TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 358, Number 6, Pages 2561–2577
S 0002-9947(05)03776-1
Article electronically published on September 22, 2005

A GENERALIZATION OF MARSHALL'S EQUIVALENCE RELATION

IDO EFRAT

ABSTRACT. For p prime and for a field F containing a root of unity of order p, we generalize Marshall's equivalence relation on orderings to arbitrary subgroups of $F^\times$ of index p. The equivalence classes then correspond to free pro-p factors of the maximal pro-p Galois group of F. We generalize to this setting results of Jacob on the maximal pro-2 Galois group of a Pythagorean field.

1. Introduction

Let p be a prime number and let F be a field of characteristic $\neq p$. We denote the compositum of all finite Galois p-extensions of F by $F(p)$, and let $G_F(p) = \mathrm{Gal}(F(p)/F)$ be the maximal pro-p Galois group of F. One of the rare cases where the group-theoretic structure of $G_F(p)$ is completely understood is when $p = 2$, F is a Pythagorean field, and $G_F(2)$ is finitely generated (as a pro-2 group). Here F is called **Pythagorean** if every sum of squares in F is already a square. This is by striking results of Bill Jacob [J], which are based on a decomposition theory for the so-called **spaces of orderings**, due to Murray Marshall [Ma1]. These spaces are an abstract setting in which one can develop most of the theory of quadratic forms over Pythagorean fields in a formal way (see [Ma3] for details). In the concrete case of spaces of orderings of Pythagorean fields, results equivalent to Marshall's were obtained by Craven in [C1] and [C2].

In what follows, an **ordering** on a field F will be an additively closed subgroup P of the multiplicative group $F^\times$ of F such that $F^\times = P \cup -P$. We denote the set of all orderings on F by X_F. Call $P_1, P_2 \in X_F$ **equivalent** if either $P_1 = P_2$, or there exist $P_3, P_4 \in X_F$ such that the orderings P_1, P_2, P_3, P_4 are distinct, and the intersection of any three of them equals the intersection of all four (such a system is called a **4-fan**). Marshall proves that this is indeed an equivalence relation on X_F (see [Ma1, Th. 2.3] and [Ma3, Th. 4.6.1(2)] for proofs in the more general case of abstract spaces of orderings, and [Mer, §4] for a proof in the concrete case of fields). As in [E1] we call this relation **Marshall-equivalence**.

Now suppose that F is Pythagorean and that $G_F(2)$ is finitely generated (or what amounts to the same thing, X_F is finite). To any Marshall-equivalence class C in X_F we associate a **closure** $F \subseteq \hat{F} \subseteq F(2)$ as follows: When C consists of a single ordering P we take $\hat{F}$ to be a Euclidean closure of F at P, i.e., a relative real closure of (F, P) inside $F(2)$. When $1 < |C|$ there exists a valuation v on F

Received by the editors September 27, 2003 and, in revised form, June 20, 2004.
2000 *Mathematics Subject Classification.* Primary 12E30; Secondary 12J15, 19C99, 12J99.
This research was supported by the Israel Science Foundation grant No. 8008/02–1.

with non-2-divisible value group, such that C consists of all orderings containing the 1-units of v (see [J]; this is also a consequence of Bröcker's "trivialization of fans" theorem [Br]). We then take $\hat{F}$ to be a decomposition field of v inside $F(2)$.

The Jacob–Marshall theory shows that for F as above, the partition of X_F into equivalence classes corresponds to a decomposition of $G_F(2)$ as a free product in the category of pro-2 groups as follows (see also [Mi], [EH, §3] and [E1]):

(1) if $\hat{F}$ is a closure of F at an equivalence class C, then $G_{\hat{F}}(2)$ cannot be decomposed as a free pro-2 product in a nontrivial way;

(2) there exist closures $\hat{F}_1, \ldots, \hat{F}_n$ of F at the distinct equivalence classes $C_1, \ldots, C_n$, respectively, of X_F such that $G_F(2) = G_{\hat{F}_1}(2) *_2 \cdots *_2 G_{\hat{F}_n}(2)$ (where $*_2$ denotes free pro-2 product);

(3) if $H_1, \ldots, H_n$ are closed subgroups of $G_F(2)$ such that $G_F(2) = H_1 *_2 \cdots *_2 H_n$, then each H_i is generated by subgroups of the form $G_{\hat{F}}(2)$, where $\hat{F}$ is a closure of F at some Marshall-equivalence class;

(4) if C is a Marshall-equivalence class in X_F with closure $\hat{F}$, then C is the image of the restriction map $X_{\hat{F}} \to X_F$, $\hat{P} \mapsto F \cap \hat{P}$.

Now the structure of the free pro-2 factors in (2) is known; namely, when $|C_i| = 1$, $G_{\hat{F}_i}(2) \cong \mathbb{Z}/2$ [B]. When $|C_i| > 1$, the valuation yielding $\hat{F}_i$ has a real Pythagorean residue field $\bar{F}_i$. In particular char $\bar{F}_i = 0$. By the Galois theory of tame valued fields, $G_{\hat{F}_i}(2) \cong \mathbb{Z}_2^m \rtimes G_{\bar{F}_i}(2)$ for $m = \dim_{\mathbb{F}_2}(v(F^\times)/2v(F^\times))$, where the action of $G_{\bar{F}_i}(2)$ on $\mathbb{Z}_2^m$ is given by multiplication by the cyclotomic character (see §3(A) for details). Since $G_{\bar{F}_i}(2)$ is generated by fewer elements than $G_{\hat{F}_i}(2)$, we inductively obtain in this way a complete *group-theoretic* description of $G_F(2)$, as mentioned above.

In this paper we generalize Marshall's equivalence relation from the case of orderings on Pythagorean fields to the case of arbitrary subgroups of $F^\times$ of index p, where F is an arbitrary field of characteristic $\neq p$ containing the pth roots of unity (of course, an ordering has index 2 in $F^\times$). We then prove generalizations of (1), (3) and (4) to our generalized equivalence relation and the pro-p group $G_F(p)$ (Theorem 6.4, Theorem 6.6, and Proposition 5.8, respectively).

The expected generalization of (2) is an arithmetic variant of the so-called *"elementary type conjecture"*. This conjecture was introduced in [Ma2] in the context of abstract Witt rings. It predicts that if such a ring is finitely generated, then it can be built-up in finitely many steps from the Witt rings of $\mathbb{C}$, $\mathbb{R}$, finite fields of characteristic $\neq 2$, and dyadic fields, using two natural algebraic constructions, called "direct sum" and "extension". The conjecture has been proved in many cases in the numerous works of Berman, Carson, Cordes, Craven, Fitzgerald, Kula, Marshall, Szczepanik, Szymiczek, Yucas and others (see the survey [Ma4] for more details and for references). Jacob and Ware ([JWr1], [JWr2]) translated this conjecture to the context of finitely generated maximal pro-2 Galois groups of fields and free pro-2 products. It was then generalized in [E2] (see also [E4, Question 4.8] and [HwJ, Remark 2.14]) to maximal pro-p Galois groups of fields (containing a primitive pth root of unity) and free pro-p products, where p is any prime number. In its "arithmetic" form, the conjecture then says that if $G_F(p)$ is finitely generated, then it is a free pro-p product of subgroups which are isomorphic to $\mathbb{Z}_p$, $\mathbb{Z}/2$ (when $p = 2$), or are decomposition groups of valuations with nontrivial inertia group. This is known for several important families of fields – among them, global fields ([E4], [E6]) and fields of transcendence degree ≤ 1 over a local field ([JP], [E7]). In

Theorem 7.4 we show that for these and several other families of fields, the natural generalization of (2) holds.

Our approach uses valuation-theoretic techniques, which are reviewed in §2. The analysis is based on the description of finitely generated groups $G_F(p)$ for F p-Henselian with residue characteristic p, as obtained in [E5], and on the indecomposability results of [E3] (which in turn are based on the pro-p version of the Kurosh subgroup theorem, as in [H] and [Mel]).

2. Valuations

Let v be a (Krull) valuation on F. We denote the valuation ring, maximal ideal, residue field, and unit group of v by O_v, $\mathfrak{m}_v$, $\bar{F}_v$, $O_v^\times$, respectively. We set $G_v = 1+\mathfrak{m}_v$, and let $\pi_v\colon O_v^\times \to \bar{F}_v^\times$ be the canonical group epimorphism with kernel G_v. One says that v is **trivial** if $F = O_v$. The valuation v induces a topology on F with a basis consisting of all sets $a + b\mathfrak{m}_v$, where $a, b \in F$ and $b \neq 0$.

Next let S be a subgroup of $F^\times$ and let $\bar{S}_v = \pi_v(S \cap O_v^\times)$ be its **push-down** to $\bar{F}_v$. Then v and π_v induce short exact sequences:

$$1 \to O_v^\times/(S \cap O_v^\times) \to F^\times/S \to v(F^\times)/v(S) \to 0 \quad ,$$

$$1 \to G_v/(S \cap G_v) \to O_v^\times/(S \cap O_v^\times) \to \bar{F}_v^\times/\bar{S}_v \to 1 \quad . \tag{2.1}$$

In particular, for $S = (F^\times)^p G_v$ we have $v(S) = pv(F^\times)$ and $\bar{S}_v = (\bar{F}_v^\times)^p$, so (2.1) combine to the following short exact sequence:

$$1 \to \bar{F}_v^\times/(\bar{F}_v^\times)^p \to F^\times/(F^\times)^p G_v \to v(F^\times)/p \to 0 \quad . \tag{2.2}$$

Given valuations v and u on F, we say that v is **finer** than u (and that u is **coarser** than v) if $G_u \leq G_v$. This is equivalent to any of the conditions $\mathfrak{m}_u \subseteq \mathfrak{m}_v$ and $O_u \supseteq O_v$. Then $O_v/\mathfrak{m}_u$ is a valuation ring on $\bar{F}_u$. We denote the corresponding valuation by v/u. One has $\bar{F}_v \cong (\overline{F_u})_{v/u}$, $\pi_u(G_v) = G_{v/u}$, and $\pi_u(O_v^\times) = O_{v/u}^\times$. Also, there is a short exact sequence of ordered abelian groups [Bo, Ch. VI, §4.3]

$$0 \to (v/u)(\bar{F}_u^\times) \to v(F^\times) \to u(F^\times) \to 0 \quad ,$$

which induces an exact sequence of abelian groups

$$0 \to ((v/u)(\bar{F}_u^\times))/p \to v(F^\times)/p \to u(F^\times)/p \to 0 \quad . \tag{2.3}$$

Finally, it is straightforward to verify that the homomorphism $\pi_u\colon O_u^\times \to \bar{F}_u^\times$ is continuous with respect to the v-topology on $O_u^\times$ and the v/u-topology on $\bar{F}_u^\times$.

A nontrivial valuation has **rank** 1 if it has no nontrivial coarsenings. Any collection of valuations v_i, $i \in I$, has a finest common coarsening u; namely, O_u is generated as a ring by O_{v_i}, $i \in I$. We say that valuations v and u on F are **comparable** if one of them is coarser than the other. We recall [Bo, Ch. VI, §4.1, Cor.]:

Proposition 2.1. *Let v_1, v_2, u be valuations on the field F, with v_1, v_2 coarser than u. Then v_1, v_2 are comparable.*

Valuations v_1 and v_2 on F are **independent** if their finest common coarsening is trivial. When v_1, v_2 are nontrivial valuations they are independent if and only if the following *weak approximation property* holds: The intersection of any two nonempty sets U_1, U_2 which are open in the v_1-topology and the v_2-topology, respectively, is nonempty (see e.g. [Bo, Ch. VI, §7.2, Th. 1]).

Lemma 2.2. *Let v_1 and v_2 be independent nontrivial valuations on the field F. For $i = 1, 2$ let U_i be a v_i-open subgroup of $F^\times$. Then $F^\times = U_1 \cdot U_2$.*

Proof. Given $a \in F^\times$, the weak approximation property yields $b \in U_1 \cap aU_2$. Then $a = b \cdot ab^{-1} \in U_1 \cdot U_2$. □

Corollary 2.3. *Let v_1, v_2 be incomparable valuations on the field F and let u be their finest common coarsening. Let U_1, U_2 be subgroups of $O_u^\times$ such that $\pi_u(U_i)$ is v_i/u-open in $\bar{F}_u^\times$, $i = 1, 2$. Then $O_u^\times = G_u U_1 U_2$.*

Proof. The map $v \mapsto v/u$ is an order-preserving bijection between the partially ordered set of all valuations v on F finer than u and the partially ordered set of all valuations on $\bar{F}_u$ (with respect to the coarsening relation; see [Bo, Ch. VI, §4.1, Prop. 2]). Hence the valuations $v_1/u, v_2/u$ on $\bar{F}_u$ are independent and nontrivial. By Lemma 2.2, $\bar{F}_u^\times = \pi_u(U_1) \cdot \pi_u(U_2) = \pi_u(U_1 U_2)$. The assertion now follows by taking inverse images with respect to π_u and recalling that $G_u = \mathrm{Ker}(\pi_u)$. □

We say that a valuation v on the field F is **almost p-adic** if $\bar{F}_v$ is a finite field of characteristic p and there is a coarsening v' of v such that $\mathrm{char}\, \bar{F}_{v'} = 0$ and such that the value group of v/v' is $\mathbb{Z}$. In particular, v/v' has rank 1, so there is no valuation on F which is strictly coarser than v and strictly finer than v'. It therefore follows from Proposition 2.1 that every proper coarsening of v is coarser than v'. We call v' the **finest coarsening** of v. Also let $E = \bar{F}_{v'}$ and let E_1 be the completion of E with respect to v/v'. Being a complete discretely valued field of characteristic 0 and with finite residue field of characteristic p, E_1 is a finite extension of $\mathbb{Q}_p$. We set

$$G'_v = \pi_{v'}^{-1}(E^\times \cap (E_1)^p) \quad .$$

It is straightforward to verify the following facts:

Lemma 2.4. (a) *$G_{v'} \leq G'_v \leq O_{v'}^\times$;*
(b) *The push-down of $(F^\times)^p G'_v$ by v' to E is $E^\times \cap (E_1^\times)^p$.*

In addition to the case of almost p-adic valuations, we define the group G'_v for valuations v with $\mathrm{char}\, \bar{F}_v \neq p$ by simply setting

$$G'_v = G_v = 1 + \mathfrak{m}_v \quad .$$

Lemma 2.5. *Let v be a valuation on F such that either $\mathrm{char}\, \bar{F}_v \neq p$ or v is almost p-adic. Let u be a valuation on F which is strictly coarser than v. Then $\pi_u(G'_v)$ is v/u-open in $\bar{F}_u$.*

Proof. If $\mathrm{char}\, \bar{F}_v \neq p$, then $\pi_u(G'_v) = \pi_u(G_v) = G_{v/u}$ is clearly v/u-open.

Next suppose that v is almost p-adic. Let v', $E = \bar{F}_{v'}$, and E_1 be as above. As observed earlier, u must be coarser than v'. By Lemma 2.4(a), $G_{v'} \leq G'_v \leq O_{v'}^\times \leq O_u^\times$. It follows that $\pi_u(G'_v) \leq \pi_u(O_{v'}^\times) = O_{v'/u}^\times$. Hence $\pi_{v'/u}(\pi_u(G'_v))$ is well defined and equals $\pi_{v'}(G'_v)$. Furthermore, $\mathrm{Ker}(\pi_{v'/u}) = G_{v'/u} = \pi_u(G_{v'}) \leq \pi_u(G'_v)$, so we obtain

$$\pi_u(G'_v) = \pi_{v'/u}^{-1}(\pi_{v'}(G'_v)) = \pi_{v'/u}^{-1}(E^\times \cap (E_1^\times)^p) \quad .$$

Now by Hensel's lemma [FeV, Ch. II, (1.3)], the subgroup $E^\times \cap (E_1^\times)^p$ of $E^\times$ contains $1 + p^2 \mathfrak{m}_{v/v'}$. Hence it is v/v'-open in E. As we have observed, the map $\pi_{v'/u} \colon O_{v'/u}^\times \to E^\times$ is continuous with respect to the v/u-topology on $O_{v'/u}^\times$ and the v/v'-topology on $E^\times$. Consequently, $\pi_u(G'_v)$ is v/u-open in this case as well. □

3. p-Henselizations

From now on we assume that F is a field of characteristic $\neq p$ containing the pth roots of unity.

A valuation v on F is called **p-Henselian** if it has a unique prolongation to $F(p)$; equivalently, Hensel's lemma holds for polynomials of degree p (see e.g. [Br], [Wd] for this and the following well-known facts). When char $\bar{F}_v \neq p$, the valuation v is p-Henselian if and only if $G_v \leq (F^\times)^p$. A **p-Henselization** of F with respect to a valuation v is a decomposition field $(\hat{F}_v, \hat{v})$ of the valued field (F, v) in $F(p)$. Then $\hat{v}$ is p-Henselian, and has the same value group and residue field as v. If u is another valuation on F which is coarser than v, then v is p-Henselian if and only if both u and v/u are p-Henselian. Also, for any p-Henselizations $\hat{F}_u, \hat{F}_v$ of $(F, u), (F, v)$, respectively, there exists $\sigma \in G_F(p)$ such that $\sigma(\hat{F}_u) \subseteq \hat{F}_v$.

(A) *The tame case:* char $\bar{F}_v \neq p$.

Lemma 3.1. *Let v be a valuation on F with* char $\bar{F}_v \neq p$ *and let $(\hat{F}_v, \hat{v})$ be a p-Henselization of (F, v). Then $F^\times/(F^\times)^p G_v \cong \hat{F}_v^\times/(\hat{F}_v^\times)^p$ canonically.*

Proof. By Hensel's lemma $G_{\hat{v}} \leq (\hat{F}_v^\times)^p$. Also, the exact sequences (2.1) (for $\hat{v}$ and for the subgroup $S = F^\times$ of $\hat{F}_v^\times$) gives $\hat{F}_v^\times = F^\times G_{\hat{v}}$. It follows that $\hat{F}_v^\times = F^\times(\hat{F}_v^\times)^p$.

Next we note that $(F^\times)^p G_v \leq F^\times \cap (\hat{F}_v^\times)^p$. For the converse inclusion, let $a \in \hat{F}_v^\times$ satisfy $a^p \in F^\times$. Write $a = bc$, with $b \in F^\times$ and $c \in G_{\hat{v}}$. Then $c^p = a^p/b^p \in G_{\hat{v}} \cap F^\times = G_v$, so $a^p = b^p c^p \in (F^\times)^p G_v$. Consequently, $(F^\times)^p G_v = F^\times \cap (\hat{F}_v^\times)^p$, and we get the desired isomorphism. □

Let $F_{\rm nr}$ be a maximal nonramified extension of (F, v) inside $F(p)$. Thus $G_{F_{\rm nr}}(p) = \mathrm{Gal}(F(p)/F_{\rm nr})$ is an **inertia group** of (F, v) relative to $F(p)$. When (F, v) is p-Henselian, $F_{\rm nr}$ is uniquely determined, and hence so is the inertia group. When char $\bar{F}_v \neq p$ one has $G_{F_{\rm nr}}(p) \cong \mathbb{Z}_p^m$, where $m = \dim_{\mathbb{F}_p}(v(F^\times)/p)$; furthermore, $G_F(p) = G_{F_{\rm nr}}(p) \rtimes G_{\bar{F}_v}(p)$. Here $\sigma \in G_{\bar{F}_v}(p)$ acts on $\tau \in G_{F_{\rm nr}}(p)$ by $\tau^\sigma = \tau^\chi$, where χ is the pro-p cyclotomic character of σ, i.e., χ is the principal p-adic unit satisfying $\sigma(\zeta) = \zeta^\chi$ for all roots of unity ζ of p-power order (see e.g. [E3, Lemma 1.1]).

(B) *The wild case.* Next we analyze in detail the structure of p-Henselizations in the more delicate case of almost p-adic valuations.

Proposition 3.2. *Let v be an almost p-adic valuation on F. Let v' be the finest coarsening of v, let $E = \bar{F}_{v'}$, and let (E_1, w_1) be the completion of E with respect to $w = v/v'$ as before. Let $(\hat{F}_v, \hat{v})$ be a p-Henselization of (F, v). Then:*

(a) *$\hat{v}$ has a unique coarsening $\hat{v}'$ which extends v';*
(b) *$v', \hat{v}'$ have the same value group;*
(c) *the valuation $\hat{w} = \hat{v}/\hat{v}'$ on the residue field $\hat{E}$ of $(\hat{F}_v, \hat{v}')$ has the same value group, residue field, and completion as (E, w);*
(d) *$E_1(p) = E_1 \cdot E(p)$;*
(e) *$\hat{E} = E(p) \cap E_1$;*
(f) *$(\hat{E}^\times)^p = \hat{E}^\times \cap (E_1^\times)^p$;*
(g) *$E^\times/(E^\times \cap (E_1^\times)^p) \cong \hat{E}^\times/(\hat{E}^\times)^p \cong E_1^\times/(E_1^\times)^p$ canonically;*
(h) *$\dim_{\mathbb{F}_p}(F^\times/(F^\times)^p G_v') \geq 3$;*
(i) *the inertia group of v in $F(p)$ is nontrivial.*

Proof. (a) The existence of $\hat{v}'$ follows from the Cohen–Seidenberg theorem (see [Jr, Lemma 9.4]). The uniqueness follows from Proposition 2.1 and from the fact that distinct prolongations of a valuation to the same algebraic extension are necessarily incomparable [Jr, Cor. 6.6].

(b), (c) We have a commutative diagram of abelian groups with short exact rows

$$\begin{array}{ccccccccc} 0 & \to & w(E^\times) & \to & v(F^\times) & \to & v'(F^\times) & \to & 0 \\ & & \downarrow & & || & & \downarrow & & \\ 0 & \to & \hat{w}(\hat{E}^\times) & \to & \hat{v}(\hat{F}_v^\times) & \to & \hat{v}'(\hat{F}_v^\times) & \to & 0 \end{array} ,$$

where the right vertical map is an embedding. Hence all the vertical maps are equalities.

The residue field of (E, w) is $\bar{F}_v$, and the residue field of $(\hat{E}, \hat{w})$ is the same as the residue field of $(\hat{F}_v, \hat{v})$, which is also $\bar{F}_v$. Thus (E, w) and $(\hat{E}, \hat{w})$ are discretely-valued fields of characteristic 0 with the same value group and residue field. Hence they have the same completion E_1.

(d) This follows from Krasner's lemma [Jr, §12].

(e) Since $\hat{F}_v/F$ is a p-extension, so is the corresponding extension $\hat{E}/E$ of residue fields. Let $\hat{E}' = E(p) \cap E_1$ and let $\hat{w}'$ be the restriction to $\hat{E}'$ of w_1. By (c), $(\hat{E}', \hat{w}')$ is a valued field extension of $(\hat{E}, \hat{w})$ with the same value group and residue field. Furthermore, since $\hat{v}$ is p-Henselian, so is $\hat{w}$. Hence $\hat{w}'$ is the *unique* extension of $\hat{w}$ to $\hat{E}'$. Since $\hat{w}, \hat{w}'$ are discrete, the fundamental equality of valuation theory [Bo, Ch. VI, §8.5, Cor. 1] implies that $\hat{E} = \hat{E}'$.

(f) Clearly $(\hat{E}^\times)^p \leq \hat{E}^\times \cap (E_1^\times)^p$. For the converse take $a \in E_1$ such that $a^p \in \hat{E}^\times$. Then $\hat{E}(a) \subseteq E(p)$, so by (e), $a \in \hat{E}$, as desired.

(g) By Hensel's lemma again, the group of p-powers in $E_1^\times$ is open with respect to the w_1-topology on E_1. Since E is w_1-dense in E_1, the homomorphism $E^\times \to E_1^\times/(E_1^\times)^p$ is therefore surjective. Hence $E^\times/(E^\times \cap (E_1^\times)^p) \cong E_1^\times/(E_1^\times)^p$ canonically.

Since (E_1, w_1) is also the completion of $(\hat{E}, \hat{w})$ (by (c)), the same argument gives an isomorphism $\hat{E}^\times/(\hat{E}^\times \cap (E_1^\times)^p) \cong E_1^\times/(E_1^\times)^p$. Therefore, by (f), $\hat{E}^\times/(\hat{E}^\times)^p \cong E_1^\times/(E_1^\times)^p$.

(h) In light of Lemma 2.4(b), the exact sequences in (2.1) (for the valuation v' on F and for $S = (F^\times)^p G_v'$) give

$$(F^\times : (F^\times)^p G_v') \geq (E^\times : E^\times \cap (E_1^\times)^p) \quad .$$

By (g), $E^\times/(E^\times \cap (E_1^\times)^p) \cong E_1^\times/(E_1^\times)^p$. Moreover, E_1 contains a primitive pth root of unity. In light of the structure of the multiplicative group of p-adic fields, the latter group has $\mathbb{F}_p$-linear dimension $[E_1 : \mathbb{Q}_p] + 2 \geq 3$ (see e.g. [S1, Ch. XIV, §4] or [E9, Prop. 4.1]).

(i) The valuations $\hat{v}$, $\hat{v}'$, and $\hat{w}$ induce epimorphisms $\rho_{\hat{v}} \colon G_{\hat{F}_v}(p) \to G_{\bar{F}_v}(p)$, $\rho_{\hat{v}'} \colon G_{\hat{F}_v}(p) \to G_{\hat{E}}(p)$, and $\rho_{\hat{w}} \colon G_{\hat{E}}(p) \to G_{\bar{F}_v}(p)$, respectively, such that $\rho_{\hat{v}} = \rho_{\hat{w}} \circ \rho_{\hat{v}'}$. Their kernels are the corresponding inertia groups. Hence $\rho_{\hat{v}'}$ maps the inertia group of v in $F(p)$ onto the inertia group of $\hat{w}$ in $E(p)$. Also, $(\hat{E}, \hat{w})$ and (E_1, w_1) have the same residue field, so the restriction isomorphism $G_{E_1}(p) \xrightarrow{\sim} G_{\hat{E}}(p)$ maps the inertia group of w_1 in $E_1(p)$ bijectively onto the inertia group of $\hat{w}$ in $E(p)$. However, the inertia group of the p-adic valuation w_1 in $E_1(p)$ is nontrivial. We conclude that the inertia group of v in $F(p)$ is also nontrivial. $\square$

We now deduce an analog of Lemma 3.1 for the almost p-adic case:

Lemma 3.3. *Let v be an almost p-adic valuation on F and let $(\hat{F}_v, \hat{v})$ be a p-Henselization of (F, v). Then $F^\times/(F^\times)^p G'_v \cong \hat{F}_v^\times/(\hat{F}_v^\times)^p$ canonically.*

Proof. We use the notation of Proposition 3.2. Set $S = (F^\times)^p G'_v$ and $S_1 = (\hat{F}_v^\times)^p$. By Proposition 3.2(f), $E^\times \cap (E_1^\times)^p = E^\times \cap (\hat{E}^\times)^p$. Hence

$$G'_v = \pi_{v'}^{-1}(E^\times \cap (E_1^\times)^p) = \pi_{v'}^{-1}(E^\times \cap (\hat{E}^\times)^p) \leq \pi_{\hat{v}'}^{-1}((\hat{E}^\times)^p) = G_{\hat{v}'}(O_{\hat{v}'}^\times)^p \leq (\hat{F}_v^\times)^p,$$

where in the last step we used Hensel's lemma for $(\hat{F}_v, \hat{v}')$. Therefore $S \leq S_1$.

By Lemma 2.4(a) and Proposition 3.2(b), $v'(S) = pv'(F^\times) = p\hat{v}'(\hat{F}_v^\times) = \hat{v}'(S_1)$. By Lemma 2.4(b), $\bar{S}_{v'} = E^\times \cap (E_1^\times)^p$. Furthermore $(\overline{S_1})_{\hat{v}'} = (\hat{E}^\times)^p$.

Now $G_{v'} \leq S$ (Lemma 2.4(a)) and $G_{\hat{v}'} \leq S_1$. Hence the exact sequences in (2.1) for F, S, and v' (resp., $\hat{F}_v$, S_1, and $\hat{v}'$) give the exactness of the upper (resp., lower) row in the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \to & E^\times/(E^\times \cap (E_1^\times)^p) & \to & F^\times/S & \to & v'(F^\times)/p & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \hat{E}^\times/(\hat{E}^\times)^p & \to & \hat{F}_v^\times/(\hat{F}_v^\times)^p & \to & \hat{v}'(\hat{F}_v^\times)/p & \to & 0 \quad . \end{array}$$

By what we have seen, the right vertical map is an isomorphism. By Proposition 3.2(g) so is the left vertical map. We conclude that the middle vertical map is also an isomorphism. □

Lemma 3.4. *Suppose that $p = 2$ and let v be an almost 2-adic valuation on F. Then G'_v is not contained in any ordering on F.*

Proof. Suppose that $G'_v \leq P$ for some ordering P on F. By Lemma 2.4(a), $G_{v'} \leq G'_v \leq P$. Hence the push-down $\bar{P}_{v'}$ of P with respect to v' is an ordering on E [L, Prop. 2.9]. By Lemma 2.4(b), it contains $E^\times \cap (E_1^\times)^2$.

Now denote $w = v/v'$. The completion (E_1, w_1) of (E, w) is a 2-adic field, hence nonreal. Therefore there exist $0 \neq x_1, \ldots, x_r \in E_1$ with $\sum_{i=1}^r x^2 = -1$. Since E is w_1-dense in E_1, we can approximate $x_1, \ldots, x_r$ by elements $y_1, \ldots, y_r \in E$, respectively, so that $\sum_{i=1}^r y_i^2 \in -(1 + 4\mathfrak{m}_w)$. By Hensel's lemma, $1 + 4\mathfrak{m}_w \leq E^\times \cap (E_1^\times)^2$. We obtain the contradiction $\sum_{i=1}^r y_i^2 \in -\bar{P}_{v'}$. □

4. p-CONNECTED VALUATIONS

Let $\hat{D}_\infty = \varprojlim D_{2^n}$ be the infinite pro-2 dihedral group. Thus $\hat{D}_\infty = \mathbb{Z}_2 \rtimes (\mathbb{Z}/2)$, where the generator ε of $\mathbb{Z}/2$ acts on a generator τ of $\mathbb{Z}_2$ by $\tau^\varepsilon = \tau^{-1}$. Alternatively, $\hat{D}_\infty = (\mathbb{Z}/2) *_2 (\mathbb{Z}/2)$, where the free factors are generated by the involutions $\varepsilon, \varepsilon\tau$. It follows from the semi-direct product decomposition of $\hat{D}_\infty$ that its closed subgroups are of one of the forms 1, $\mathbb{Z}/2$, $\mathbb{Z}_2$, and $\hat{D}_\infty$.

A field E is **Euclidean** if $(E^\times)^2$ is an ordering on E. Equivalently, $G_E(2) \cong \mathbb{Z}/2$ [B]. We say that a valuation v on our field F is **exceptional** if $p = 2$, $(v(F^\times) : 2v(F^\times)) = 2$ and $\bar{F}_v$ is Euclidean. Then in particular char $\bar{F}_v = 0$ and $(F^\times : (F^\times)^2 G_v) = 4$, by (2.2).

Lemma 4.1. *Suppose that $p = 2$ and let (F, v) be a 2-Henselian valued field such that $v(F^\times) \neq 2v(F^\times)$. Then $G_F(2) \cong \hat{D}_\infty$ if and only if v is exceptional.*

Proof. The "if" part follows from the Galois theory of tame p-Henselian fields, as in §3(A).

For the "only if" part, suppose that $G_F(2) \cong \hat{D}_\infty$. By Kummer's theory,

$$F^\times/(F^\times)^2 \cong \mathrm{Hom}(G_F(2), \mathbb{Z}/2) = \mathrm{Hom}(\hat{D}_\infty, \mathbb{Z}/2) \cong (\mathbb{Z}/2)^2 \quad .$$

Since $\hat{D}_\infty$ contains involutions, F is an ordered field. Hence so is its residue field $\bar{F}_v$ [L, Th. 3.16(2)]. In particular, $\mathrm{char}\ \bar{F}_v = 0$ and $\bar{F}_v^\times \neq (\bar{F}_v^\times)^2$.

If $(v(F^\times) : 2v(F^\times)) > 2$, then $G_F(2) \cong \hat{D}_\infty$ would contain a copy of $\mathbb{Z}_2^2$ (see again §3(A)), a contradiction. Conclude that $(v(F^\times) : 2v(F^\times)) = 2$. By (2.2),

$$(v(F^\times) : 2v(F^\times))(\bar{F}_v^\times : (\bar{F}_v^\times)^2) = (F^\times : (F^\times)^2) = 4 \quad .$$

Therefore $(\bar{F}_v^\times : (\bar{F}_v^\times)^2) = 2$. Hence $\bar{F}_v$ is Euclidean and v is exceptional. □

Remark 4.2. This exceptional case can also be interpreted in terms of the theory of ordered fields. Namely, if v is an exceptional valuation on F, then $(F^\times)^2 G_v$ is a preordering on F which is contained in precisely two orderings. Hence it is a trivial fan, in the sense of [L, Def. 5.1]. However, not every fan which is contained in just two orderings arises from a valuation in this way. See [L, §5] for more information on fans and their connection to valuations.

Definition 4.3. We say that a valuation v on the field F is **p-connected** if:

(i) either $\mathrm{char}\ \bar{F}_v \neq p$ or v is almost p-adic;
(ii) $v(F^\times) \neq pv(F^\times)$;
(iii) $(F^\times : (F^\times)^p G'_v) > p$; and
(iv) v is not exceptional.

Lemma 4.4. *Let v be a p-connected valuation on F and let u be a valuation on F which is strictly coarser than v. Then:*

(a) $\mathrm{char}\ \bar{F}_u \neq p$;
(b) $G_u \leq G'_v \leq O_u^\times$.

Proof. If $\mathrm{char}\ \bar{F}_v \neq p$, then $p \notin \mathfrak{m}_v$, so $p \notin \mathfrak{m}_u$, whence (a). Moreover, $G'_v = G_v$, so $G_u \leq G'_v \leq O_v^\times \leq O_u^\times$ in this case.

Next suppose that v is almost p-adic. Then u is coarser than the finest coarsening v' of v. Since $\mathrm{char}\ \bar{F}_{v'} = 0$, also $\mathrm{char}\ \bar{F}_u = 0$. By Lemma 2.4(a), $G_u \leq G_{v'} \leq G'_v \leq O_{v'}^\times \leq O_u^\times$ in this case as well. □

Lemma 4.5. *Let v be a p-connected valuation on F. Then every coarsening u of v is nonexceptional.*

Proof. Suppose that u is exceptional. Then $p = 2$ and $\mathrm{char}\ \bar{F}_u = 0$. We choose 2-Henselizations $(\hat{F}_u, \hat{u})$, $(\hat{F}_v, \hat{v})$ of (F, u) and (F, v), respectively, such that $\hat{F}_u \subseteq \hat{F}_v$. The valuation $\hat{u}$ is also exceptional, so by Lemma 4.1, $G_{\hat{F}_u}(2) \cong \hat{D}_\infty$. Hence $G_{\hat{F}_v}(2)$ is isomorphic to one of $1, \mathbb{Z}/2, \mathbb{Z}_2$ or $\hat{D}_\infty$.

By condition (iii) of Definition 4.3, $(F^\times : (F^\times)^2 G'_v) > 2$. From Lemma 3.1 and Lemma 3.3 we deduce that $(\hat{F}_v^\times : (\hat{F}_v^\times)^2) > 2$, so $G_{\hat{F}_v}(2) \ncong 1, \mathbb{Z}/2, \mathbb{Z}_2$. Thus $G_{\hat{F}_v}(2) \cong \hat{D}_\infty$. It follows from Lemma 4.1 and from condition (ii) of Definition 4.3 that $\hat{v}$ is exceptional, and hence so is v. This contradicts condition (iv). □

5. p-EQUIVALENCE

The next result is the key fact needed for our generalization of Marshall's equivalence relation:

Proposition 5.1. *Let v_1, v_2 be p-connected valuations on F and let u be their finest common coarsening. If $(F^\times)^p G'_{v_1} G'_{v_2} < F^\times$, then u is p-connected as well.*

Proof. If v_1 is coarser (resp., finer) than v_2, then $v_1 = u$ (resp., $v_2 = u$), so u is p-connected.

We may therefore assume that v_1 and v_2 are incomparable. Then u is strictly coarser than both of them. We show that it satisfies conditions (i)–(iv) of Definition 4.3.

By Lemma 4.4(a), char $\bar{F}_u \neq p$, so $G'_u = G_u$ and condition (i) holds for u.

For $i = 1, 2$ Lemma 4.4(b) gives $G_u \leq G'_{v_i} \leq O_u^\times$. In particular, (iii) holds for u. Furthermore, by Lemma 2.5, $\pi_u(G'_{v_i})$ is v_i/u-open in $\bar{F}_u^\times$. Corollary 2.3 therefore implies that $O_u^\times = G'_{v_1} G'_{v_2}$. It follows from the assumption that $(F^\times)^p O_u^\times = (F^\times)^p G'_{v_1} G'_{v_2} < F^\times$. Hence condition (ii) holds for u.

Finally, Lemma 4.5 gives condition (iv). □

From this and from Lemma 4.4 we deduce:

Corollary 5.2. *Let T be a proper subgroup of $F^\times$ containing $(F^\times)^p$. The collection of all p-connected valuations v on F with $G'_v \leq T$ forms an inverse system with respect to coarsening; namely, if v_1, v_2 are in this collection, then so is their finest common coarsening.*

We denote the collection of all subgroups T of $F^\times$ such that $(F^\times : T) = p$ by $\mathcal{X}_p$.

Definition 5.3. We say that $T_1, T_2 \in \mathcal{X}_p$ are **p-equivalent** if either:

(i) $T_1 = T_2$; or
(ii) $T_1 \neq T_2$ and there is a p-connected valuation v on F such that $G'_v \leq T_1 \cap T_2$.

This relation is trivially reflexive and symmetric; Corollary 5.2 and Lemma 4.4 imply that it is transitive, hence an equivalence relation. When $p = 2$ it extends the Marshall-equivalence relation on orderings on a Pythagorean field, as we now show.

Proposition 5.4. *Assume that $p = 2$ and that F is Pythagorean. The following conditions on distinct orderings P_1, P_2 on F are equivalent:*

(a) *P_1, P_2 are 2-equivalent;*
(b) *P_1, P_2 are Marshall-equivalent;*
(c) *there is a valuation v on F such that $G_v \leq P_1, P_2$ and either*
  (1) *$(v(F^\times) : 2v(F^\times)) \geq 4$ or*
  (2) *$(v(F^\times) : 2v(F^\times)) = 2$, and there are at least two orderings on $\bar{F}_v$.*

Proof. (b)⇔(c): This is proved in [E1, Lemma 2.2].

(a)⇒(c): Take a 2-connected valuation v on F such that $G'_v \leq P_1, P_2$. By Lemma 3.4, v cannot be almost 2-adic. Hence char $\bar{F}_v \neq 2$, so $G'_v = G_v$. By condition (ii) of Definition 4.3, $(v(F^\times) : 2v(F^\times))$ is divisible by 2. If it is precisely 2, then $\bar{F}_v$ is not Euclidean (by Definition 4.3(iv)). However it is Pythagorean (since F is). Thus $(\bar{F}_v^\times)^2$ is the intersection of all orderings on $\bar{F}_v$. Consequently, there are at least two such orderings.

(c)⇒(a): Let v be as in (c). By [L, Prop. 2.9], $\bar{F}_v$ is an ordered field. Hence $\operatorname{char} \bar{F}_v = 0$, so again $G'_v = G_v$. By the exactness of (2.2),

$$(F^\times : (F^\times)^2 G_v) = (v(F^\times) : 2v(F^\times))(\bar{F}_v^\times : (\bar{F}_v^\times)^2) \geq 4 \quad .$$

Thus v is 2-connected, so P_1, P_2 are 2-equivalent. □

Let C be a p-equivalence class in $\mathcal{X}_p$ and let v be a p-connected valuation. We say that v **corresponds to** C if $G'_v \leq T$ for some $T \in C$. We note that every p-connected valuation corresponds to a unique p-equivalence class. Conversely, when $|C| > 1$ there is at least one p-connected valuation corresponding to C.

Lemma 5.5. *Suppose that C is a p-equivalence class in $\mathcal{X}_p$ with $|C| > 1$. Then $\bigcap C = \bigcap_v ((F^\times)^p G'_v)$, where v ranges over all p-connected valuations on F corresponding to C.*

Proof. Since $\bigcap_v ((F^\times)^p G'_v)$ contains $(F^\times)^p$, it is the intersection of all the groups $T \in \mathcal{X}_p$ containing it. Therefore it suffices to show that for $T \in \mathcal{X}_p$ one has $T \in C$ if and only if $\bigcap_v ((F^\times)^p G'_v) \leq T$.

Let $T \in \mathcal{X}_p$ contain $\bigcap_v (F^\times)^p G'_v$. Choose a p-connected valuation v corresponding to C. Thus there exists $T' \in C$ such that $G'_v \leq T'$. As $G'_v \leq T \cap T'$, the subgroups T, T' are p-equivalent. Hence $T \in C$.

Conversely, assume that $T \in C$. Choose $T \neq T' \in C$. Then T, T' are p-equivalent, so there exists a p-connected valuation v_0 such that $G'_{v_0} \leq T, T'$. Hence $\bigcap_v ((F^\times)^p G'_v) \leq (F^\times)^p G'_{v_0} \leq T$. □

Lemma 5.6. *Let C be a finite p-equivalence class in $\mathcal{X}_p$ with $|C| > 1$. Then there exists a p-connected valuation v on F corresponding to C and such that $\bigcap C = (F^\times)^p G'_v$. Moreover, this holds for every p-connected coarsening of v.*

Proof. By the finiteness assumption, $(F^\times : \bigcap C) < \infty$. Therefore Lemma 5.5 gives rise to p-connected valuations $v_1, \ldots, v_n$ corresponding to C such that $\bigcap C = \bigcap_{i=1}^n ((F^\times)^p G'_{v_i})$. The finest common coarsening v_0 of $v_1, \ldots, v_n$ is p-connected (Proposition 5.1).

In light of Corollary 5.2 it suffices to show that $\bigcap C = (F^\times)^p G'_v$ for every p-connected coarsening v of v_0. Indeed, by Lemma 4.4(b), $G'_v \leq G'_{v_i}$, $i = 1, \ldots, n$. Hence v also corresponds to C, so we are done by Lemma 5.5 again. □

Corollary 5.7. *Let C be a finite p-equivalence class in $\mathcal{X}_p$ and let $T \in \mathcal{X}_p$. Then $T \in C$ if and only if $\bigcap C \leq T$.*

Proof. The "only if" part is trivial, and so is the "if" part when $|C| = 1$. Suppose that $|C| > 1$ and $\bigcap C \leq T$. Lemma 5.6 yields a p-connected valuation v on F corresponding to C such that $\bigcap C = (F^\times)^p G'_v$. Choose $T' \in C$. Then $G'_v \leq T \cap T'$, so T, T' are p-equivalent. We conclude that $T \in C$. □

It is convenient to distinguish between the following three types of p-equivalence classes C in $\mathcal{X}_p$:

TYPE 1: $C = \{P\}$, with P an ordering on F (then necessarily $p = 2$, since otherwise $-1 \in (F^\times)^p \leq P$).

TYPE 2: $C = \{T\}$, with T not an ordering.

TYPE 3: $|C| > 1$.

Definition. Let C be a p-equivalence class in $\mathcal{X}_p$. A **closure** of F at C will be a subextension $F \subseteq \hat{F} \subseteq F(p)$ as follows:

- if $C = \{P\}$ is of type 1, then $\hat{F}$ is a Euclidean closure of F at P;
- if $C = \{T\}$ is of type 2, then $T \leq (\hat{F}^\times)^p$ and $F^\times/T \cong \hat{F}^\times/(\hat{F}^\times)^p$ canonically;
- if C is of type 3, then $\hat{F}$ is a p-Henselization of F with respect to a p-connected valuation v corresponding to C such that $F^\times/\bigcap C \cong \hat{F}^\times/(\hat{F}^\times)^p$ canonically.

Such a closure always exists. Indeed, for C of type 1 this follows from [B]. For C of type 2 it follows from Kummer theory. For C of type 3 Lemma 5.6 yields a p-connected valuation v corresponding to C such that $\bigcap C = (F^\times)^p G'_v$, and we apply Lemma 3.1 and Lemma 3.3.

If $\hat{F}$ is a closure of F at C, then so is $\sigma(\hat{F})$ for every $\sigma \in G_F(p)$. Also, for all three types, $F^\times/\bigcap C \cong \hat{F}^\times/(\hat{F}^\times)^p$ canonically. Consequently we get the following generalization of part (4) of the Jacob–Marshall decomposition theory, as described in the Introduction.

Proposition 5.8. *Let $\hat{F}$ be a closure of F at a finite equivalence class C. Then C consists of all restrictions $F \cap \hat{T}$ to F of subgroups $\hat{T}$ of $\hat{F}^\times$ of index p.*

Proof. Use the canonical isomorphism $F^\times/\bigcap C \cong \hat{F}^\times/(\hat{F}^\times)^p$ and Corollary 5.7. □

6. Free pro-p products of Galois groups

We say that a pro-p group H is **indecomposable** if it cannot be written as a free pro-p product $H = H_1 *_p H_2$, with H_1, H_2 nontrivial closed subgroups of H. We say that H is **strongly indecomposable** if it is generated by a collection of closed indecomposable finitely generated subgroups $H_i \ncong \mathbb{Z}_p$, $i \in I$, such that $H_i \cap H_j \neq 1$ for all distinct $i, j \in I$. Clearly, every finitely generated indecomposable pro-p group $H \ncong \mathbb{Z}_p$ is strongly indecomposable. Conversely, a strongly indecomposable group is indecomposable — this is an immediate consequence of the following result, which is proved in [E3, Lemma 5.1]:

Proposition 6.1. *Let $H, G_1, \ldots, G_n$ be closed subgroups of a pro-p group G such that $G = G_1 *_p \cdots *_p G_n$ and such that H is strongly indecomposable. Then there exist $1 \leq j \leq n$ and $\sigma \in G$ such that $H \leq G_j^\sigma$.*

Next we show that closures at p-equivalence classes give rise to indecomposable pro-p Galois groups. To this end we first need a few preliminary facts.

Given a pro-p group G let $H^r(G) = H^r(G, \mathbb{Z}/p)$ be the rth profinite cohomology group of G with respect to its trivial action on $\mathbb{Z}/p$ [S2]. Let $H^*(G) = \bigoplus_{r=0}^{\infty} H^r(G)$ be the cohomology ring with the cup product. One says that G is a **Demuškin group** [S2, I, §4.5] if it is finitely generated, $H^2(G) \cong \mathbb{Z}/p$, and the cup product $\cup\colon H^1(G) \times H^1(G) \to H^2(G)$ is nondegenerate (i.e., it has trivial left and right kernels).

Lemma 6.2. *A pro-p Demuškin group is indecomposable.*

Proof. Let G_1, G_2 be closed subgroups of a pro-p Demuškin group G with $G = G_1 *_p G_2$. Then $H^1(G_1) \cup H^1(G_2) = 0$ in $H^2(G)$, and $H^2(G) = H^2(G_1) \oplus H^2(G_2) \cong \mathbb{Z}/p$. Therefore, without loss of generality, $H^2(G_1) = 0$. For every $\varphi \in H^1(G_1)$ we obtain that

$$\varphi \cup H^1(G) = \varphi \cup H^1(G_1) + \varphi \cup H^1(G_2) = 0 \quad .$$

Since the cup product is nondegenerate, $\varphi = 0$. Thus $H^1(G_1) = 0$, so $G_1 = 1$. □

We will also need the following fact which is proved in [E3, Lemma 5.3 and Lemma 5.4]:

Proposition 6.3. *Let L be a field of characteristic $\neq p$ containing the roots of unity of order p. Suppose that $G_L(p) \not\cong \mathbb{Z}_p, \hat{D}_\infty$ and that L is p-Henselian with respect to a valuation $\hat{v}$ such that $\hat{v}(L^\times) \neq p\hat{v}(L^\times)$ and* char $\bar{L}_{\hat{v}} \neq p$. *Then $G_L(p)$ is strongly indecomposable.*

We can now generalize part (1) of the Jacob–Marshall theory as in the Introduction:

Theorem 6.4. *Let $\hat{F}$ be a closure of F at a p-equivalence class C. Then $G_{\hat{F}}(p)$ is indecomposable. Moreover, if C has type* 1 *or* 3, *then $G_{\hat{F}}(p)$ is strongly indecomposable.*

Proof. When C has type 1, $p = 2$ and $\hat{F}$ is Euclidean, so $G_{\hat{F}}(p) \cong \mathbb{Z}/2$ is strongly indecomposable.

When C has type 2, $\hat{F}^\times/(\hat{F}^\times)^p \cong \mathbb{Z}/p$, so $G_{\hat{F}}(p)$ is pro-p cyclic and nontrivial. Hence it is indecomposable (in fact, $G_{\hat{F}}(p) \cong \mathbb{Z}_p$).

Finally suppose that C has type 3. Then $\hat{F}$ is a p-Henselization of F with respect to a p-connected valuation v corresponding to C. If char $\bar{F}_v \neq p$, then $G_{\hat{F}}(p)$ is strongly indecomposable by Proposition 6.3.

If char $\bar{F}_v = p$, then v is almost p-adic. Let $v', \hat{v}', E, \hat{E}, E_1$ be as in Proposition 3.2. When $\hat{v}'(F^\times) \neq p\hat{v}'(F^\times)$ we are done again by Proposition 6.3. Finally, suppose that $\hat{v}'(F^\times) = p\hat{v}'(F^\times)$. Then $G_{\hat{F}}(p) \cong G_{\hat{E}}(p)$ (see §3(A)). Moreover, by Proposition 3.2(d)(e), $G_{\hat{E}}(p) \cong G_{E_1}(p)$. Since E_1 is a p-adic field containing the roots of unity of order p, local class field theory implies that $G_{E_1}(p)$ is a finitely generated pro-p Demuškin group of rank ≥ 3 [S2, II, §5.6, Th. 4]. By Lemma 6.2 it is indecomposable. Being finitely generated and not isomorphic to $\mathbb{Z}_p$, it is in fact strongly indecomposable. □

Lemma 6.5. *Let $F \subseteq L_1, \ldots, L_n \subseteq F(p)$ be intermediate fields such that $G_F(p) = G_{L_1}(p) *_p \cdots *_p G_{L_n}(p)$. For each $1 \leq i \leq n$ let $S_i = F^\times \cap L_i^p$. Let T be a group in $\mathcal{X}_p$ which contains S_i for some $1 \leq i \leq n$, and let C be the p-equivalence class of T. Then:*

(a) *$S_i \leq \bigcap C$; and*
(b) *there is a closure $\hat{F}$ of F at C containing L_i.*

Proof. The decomposition $H^1(G_F(p)) = \bigoplus_{l=1}^n H^1(G_{L_l}(p))$ combined with the Kummer isomorphism gives a canonical isomorphism $F^\times/(F^\times)^p \cong \bigoplus_{l=1}^n L_l^\times/(L_l^\times)^p$ (recall that F contains the pth roots of unity). It follows that $F^\times/S_l \cong L_l^\times/(L_l^\times)^p$, $l = 1, \ldots, n$, and $F^\times/(F^\times)^p \cong \prod_{l=1}^n F^\times/S_l$ canonically. Therefore $F^\times = S_i \cdot \bigcap_{l \neq i} S_l$.

Assume first that C has type 1 or type 3. Choose a closure $\hat{F}$ of F at C. By Theorem 6.4, $G_{\hat{F}}(p)$ is strongly indecomposable. Proposition 6.1 therefore yields $1 \leq j \leq n$ and $\sigma \in G_F(p)$ such that $L_j \subseteq \sigma(\hat{F})$. We may replace $\hat{F}$ by $\sigma(\hat{F})$ to assume without loss of generality that $\sigma = 1$. Then

$$S_j = F^\times \cap L_j^p \leq F^\times \cap \hat{F}^p = \bigcap C \leq T \quad ,$$

as well as $S_i \leq T$. Since $T \neq F^\times$ and $F^\times = S_i \cdot S_l$ for $l \neq i$, these two facts imply that $i = j$. Thus $S_i \leq \bigcap C$ and $L_i \subseteq \hat{F}$, as desired.

Finally, suppose that C has type 2, i.e., $C = \{T\}$ with T not an ordering. Then (a) is clear. Since $S_i \le T \in \mathcal{X}_p$ and $F^\times/S_i \cong L_i^\times/(L_i^\times)^p$ canonically, there exists a unique subgroup $T' < L_i^\times$ of index p containing T and such that $F^\times/T \cong L_i^\times/T'$. Next Kummer theory gives rise to a subextension $L_i \subseteq \hat{F} \subseteq F(p)$ such that $T' \le (\hat{F}^\times)^p$ and $L_i^\times/T' \cong \hat{F}^\times/(\hat{F}^\times)^p$ canonically. Then $T = F^\times \cap \hat{F}^p$. Thus $\hat{F}$ is a closure of F at C as required in (b). □

We can now generalize part (3) of the Jacob–Marshall decomposition theory:

Theorem 6.6. *Let $F \subseteq L_1, \dots, L_n \subseteq F(p)$ be intermediate fields. Suppose that $G_F(p) = G_{L_1}(p) *_p \cdots *_p G_{L_n}(p)$. Then each free factor $G_{L_i}(p)$ is generated by subgroups of the form $G_{\hat{F}}(p)$ for closures $\hat{F}$ of F at p-equivalence classes.*

Proof. For each $1 \le i \le n$ we again set $S_i = F^\times \cap L_i^p$. Since S_i contains $(F^\times)^p$, it is the intersection of all the groups $T \in \mathcal{X}_p$ containing it. Given such T, let C_T be its p-equivalence class. By Lemma 6.5, $S_i \le \bigcap C_T \le T$, and furthermore, F has a closure $\hat{F}_T$ at C_T containing L_i. Hence $S_i = \bigcap_T(\bigcap C_T) = \bigcap_T(F^\times \cap \hat{F}_T^p)$, where the intersection is over all $T \in \mathcal{X}_p$ containing S_i. Let $M_i = \bigcap_T \hat{F}_T$. Then $L_i \subseteq M_i \subseteq F(p)$ and $S_i = F^\times \cap M_i^p$. Thus the composed homomorphism

$$F^\times/S_i \;\to\; L_i^\times/(L_i^\times)^p \;\to\; M_i^\times/(M_i^\times)^p$$

is injective. The left map is an isomorphism, so the right map is also injective. This implies that $L_i = M_i$. The assertion follows. □

7. Elementary decompositions

In this final section we relate our results to the arithmetic pro-p version of the elementary-type conjecture as discussed in the Introduction. To this end we need several preliminary results. Part (a) of the following Proposition is proved in [E5, Prop. 3.4]. Part (b) is implicit in the proof of [P, Kor. 2.7] (and was explicitly stated in [E5, Prop. 3.1]).

Proposition 7.1. *Let v be a valuation on F such that* char $\bar{F}_v = p$. *Suppose that $F^\times/(F^\times)^p$ is finite.*

(a) *If $v(F^\times)$ is p-divisible and v is p-Henselian, then $G_F(p)$ is a free pro-p group.*
(b) *If $v(F^\times)$ is not p-divisible and has rank 1, then it is isomorphic to $\mathbb{Z}$ and $\bar{F}_v$ is finite.*

Note that since F contains the pth roots of unity, $F^\times/(F^\times)^p$ is finite if and only if $G_F(p)$ is finitely generated.

Lemma 7.2. *Let v be a valuation on F with p-Henselization of $\hat{F}_v$. Suppose that:*

(1) *the inertia group of v in $F(p)$ is nontrivial;*
(2) *$G_{\hat{F}_v}(p)$ is not a free pro-p group and is not $\hat{D}_\infty$;*
(3) *$G_F(p)$ is finitely generated.*

Then:

(a) *every coarsening u of v with* char $\bar{F}_u \ne p$ *and $u(F^\times) \ne pu(F^\times)$ is p-connected.*
(b) *there exists a p-connected valuation u on F which is coarser than v.*

Proof. (a) Conditions (i) and (ii) of Definition 4.3 hold by assumption.

Next we claim that $G_{\hat{F}_v}(p) \ncong \mathbb{Z}/2$. Otherwise $p = 2$ and $\hat{F}_v$ is an ordered field. Therefore so is its residue field $\bar{F}_v$ [L, Th. 3.16(2)]. Furthermore, since the inertia group of v is nontrivial (by (1)), it must be all of $G_{\hat{F}_v}(2)$. Hence $\bar{F}_v$ is quadratically closed, and therefore carries no orderings, a contradiction.

The claim and (2) imply that $G_{\hat{F}_v}(p)$ does not embed in $\hat{D}_\infty$. Take a p-Henselization $(\hat{F}_u, \hat{u})$ of (F, u) such that $\hat{F}_u \subseteq \hat{F}_v$. It follows that $G_{\hat{F}_u}(p)$ is not pro-p cyclic and is not isomorphic to $\hat{D}_\infty$. Now by Lemma 3.1, $(F^\times : (F^\times)^p G_u) = (\hat{F}_u^\times : (\hat{F}_u^\times)^p) > p$, proving condition (iii). By Lemma 4.1, $\hat{u}$ is not exceptional, and therefore neither is u, proving condition (iv).

(b) If $\mathrm{char}\, \bar{F}_v \neq p$, then by (1), $v(F^\times)/p \neq 0$. In light of (a), we may therefore take $u = v$ in this case.

Next suppose that $\mathrm{char}\, \bar{F}_v = p$. The Zariski spectrum of the valuation ring O_v is linearly ordered by inclusion. Hence there are coarsenings v', v'' of v with v' coarser than v'', such that $w = v''/v'$ has rank 1, $\mathrm{char}\, \bar{F}_{v'} = 0$, and $\mathrm{char}\, \bar{F}_{v''} = p$ [E9, Lemma 1.7]. If $v'(F^\times)/p \neq 0$, then, by (a), we may take $u = v'$.

Finally, suppose that $v'(F^\times)/p = 0$. Let $E = \bar{F}_{v'}$. Then $\mathrm{char}\, E = 0$. By (3), $F^\times/(F^\times)^p$ is finite, and hence so is its epimorphic image $\hat{F}_v^\times/(\hat{F}_v^\times)^p$ (see Lemma 3.3). Also, $w(E^\times)/p \cong v(F^\times)/p = \hat{v}(\hat{F}_v^\times)/p$ (by (2.3)). In light of assumption (2), Proposition 7.1(a) for $(\hat{F}_v, \hat{v})$ now implies that the latter group is nontrivial. Also, since $F^\times/(F^\times)^p$ is finite, so is $E^\times/(E^\times)^p = \bar{F}_{v'}^\times/(\bar{F}_{v'}^\times)^p$ (by (2.2)). Hence Proposition 7.1(b) for (E, w) shows that $w(E^\times) \cong \mathbb{Z}$ and $\bar{F}_{v''} = \bar{E}_w$ is finite. Therefore the valuation v/v'' on this field is trivial, i.e., $v = v''$. It follows that v is almost p-adic. Furthermore, since $\mathrm{char}\, \bar{F}_v = p > 0$, v is not exceptional. Finally, Proposition 3.2(h) shows that $(F^\times : (F^\times)^p G'_v) > p$. Conclude that in this case $u = v$ is p-connected. □

Call a subextension $F \subseteq L \subseteq F(p)$ p-**local** if either:

- $G_L(p) \cong \mathbb{Z}/2$ (i.e., $p = 2$ and L is Euclidean);
- $G_L(p) \cong \mathbb{Z}_p$; or
- L is a p-Henselization of F with respect to a valuation v having a nontrivial inertia group in $F(p)$.

Proposition 7.3. *For $G_F(p)$ finitely generated, the following conditions are equivalent:*

(a) *there exist p-local subextensions $F \subseteq L_1, \ldots, L_n \subseteq F(p)$ such that*

$$G_F(p) = G_{L_1}(p) *_p \cdots *_p G_{L_n}(p) \quad ;$$

(b) *there exist closures $L_1, \ldots, L_n$ of F with respect to p-equivalence classes such that*

$$G_F(p) = G_{L_1}(p) *_p \cdots *_p G_{L_n}(p) \quad .$$

Proof. (a)⇒(b): As $G_F(p)$ is finitely generated, so are its quotients $G_{L_i}(p)$, $i = 1, \ldots, n$. If any of these free factors is a free pro-p group, then we may decompose it further into finitely many factors of the form $\mathbb{Z}_p$. We may therefore assume that each of the factors is either isomorphic to $\mathbb{Z}_p$ or is not a free pro-p group. Likewise, if $G_{L_i}(p) \cong \hat{D}_\infty = (\mathbb{Z}/2) *_2 (\mathbb{Z}/2)$ for some $1 \leq i \leq n$, then we can replace $G_{L_i}(p)$ by two factors of order 2. Thus we may assume that $G_{L_i}(p) \ncong \hat{D}_\infty$ for all i.

With these assumptions being made, we now show that each L_i is a closure of F at some p-equivalence class.

By Theorem 6.6 each $G_{L_i}(p)$ is generated by subgroups of the form $G_{\hat{F}}(p)$, where $\hat{F}$ is a closure of F at some p-equivalence class. If $G_{L_i}(p)$ is pro-p cyclic, then it must coincide with one such group, so L_i is a closure as desired.

Next suppose that $G_{L_i}(p)$ is not pro-p cyclic. Then $L_i = \hat{F}_v$ is a p-Henselization of F with respect to a valuation v having a nontrivial inertia group in $F(p)$. In light of the reductions above, Lemma 7.2(b) yields a p-connected coarsening u of v.

Let C be the unique p-equivalence class to which u corresponds. Note that $|C| > 1$. In light of Lemma 5.6, we may replace u by a coarser p-connected valuation to assume without loss of generality that $\bigcap C = (F^\times)^p G'_u$. Let $\hat{F}_u$ be a p-Henselization of (F, u). In light of Lemma 3.1 and Lemma 3.3, $F^\times / \bigcap C \cong \hat{F}_u^\times / (\hat{F}_u^\times)^p$. Thus $\hat{F}_u$ is a closure of F at C. After replacing $\hat{F}_u$ by an F-isomorphic copy we may also assume that $\hat{F}_u \subseteq \hat{F}_v = L_i$. Since $G_{L_i}(p)$ is not pro-p cyclic, neither is $G_{\hat{F}_u}(p)$. Theorem 6.4 therefore implies that $G_{\hat{F}_u}(p)$ is strongly indecomposable. Now Proposition 6.1 gives rise to $1 \leq j \leq n$ and $\sigma \in G_F(p)$ such that $G_{\hat{F}_u}(p) \leq G_{L_j}(p)^\sigma$. Also, $G_{L_i}(p) \leq G_{\hat{F}_u}(p)$. In particular, $G_{L_i}(p) \cap G_{L_j}(p)^\sigma \neq 1$. In light of the structure theory of free pro-p products ([HR, Th. B'], [Mel, Prop. 4.9]), this can happen only when $i = j$ and $\sigma \in G_{L_i}(p)$. It follows that $\hat{F}_u = L_i$, and we are done once again.

(b)⇒(a): We show that every closure $\hat{F}$ of F at a p-equivalence class C is p-local.

If $|C| = 1$, then $G_{\hat{F}}(p)$ is pro-p cyclic, so this follows from [B].

If $|C| > 1$, then $\hat{F} = \hat{F}_v$ is a p-Henselization of F with respect to some p-connected valuation v. If $\mathrm{char}\, \bar{F}_v \neq p$, then the inertia group of (F, v) in $F(p)$ is isomorphic to $\mathbb{Z}_p^m$, with $m = \dim_{\mathbb{F}_p}(v(F^\times)/p) \geq 1$ (§3(A)). Hence it is nontrivial. If v is almost p-adic, then its inertia group in $F(p)$ is nontrivial by Proposition 3.2(i). Conclude that $\hat{F}$ is p-local in this case as well. □

We call a free product decomposition as in Proposition 7.3(a) an **elementary decomposition** of $G_F(p)$. Thus the arithmetic version of the elementary-type conjecture discussed in the Introduction says that whenever F contains a primitive pth root of unity and $G_F(p)$ is finitely generated, $G_F(p)$ has an elementary decomposition.

A field is called **pseudo-algebraically closed** if every geometrically irreducible affine variety over it has a rational point in the field [FJ, Ch. X]. We now obtain a *partial* generalization of part (2) of the Jacob–Marshall decomposition theory:

Theorem 7.4. *Suppose that $G_F(p)$ is finitely generated. Then it has an elementary decomposition in each of the following cases:*

(i) *F is an algebraic extension of a global field;*
(ii) *F is an extension of transcendence degree ≤ 1 of a local field;*
(iii) *F is an extension of transcendence degree ≤ 1 of a pseudo-algebraically closed field;*
(iv) *F is an intersection of finitely many p-extensions of it which are either Euclidean (if $p = 2$) or p-Henselizations with respect to a valuation having nontrivial inertia groups and residue characteristics $\neq p$;*
(v) *$p = 2$ and F is Pythagorean.*

Proof. This is proved in [E4] and [E6] (for case (i)), [JP] and [E7] (for case (ii)), [E8] (case (iii)), [E3] (case (iv)), and [J] and [Mi] (case (v)); note that case (v) is contained in case (iv). □

Remark 7.5. As is explained in [JWr1] and [JWr2], when $p = 2$ an elementary decomposition of the finitely generated group $G_F(2)$ (as in Proposition 7.3(a)) gives a direct product decomposition of abstract Witt rings (in the sense of [Ma2]) $W(F) = W(L_1) \times \cdots \times W(L_n)$. Furthermore, the direct factors $W(L_i)$ have the following structure:

- When L_i is Euclidean, $W(L_i) \cong W(\mathbb{R})$.
- When $G_{L_i}(2) \cong \mathbb{Z}_2$ and $\sqrt{-1} \notin L_i$ one has $W(L_i) \cong W(\mathbb{F}_3)$.
- When $G_{L_i}(2) \cong \mathbb{Z}_2$ and $\sqrt{-1} \in L_i$ one has $W(L_i) \cong W(\mathbb{F}_5)$.
- When L_i is a 2-Henselization of F with respect to a valuation v with nontrivial inertia group in $F(2)$ and char $\bar{F}_v \neq 2$, one has $m = \dim_{\mathbb{F}_2}(v(F^\times)/2v(F^\times)) \geq 1$ (§3(A)), and $W(L_i)$ is the extension of $W(\bar{F}_v)$ by an elementary abelian 2-group of rank m (see [Ma2]).
- When L_i is a 2-Henselization of F with respect to a valuation v with char $\bar{F}_v = 2$, the Witt ring $W(L_i)$ has elementary type [E5, Th. 5.5]. In fact, the proof of [E5, Th. 5.5] shows that $W(L_i)$ is an extension by an elementary abelian 2-group of either the Witt ring of a dyadic field, or of the direct product of finitely many Witt rings of finite fields.

Thus the arithmetic version of the elementary-type conjecture (for maximal pro-2 Galois groups) implies the elementary-type conjecture for Witt rings.

References

[B] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern,* J. reine angew. Math. **268–269** (1974), 41–52. MR0354625 (50:7103)

[Bo] N. Bourbaki, *Commutative Algebra,* Hermann, Paris, 1972. MR0360549 (50:12997)

[Br] L. Bröcker, *Characterization of fans and hereditarily pythagorean fields*, Math. Z. **151** (1976), 149–163. MR0422233 (54:10224)

[C1] T.C. Craven, *Characterizing reduced Witt rings of fields,* J. Algebra **53** (1978), 68–77. MR0480332 (58:505)

[C2] T.C. Craven, *Characterizing reduced Witt rings II,* Pacific J. Math. **80** (1979), 341–349. MR0539420 (80i:10025)

[E1] I. Efrat, *Free product decompositions of Galois groups over pythagorean fields,* Comm. Algebra **21** (1993), 4495–4511. MR1242845 (95a:12003)

[E2] I. Efrat, *Orderings, valuations and free products of Galois groups,* In: Séminaire de Structures Algébriques Ordonnées, Lecture Notes No. **54**, University of Paris VII, 1995.

[E3] I. Efrat, *Free pro-p product decompositions of Galois groups,* Math. Z. **225** (1997), 245–261. MR1464929 (98i:12004)

[E4] I. Efrat, *Pro-p Galois groups of algebraic extensions of* $\mathbb{Q}$, J. Number Theory **64** (1997), 84–99. MR1450486 (98i:11096)

[E5] I. Efrat, *Finitely generated pro-p Galois groups of p-henselian fields,* J. Pure Appl. Algebra **138** (1999), 215–228. MR1691472 (2000e:12011)

[E6] I. Efrat, *Finitely generated pro-p absolute Galois groups over global fields*, J. Number Theory **77** (1999), 83–96. MR1695702 (2000c:12007)

[E7] I. Efrat, *Pro-p Galois groups of function fields over local fields,* Comm. Algebra **28** (2000), 2999–3021. MR1757442 (2001g:12001)

[E8] I. Efrat, *A Hasse principle for function fields over PAC fields,* Israel J. Math. **122** (2001), 43–60. MR1826490 (2002a:14018)

[E9] I. Efrat, *Demuškin fields with valuations,* Math. Z. **243** (2003), 333–353. MR1961869 (2004d:11116)

[EH] I. Efrat and D. Haran, *On Galois groups over pythagorean and semi-real closed fields,* Israel J. Math. **85** (1994), 57–78. MR1264339 (94m:12002)

[FeV] I.B. Fesenko and S.V. Vostokov, *Local Fields and their Extensions – A Constructive Approach,* AMS, Providence, Rhode Island, 1993. MR1218392 (94d:11095)

[FJ] M. Fried and M. Jarden, *Field Arithmetic*, Springer, Heidelberg, 1986. MR0868860 (89b:12010)

[H] D. Haran, *On closed subgroups of free products of profinite groups,* Proc. London Math. Soc. **55** (1987), 266–298. MR0896222 (88i:20047)

[HR] W.N. Herfort and L. Ribes, *Torsion elements and centralizers in free products of profinite groups,* J. reine angew. Math. **358** (1985), 155–161. MR0797680 (86k:20024)

[HwJ] Y.S. Hwang and B. Jacob, *Brauer group analogues of results relating the Witt ring to valuations and Galois theory,* Canad. J. Math. **47** (1995), 527–543. MR1346152 (97a:12004)

[J] B. Jacob, *On the structure of Pythagorean fields,* J. Algebra **68** (1981), 247–267. MR0608534 (82g:12020)

[JWr1] B. Jacob and R. Ware, *A recursive description of the maximal pro-2 Galois group via Witt rings,* Math. Z. **200** (1989), 379–396. MR0978598 (90b:11127)

[JWr2] B. Jacob and R. Ware, *Realizing dyadic factors of elementary type Witt rings and pro-2 Galois groups,* Math. Z. **208** (1991), 193–208. MR1128705 (92h:11032)

[Jr] M. Jarden, *Intersections of local algebraic extensions of a Hilbertian field*, NATO Adv. Sci. Inst. Ser. C, *"Generators and Relations in Groups and Geometries"*, Ed.: Barlotti et. al., pp. 343–405, 1991. MR1206921 (94c:12003)

[JP] C.U. Jensen and A. Prestel, *Finitely generated pro-p-groups as Galois groups of maximal p-extensions of function fields over $\mathbb{Q}_q$,* manusc. math. **90** (1997), 225–238. MR1391210 (97f:11091)

[L] T.Y. Lam, *Orderings, valuations and quadratic forms,* Conf. Board of the Mathematical Sciences **52**, AMS 1983. MR0714331 (85e:11024)

[Ma1] M. Marshall, *Spaces of orderings IV,* Canad. J. Math. **32** (1980), 603–627. MR0586979 (81m:10035)

[Ma2] M. Marshall, *Abstract Witt Rings,* Queen's Pap. Pure Appl. Math. **57**, Kingston, 1980. MR0674651 (84b:10032)

[Ma3] M. Marshall, *Spaces of Orderings and Abstract Real Spectra,* Lect. Notes Math. **1636**, Springer, Berlin–Heidelberg, 1996. MR1438785 (98b:14041)

[Ma4] M. Marshall, *The elementary type conjecture in quadratic form theory,* Cont. Math. **344** (2004), 275–293. MR2060204 (05b:11046)

[Mel] O.V. Melnikov, *Subgroups and homologies of free products of profinite groups,* Izvestiya Akad. Nauk SSSR, Ser. Mat. **53** (1989), 97–120 (Russian); Math. USSR Izvestiya **34** (1990), 97–119 (English translation). MR0992980 (91b:20033)

[Mer] J. Merzel, *Quadratic forms over fields with finitely many orderings,* Contemporary Math. **8** (1982), 185–229. MR0653183 (83j:10021)

[Mi] J. Mináč, *Galois groups of some 2-extensions of ordered fields,* C.R. Math. Rep. Acad. Sci. Canada **8** (1986), 103–108. MR0831786 (88k:12003a)

[P] F. Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper,* J. reine angew. Math. **392** (1988), 145–175. MR0965062 (89k:12014)

[S1] J.-P. Serre, *Local Fields,* Springer, Berlin, 1979. MR0554237 (82e:12016)

[S2] J.-P. Serre, *Galois Cohomology,* Springer Monographs in Mathematics, Springer, Berlin Heidelberg, 1997. MR1466966 (98g:12007)

[Wd] A.R. Wadsworth, *p-Henselian fields: K-theory, Galois cohomology, and graded Witt rings,* Pac. J. Math. **105** (1983), 473–496. MR0691616 (84m:12026)

Department of Mathematics, Ben-Gurion University of the Negev, P.O. Box 653, Be'er-Sheva 84105, Israel

E-mail address: efrat@math.bgu.ac.il