $\{X_i\}, \{Y_j\}$ are independence families with respect to the Haar measure of $\mathrm{Gal}(K)$. We conclude (lemma 3.2.2) that $\{X_i \times Y_i\}$ are independence family with respect to the product measure.

Since $\mu(X_i) = \mu(Y_i) = \frac{1}{\#I} > 0$ follows

$$(\mu \times \mu)(X_i \times Y_i) = \mu(X_i) \cdot \mu(Y_i) = \frac{1}{(\#I)^2},$$

and thus $\sum_{i=1}^{\infty} (\mu \times \mu)(X_i \times Y_i) = \infty$. Using Borel-Cantelli's lemma [FrJ, Lemma 18.3.5] yields $(\mu \times \mu)(\bigcap_{N=1}^{\infty} \bigcup_{i=N}^{\infty} (X_i \times Y_i)) = 1$. $\square$

3.3 Unbounded profinite groups

An abelian profinite group A is called **bounded** if the set $\{\mathrm{ord}(a) \mid a \in A\} \subseteq \mathbb{N}$ is bounded [Ro, Page 104], otherwise we call A **unbounded**.

[Ra, Lemma 3.2] says that if an abelian profinite group A is unbounded, then $\mu\{a \in A \mid \mathrm{ord}(a) = \infty\} = 1$. This motivates us to generalize the definition of unbounded profinite groups:

Definition 3.3.1. Let A be a profinite group. We say that A is **unbounded** if $\mu(\{a \in A \mid \mathrm{ord}(a) = \infty\}) = 1$.

Proposition 3.3.2. *let A be a profinite group. Then the following are equivalent:*

a. A is unbounded.

b. $\mu(\{a \in A \mid \mathrm{ord}(a) \geq m\}) = 1$ for each $m \in \mathbb{N}$.

c. *For each* $\varepsilon > 0$, $m \in \mathbb{N}$ *there exist a normal subgroup* N *of* A *with* $\mu(\{a \in A \mid \mathrm{ord}_N(a) \geq m\}) \geq 1 - \varepsilon$. *Here* $\mathrm{ord}_N(a)$ *is the order of* aN *in the group* A/N.

Proof. Put $X_\infty = \{a \in A \mid \mathrm{ord}(a) = \infty\}$, $X_m = \{a \in A \mid \mathrm{ord}(a) \geq m\}$, $X_m(N) = \{a \in A \mid \mathrm{ord}_N(a) \geq m\}$. The set X_m is open for each $m \in \mathbb{N}$, since if $\mathrm{ord}(y) \geq m$, then there exist an open normal subgroup N of A with $\mathrm{ord}_N(y) \geq m$, and thus $yN \subseteq X_m$.

$1 \Leftrightarrow 2$ This part follows immediately from $X_\infty = \bigcap_{m=1}^{\infty} X_m$.

$2 \Leftarrow 3$ $X_m(N) \subseteq X_m$ for every $N \triangleleft A$. Thus for every $\varepsilon > 0$ we can find open normal subgroup N of A with $\mu(X_m) \geq \mu(X_m(N)) \geq 1-\varepsilon$. Thus $\mu(X_m) = 1$.

$3 \Leftarrow 2$ Let $\varepsilon > 0$, $m \in \mathbb{N}$. The Haar measure is regular and $\mu(X_m) = 1$, thus there exist closed (and thus compact) $K \subseteq X_m$ such that $\mu(K) \geq 1-\varepsilon$. The set X_m is open, hence for each $y \in K$ we can find open norma subgroup N_y of A satisfying $yN_y \subseteq X_m$. From the compactness of K we can choose from the open covering $K \subseteq \bigcup_{y \in K} yN_y$ a finite sub covering, say $y_1N_1, \ldots, y_rN_r$. Put

$$N = N_1 \cap N_2 \cap \cdots \cap N_r.$$

It enough to show that $K \subseteq X_m(N)$. Indeed, if $y \in K$, then $y \in y_iN_i$ for some $1 \leq i \leq r$. Thus, $\mathrm{ord}_{N_i}(y) \geq m$ and in particular $\mathrm{ord}_N(y) \geq \mathrm{ord}_{N_i}(y) \geq m$ (proposition 2.1.2f).

□

4 Applications

In this section we prove Razon's Theorem using twisted wreath products and measure theory.

4.1 Notations

Definition 4.1.1. Let K be a field and let M be a Galois extension of K. We call M/K **unbounded** if $\mathrm{Gal}\,(M/K)$ is unbounded.

Let K be a countable Hilbertian field with absolute Galois group G and let M/K be an unbounded abelian extension of K. Let $e \geq 2$ be an integer. We denote μ, μ_e the Haar measures of $\mathcal{G}$, $\mathcal{G}^e$ respectively.

4.2 One polynomial

Let $f(T, X)$ be an absolutely irreducible polynomial. We woulde like to show that for almost every $\boldsymbol{\sigma}$ we can find infinitely many a's such that $f(a, X)$ remains irreducible over $MK_s(\boldsymbol{\sigma})$ and even over $K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$. For this section we *do not* assume that K is countable.

For the main ingredient we need the following fields theoretic lemma.

Lemma 4.2.1. *Let M/K be an abelian extension and let K_0/K be a Galois extension of degree n_0. Put $G = \mathrm{Gal}\,(MK_0/K)$. Then $\beta^{n_0} \in \mathrm{Z}(G)$ for all $\beta \in G$.*

Proof. By Galois theory $G \leq \mathrm{Gal}\,(M/K) \times \mathrm{Gal}\,(K_0/K)$. Write $\beta = (x, y)$ where $x \in \mathrm{Gal}\,(M/K)$, $y \in \mathrm{Gal}\,(K_0/K)$. Thus, $\beta^{n_0} = (x^{n_0}, y^{n_0}) = (x^{n_0}, 1)$. Since $\mathrm{Gal}\,(M/K)$ is abelian, we conclude that $\beta^{n_0} \in \mathrm{Z}(G)$. ∎

Lemma 4.2.2. *Let K be a Hilbertian field, $v_1, v_2 \in K_s$ and $f(T, X) \in K(v_1)[T, X]$ an absolutely irreducible polynomial, monic in X and Galois over $K(v_1, v_2)(T)$. Let $\varepsilon > 0$. Then $\exists \Upsilon \subseteq \mathcal{G}^2$ with $\mu_2(\Upsilon) \geq 1 - \varepsilon$ such that every $\boldsymbol{\sigma} \in \Upsilon$ satisfy:*
(*) If $v_1 \in K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$, then for infinitely many $a \in M(v_1)$, $f(a, X)$ is irreducible over $K_{\mathrm{ab}}(v_1, v_2)K_s(\boldsymbol{\sigma})$.

Proof. Let $A = \mathrm{Gal}\,(f, K_s(T))$ and $n = \mathrm{rank} A$. let K_0 be a finite Galois extension of K containing $K(v_1, v_2)$. Set $n_0 = [K_0 : K]$. Let $m \geq 2nn_0$.
Part A: Construction of Υ.
Step 1: Construction of G and G'. The extension M/K is unbounded (Definition 3.3.1). Hence, there exist a finite extension M_0 of K contained in M satisfying $\mu(\{\sigma \in \mathcal{G} \mid \mathrm{ord}_{M_0}(\sigma) \geq m\}) \geq 1 - \varepsilon$ (Proposition 3.3.2). Set $K' = M_0(v_1)$ and $L = M_0K_0$. Then L/K is finite Galois extension. Put $G = \mathrm{Gal}\,(L/K)$ and $G' = \mathrm{Gal}\,(L/K')$. then G' acts on $A \cong \mathrm{Gal}\,(f, L(T))$.

$$\begin{tikzcd} M_0 \arrow[r, dash] \arrow[d, dash] & K' \arrow[r, dash, "G'"] \arrow[d, dash] & L \arrow[d, dash] \\ K \arrow[r, dash] \arrow[urr, dotted, dash, "G"] & K(v_1) \arrow[r, dash] & K_0 \end{tikzcd}$$

Let $\Sigma_1' = \{\sigma \in \mathcal{G} \mid \mathrm{ord}_{K'}(\sigma) \geq m\}$ (see definition 2.3.1). $\mathrm{ord}_{K'}(\sigma) \geq m$ whenever $\mathrm{ord}_{M_0}(\sigma) \geq m$ (proposition 2.3.2). Thus

$$\mu(\Sigma_1') \geq 1 - \varepsilon \tag{1}$$

Step 2: realization of $A \,\mathrm{wr}_{G'}\, G$ over K. The polynomial $f(T, X)$ is defined over K' and Galois over $L(T)$. Let $d_1, \dots, d_r$ be a Basis of K' over K and let $\boldsymbol{t} = (t_1, \dots, t_r)$ be a set of algebraically independent intermediates. By [FrJ, Lemma 13.8.1] there exists $F^*, \hat{F}^*$ satisfying

(a) $K(\boldsymbol{t}), K'(\boldsymbol{t}), L(\boldsymbol{t}), F^*, \hat{F}^*$ realize $A \,\mathrm{wr}_{G'}\, G$ and $\hat{F}^*$ is regular over L,

(b) $F^* = L(\boldsymbol{t})(z)$ and $\mathrm{irr}(z, L(\boldsymbol{t})) = f\left(\sum_{i=1}^{r} d_i t_i, Z\right) \in K'[\boldsymbol{t}, Z]$.

The extension $\hat{F}^*$ is regular over L and K is a Hilbertian field. In similar construction as in [FrJ, Lemma 16.2.6], we can find infinite many specializations $\boldsymbol{t} \mapsto \boldsymbol{b}_i$, $\boldsymbol{b}_i = (b_{1i}, \dots, b_{ri}) \in K^r$, which extends to L-places, $\varphi_i\colon \hat{F}^* \to \hat{F}_i \cup \{\infty\}$, such that $\mathrm{Gal}\left(\hat{F}_i/K\right) \cong A \,\mathrm{wr}_{G'}\, G$ and $\hat{F}_i$ linearly disjoint over L. Moreover, we can choose $\boldsymbol{b}_i \in K^r$ such that φ_i maps $K(\boldsymbol{t})$, $K'(\boldsymbol{t})$ and $L(\boldsymbol{t})$ onto $K(\boldsymbol{b}_i) \cup \{\infty\} = K \cup \{\infty\}$, $K'(\boldsymbol{b}_i) \cup \{\infty\} = K' \cup \{\infty\}$, $L(\boldsymbol{b}_i) \cup \{\infty\} = L \cup \{\infty\}$, respectively, $i = 1, 2, \dots$ (see [FrJ, Lemma 2.2.7]).

If we write $c_i = \sum_j d_j b_{ji} \in K'$ and $x_i = \varphi_i(z)$, then x_i is a root $f(c_i, X)$, and the image F_i of F^* under φ_i satisfy $F_i = L(x_i)$. $d_1 \neq d_r$ are linearly independent over K and $\boldsymbol{b}_i \in K^r$. Thus, distinct specializations $\boldsymbol{t} \mapsto \boldsymbol{b}_i$ give distinct elements c_i.

$$\begin{tikzcd}
\hat{F}^* \arrow[r, dotted, "\varphi_i"] \arrow[d, dash] & \hat{F}_i \arrow[d, dash] \\
F^* = L(\boldsymbol{t})(z) \arrow[r, dotted] \arrow[d, dash] & F_i = L(x_i) \arrow[d, dash] \\
L(\boldsymbol{t}) \arrow[r, dotted] \arrow[d, dash] & L \arrow[d, dash] \\
K'(\boldsymbol{t}) \arrow[r, dotted] \arrow[d, dash] & K' \arrow[d, dash] \\
K(\boldsymbol{t}) \arrow[r, dotted, "\mathbf{t}\mapsto\mathbf{b}_i"] & K
\end{tikzcd}$$

Step 3: Construction of Υ. Recall that $G \le A \operatorname{wr}_{G'} G$. For all $\tau \in A \operatorname{wr}_{G'} G$ we denote by G_i, τ_i the images of G, τ under the isomorphism which maps $A \operatorname{wr}_{G'} G$ onto $\mathrm{Gal}\left(\hat{F}_i/K\right)$.

Fix $\beta \in \mathrm{Gal}(L/K)$ with $\mathrm{ord}_{K'}(\beta) \ge m$. $\beta^{n_0} \in \mathrm{Z}(G)$ (Lemma 4.2.1). Applying Lemma 2.3.7 with $M = K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ we get $\zeta \in \mathrm{Ind}_{G'}^{G}(A)$ (ζ is dependent on β) such that for every $\sigma_1, \sigma_2 \in \mathcal{G}$, $\sigma_1|_{\hat{F}_i} = \beta_i$, $\sigma_2|_{\hat{F}_i} \in G_i\zeta_i$: if $v_1 \in K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$, then

$$[F_iK_{\mathrm{ab}}K_s(\boldsymbol{\sigma}) : LK_{\mathrm{ab}}K_s(\boldsymbol{\sigma})] = [F_i : L]. \tag{2}$$

Let

$$\Sigma_{12}(\beta) = \{(\sigma_1, \sigma_2) \in \mathcal{G}^2 \mid \text{For infinitely many} i\text{'s } \mathrm{res}_{\hat{F}_i}(\sigma_1, \sigma_2) \in G_i \times G_i\zeta_i\}.$$

Then $\mu_2(\Sigma_{12}(\beta)) = 1$ (Corollary 3.2.3).

Decompose Σ_1' to left cosets of $\mathrm{Gal}(L)$, i.e.,

$$\Sigma_1' = \dot{\bigcup_{\substack{\beta\in\mathrm{Gal}(L/K)\\ \mathrm{ord}_{K'}(\beta)\ge m}}} \Sigma_1(\beta),$$

where $\Sigma_1(\beta) = \{\sigma \in \mathcal{G} \mid \sigma|_L = \beta\}$. Finally define

$$\Upsilon = \dot{\bigcup_{\substack{\beta\in\mathrm{Gal}(L/K)\\ \mathrm{ord}_{K'}(\beta)\ge m}}} (\Sigma_1(\beta) \times \mathcal{G}) \cap \Sigma_{12}(\beta).$$

More explicitly, $(\sigma_1, \sigma_2) \in \Upsilon$ is and only if $\mathrm{ord}_{K'}(\sigma_1) \ge m$ and for infinitely many i's $\sigma_1|_{\hat{F}_i} \in G_i$, $\sigma_2|_{\hat{F}_i} \in G_i\zeta_i$ where ζ_i is suitable for β. Since $\mu_2(\Sigma_{12}(\beta)) = 1$,

$$\begin{aligned} \mu_2(\Upsilon) &= \sum_{\beta} \mu_2\left((\Sigma_1(\beta) \times \mathcal{G}) \cap \Sigma_{12}(\beta)\right) \\ &= \sum_{\beta} \mu\left(\Sigma_1(\beta)\right) = \mu(\Sigma_1') \overset{(1)}{\ge} 1 - \varepsilon \end{aligned}$$

Part B: Every $\boldsymbol{\sigma} \in \Upsilon$ satisfy condition (*).

Let $\boldsymbol{\sigma} \in \Upsilon$. Put $N = K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ and assume $v_1 \in N$. Let $i \in \mathbb{N}$ with $\mathrm{res}_{\hat{F}_i}(\sigma_1, \sigma_2) \in G_i \times G_i\zeta_i$. By equation (2), $[F_iN : LN] = [F_i :$

$L] = \deg f(c_i, X)$. Since $F_i = L(x_i)$, $F_iN = LN(x_i)$. $f(c_i, x_i) = 0$ thus, $f(c_i, X) = \mathrm{irr}(x_i, LN)$. We conclude that $f(c_i, X)$ is irreducible over LN and thus irreducible over $K_{\mathrm{ab}}(v_2)K_s(\boldsymbol{\sigma})$. Since we found infinitely many i's satisfying this, there are infinitely many $c \in K' \subseteq M(v_1)$ such that $f(c, X)$ is irreducible over $K_{\mathrm{ab}}(v_2)K_s(\boldsymbol{\sigma})$. ☐

Lemma 4.2.3. *Let K be hilbertian field, $e \geq 2$ and $v_1, v_2 \in K_s$. Let $f(T, X) \in K(v_1)[T, X]$ be an absolutely irreducible polynomial, monic in X and Galois over $K(v_1, v_2)(T)$. Then condition (*) fulfill for almost every $\boldsymbol{\sigma} \in \mathcal{G}^e$.*

Proof. We start the proof with the case $e = 2$. In the previous lemma we construct $\Upsilon_\varepsilon \subseteq \mathcal{G}^2$ for every $\varepsilon > 0$ such that $\mu_2(\Upsilon) \geq 1 - \varepsilon$, and (*) fulfill for every $\boldsymbol{\sigma} = (\sigma_1, \sigma_2) \in \Upsilon$. Thus, $\Sigma = \bigcup_{n \in \mathbb{N}} \Upsilon_{\frac{1}{n}}$ is measurable and has measure 1.

For $e > 2$ Take $\Sigma' = \Sigma \times \overbrace{\mathcal{G} \times \cdots \times \mathcal{G}}^{e-2 \text{ times}}$ where Σ is the above set. Σ' is a subset of $\mathcal{G}^e$ with $\mu(\Sigma') = 1$. Let $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \Sigma'$. If $v_1 \in K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$, then $v_1 \in K_{\mathrm{ab}}K_s(\sigma_1, \sigma_2)$. Thus there are infinitely many $a \in M(v_1)$ such that $f(a, X)$ is irreducible over $K_{\mathrm{ab}}(v_2)K_s(\sigma_1, \sigma_2)$. Hence, $f(a, X)$ is also irreducible over the subfield $K_{\mathrm{ab}}(v_1, v_2)K_s(\boldsymbol{\sigma})$ of $K_{\mathrm{ab}}(v_1, v_2)K_s(\sigma_1, \sigma_2)$. ☐

4.3 Main Theorem

Firstly, we formulate criterion for Hilbertianity of sub extensions.

Lemma 4.3.1. *Let P/M be a separable algebraic extension of fields. If for every M' finite sub extension of P/M for every finite Galois extension P'/P and for every absolutely irreducible polynomial $f \in M'[T, X]$, monic in X and Galois over $P'(T)$, there exists infinitely many $a \in M'$ such that $f(a, X)$ is irreducible over P', then every sub extension of P/M is Hilbertian.*

Proof. Let Q be sub extension of P/M. In order to prove that Q is Hilbertian we use the criterion [FrJ, Lemma 13.1.4], i.e. for every $f \in Q[T, X]$ absolutely irreducible polynomial, monic in X and for every finite Galois extension Q' of Q such that $f(T, X)$ is Galois over $Q'(T)$, there are infinitely many $a \in Q$ such that $f(a, X)$ irreducible over Q'. Let f, Q and Q' as above. Let $M' \subseteq Q$ finite extension of M such that f defined over M'. Put $P' = PQ'$. Then by the assumption of the lemma there are infinitely many $a \in M' \subseteq P$ such that $f(a, X)$ is irreducible over P' and thus $f(a, X)$ irreducible over Q'. ☐

Theorem 4.3.2. *Let $e \geq 2$, K be a countable Hilbertian field and M/K be an unbounded abelian extension. Then every sub extension of $K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})/M$ is Hilbertian for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.*

Proof. For every $f \in K_s[T, X]$ absolutely irreducible polynomial monic in X and for every $v_1, v_2 \in K_s$ such that f defined over $K(v_1)$ and Galois over $K(v_1, v_2)(T)$, define $\Sigma(f, v_1, v_2)$ be the set of $\boldsymbol{\sigma}$'s from Lemma 4.2.3. Define

$$\Sigma = \bigcap_{f, v_1, v_2} \Sigma(f, v_1, v_2),$$

Since $\mu(\Sigma(f, v_1, v_2)) = 1$ and there are only countable many triples follows that $\mu(\Sigma) = 1$.

Let $\boldsymbol{\sigma} \in \Sigma$. Put $P = K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ and apply Lemma 4.3.1. Let $f \in P[T, X]$ be an absolutely irreducible polynomial, monic in X, and let P'/P be finite Galois extension where f is Galois over $P'(T)$. Let M' be sub extension of P/M such that f defined over M'. Choose $v_1 \in M'$ such that $f \in K(v_1)[T, X]$.

Let $v_2 \in K_s$ such that $P' \subseteq P(v_2)$ and f is Galois over $K(v_1, v_2)(T)$. Since $\boldsymbol{\sigma} \in \Sigma(f, v_1, v_2)$, by Lemma 4.2.3 there are infinitely many $a \in M(v_1)$, and thus $a \in M'$, such that $f(a, X) \in P[X]$ is irreducible over $P(v_2)$ and thus over P'. $\square$

The proof of Razon's Theorem in this way naturally leads to the question whether one can replace the abelian unbounded extension with other extensions.

We formulate two conjectures with resemblance to Haran's Diamond Theorem.

Conjecture 4.3.3. *Let M_1, M_2 be two Galois extensions of Hilbertian countable field K and Let $e \geq 2$. If M_1M_2/M_i is unbounded $(i = 1, 2)$, then for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ every field between $M_1M_2K_s(\boldsymbol{\sigma})$ and M_1M_2 is Hilbertian.*

Or maybe more general form:
We can generalize definition 4.1.1 in the following way: an extension M of K is called **unbounded** if $\mu\{\sigma \in \mathrm{Gal}(K) \,|\mathrm{ord}_M \sigma = \infty\} = 1$.

Conjecture 4.3.4. *Let M_1, M_2 be Galois extensions of Hilbertian countable field K. Let $e \geq 2$. Let M be an extension of K such that $M \subseteq M_1M_2$ and $M/M \cap M_i$ is unbounded $(i = 1, 2)$. Then for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ every field between $MK_s(\boldsymbol{\sigma})$ and M is Hilbertian.*

References

[FrJ] M. Fried, M. Jarden, Field Arithmetic, Second Edition. Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2004

[Ha] D. Haran, Hilbertian fields under seprable algebraic extensions. Inventiones mathematicae **137**, 85-112 (1999)

[JL] M. Jarden, A. Lubotzky, Hilbertian fields and free profinite groups. J. London Math. Soc. **46**, 205-227 (1992)

[JR] M. Jarden, A. Razon, Pseudo Algebriacally closed field over rings. Israel Journal of Mathematics **86**, 25-59 (1994)

[La] S. Lang, Algebra 3rd-edition. Addison-Wesley, Reading, 1993 Algebra, third edition, Addison-Wesley, Reading, (1994)

[Ra] A. Razon, Abundance of Hilbertian domains, manuscripta math. **94**, 531-542 (1997)

[Ro] Robinson, D. : A course in the theory of groups. Graduate texts in mathematics **80**, Springer, New York, (1982)